Shojiro Asai *Editor*

VLSI Design and Test for Systems Dependability

Springer

VLSI Design and Test for Systems Dependability

A group picture of participants in the DVLSI Program: researchers from universities, national laboratories and industry, external program advisors and the staff members of JST are photographed. 13 March, 2013

Shojiro Asai
Editor

VLSI Design and Test for Systems Dependability

Springer

Editor
Shojiro Asai
Rigaku Corporation
Tokyo
Japan

ISBN 978-4-431-56592-5 ISBN 978-4-431-56594-9 (eBook)
https://doi.org/10.1007/978-4-431-56594-9

Library of Congress Control Number: 2017963009

Printed on acid-free paper

This Springer imprint is published by the registered company Springer Japan KK part of Springer Nature
The registered company address is: Shiroyama Trust Tower, 4-3-1 Toranomon, Minato-ku, Tokyo 105-6005, Japan

Preface

The technological progress, with its tremendous economic impact, of electronic systems stands out among other industrial products of modern times and has produced various innovations over the last 50 years or so. It has had two major enablers, computer programs and the very-large-scale integration (VLSI) of semiconductor circuits. The concept of programed computing first materialized in computers that crunched alphanumeric data. The computer program has gone through a remarkable transformation since the introduction of high-level programing languages, close in form to human languages, describing how information is to be processed in the system; translating the program into machine-executable codes became a part of the job of computers. Electronic systems hardware has likewise shown progress in performance at an unprecedented pace starting out from the vacuum tube to the transistor to VLSI. High-performance computers, consisting of thousands of VLSI processors, each one containing billions of transistors, are being used for scientific calculations and big-data analysis. More remarkably, VLSI is used today in a far greater variety of electronic systems. Public infrastructures, such as transportation, utilities, public safety, and telecommunications, are large-scale electronic systems. Consumer items such as cell phones and automobiles are other examples of advanced electronic systems. All these electronic systems, in contrast to computers used for general computing, are customarily called computer-embedded systems. Progress in the development of these systems has been driven by the evolution of computer software (programing) and electronic hardware (VLSI among others), considered as twin engines working in harmony.

The three most important value metrics of an electronic system are performance, cost (price), and dependability. All three are carefully considered when a user is about to buy a system, or a manufacturer contemplates developing a system for sale. What is meant by performance and cost (price) is obvious and is talked about in terms of straightforward quantitative metrics. The concept of dependability, a term that has evolved from reliability, has expanded its attributes to range from a relatively simple quantity, such as mean time to failure (MTTF), a good statistical index of the availability of systems, to far harder to quantify metrics such as safety and tamper resistance. The bearings of dependability have become much more important as humans increasingly rely on the convenience and benefit of electronic systems while the scale and severity of the detrimental effects of potential failures in such systems have become more devastating. The purpose of this book is to discuss how design and testing can help mitigate threats to the dependability of VLSI systems. Here the term VLSI system is meant to cover not only VLSI per se but also electronic systems that use VLSI (of semiconductor circuits) as a key component.

This book consists of three parts. Part I is a general introduction to the book and is made up of two chapters. It starts by describing in Chap. 1 the background and motivation that led to the undertaking of a government-funded research program entitled, "Fundamental technologies for dependable VLSI systems (called DVLSI hereafter)," funded by the Japan Science and Technology Agency (JST) under the Core Research of Evolutional Science and Technology (CREST) initiative. The program was started in April 2007 and lasted for about 8 years until March 2015, with 11 teams of researchers participating from universities, government laboratories, and industrial corporations. The rest of Chap. 1 describes the scope, activities, and management of the program. Detailed accounts are given as to how overarching issues of dependability were covered, how efforts were made to push expected deliverables toward applications, how exciting industry–academia collaborations were promoted during the term, and the final outcomes of the program. Chapter 2 begins with a quick overview of the principles and disciplines of design and verification/testing of electronic systems. Then, using this as a background, the implications of new technologies developed in the DVLSI program are discussed in light of other emerging trends in technology and the markets.

Part II of this book is entitled, "VLSI Issues in Systems Dependability." Chapters 3 through 12 discuss various threats to the dependability of VLSIs: ionizing radiation, electromagnetic interference, time-dependent degradation, variations in device characteristics, design errors, malicious tampering, etc., and what design and testing can do to manage these threats. Part III, which is entitled, "Design and Test of VLSI for Systems Dependability," consists of Chaps. 13 through 29, which describe technologies developed in the program as possible solutions for dependability in the design and testing of realistic systems such as robots and vehicles, data processing and storage in the cloud environment, wireless public telecommunications with improved connectivity, advanced electronic packaging with wireless interconnect, and so forth. Most chapters and sections of Part II and Part III are authored by the members of research teams in the DVLSI program, but some are contributed by "invited" authors, who, having participated in the various events of the program in one way or other, kindly agreed to express their thoughts in this book.

This book is intended to be a reference for engineers who work on the design and testing of electronic systems with particular attention on dependability. It can be used as an auxiliary textbook in undergraduate and graduate courses as well. It is also hoped that readers of this book with non-engineering backgrounds, such as mathematics and social economists, will gain insight into the problems of systems dependability, and may consider taking them on as innovative challenges.

It was a real pleasure to be able to work with the members of the DVLSI program, and to witness industry–university collaborations from inception to fruition. I am thankful to numerous speakers from outside the program who gave stimulating talks and shared thoughts and discussions at program conferences. It was good to have been able to interact and exchange ideas with scholars and engineers from various parts of the world (the United States, China, Taiwan, India, and Germany) including active members of the United States program, “Failure-Resistant Systems (FRS)” sponsored by the National Science Foundation (NSF) and the Semiconductor Research Corporation (SRC), and the German program, “SPP1500 Dependable Embedded Systems,” sponsored by the Deutsche Forschungsgemeinschaft (DFG). I only wish we had closer interactions between these programs—FRS (2013–present), SPP1500 (2012–2016), and DVLSI (2007–2015)—with more overlapping elements.

My heartfelt thanks go to the following gentlemen: Tohru Kikuno, Atsushi Hasegawa, Masatoshi Ishikawa, Yoshio Masubuchi, Naoki Nishi, Koki Noguchi, Tadayuki Takahashi, Koichiro Takayama, and Kazuo Yano, all of whom are advisory members of the DVLSI program. I would like to thank JST and all its management and staff members for their encouraging and patient support for this program: Kazunori Tsujimoto, Shinobu Masubuchi, Daichi Terashita, Toshiaki Ikoma, Michiharu Nakamura, and the late Koichi Kitazawa, to name but a few.

I would like to thank Toyota Motors Corporation for kindly providing a chart describing the power train of a hybrid vehicle to be used in this book as an illustration, and the Xilinx Company for kindly agreeing that the use of a chart showing an FPGA (Field Programmable Gate Array) coupled with an ARM (ARM is a company that provides an embedded processor architecture) processor, could be included in this book.

I am also thankful to Hikaru Shimura of the Rigaku Corporation who generously allowed me to spend some of my time on the job overseeing this program, and to his technical staff members, of which Kenji Wakasaya was one, who kindly shared their experience in systems design. I am thankful to Binu Thomas of Quest Global, a partner of Rigaku’s in software development, for sharing his thoughts about verification and testing. I cannot thank my colleagues enough at Hitachi Ltd. for stimulating and helping me form ideas about what systems design is. Just to single out a person from the many I worked with, Masayoshih Tsutsumi was an engineer–philosopher who shared his great insight into how to guide thoughts in designing a product, which I have tried to reproduce, only to a very limited extent, in Chap. 2. My last thanks go to Shigeru Oho and Koki Noguchi for thoroughly reviewing the first two chapters and suggesting many important and necessary corrections.

Tokyo, Japan Shojiro Asai
March 2017

Contents

Part I Introduction

Part I
Introduction

Chapter 1
Challenges and Opportunities in VLSI for Systems Dependability

Shojiro Asai

Abstract This chapter describes the scope, activities, and results of a research program entitled, “Fundamental Technologies for Dependable VLSI Systems (DVLSI for short henceforth)” which began in 2007 and ended in 2015. The program, funded by JST (Japan Science and Technology Agency) under the CREST (Core Research of Evolutional Science and Technology) initiative, consisted of 11 projects and addressed problems in dependability of electronic systems from various different angles. VLSI is a complex system in its own right and involves a number of potential hazards that arise internally from aging in elements or those that can be caused by external disturbances such as ionizing radiations. Coping with these phenomena has always been a challenge in semiconductor engineering and this program as well. Fabrics (physical structures) robust against threats, bit-error correction methods, and logic-level redundancies have been extensively studied. To go further, challenges of 3-D integration, chip-area (on-chip and across-chip) network, and wireless packaging have been taken on. Exploiting the potential of VLSI in solving problems in systems that call for hard real-time response and/or synchronicity as in robotics and wireless telecommunications has been addressed as new great opportunities for VLSIs. Advanced ways of verification and test for VLSIs have also been dealt with. We will begin this chapter by going over the background of VLSIs for electronic systems and reviewing the necessity of dependability. We will then describe how this multi-project program of CREST DVLSI was formed and conducted. The university-industry collaboration in goal-oriented management efforts is highlighted as essential. A summary of results obtained follows.

Keywords Dependable system · VLSI · CREST · University-industry collaboration · Goal-oriented management

S. Asai (✉)
Rigaku Corporation, Tokyo, Japan
e-mail: asai@rigaku.co.jp

S. Asai (ed.), *VLSI Design and Test for Systems Dependability*,
https://doi.org/10.1007/978-4-431-56594-9_1

1.1 VLSI in Electronic Systems and Their Dependability

1.1.1 Pervasiveness of VLSI

The VLSI (Very Large Scale Integration of semiconductor circuits) and software (computer program) are two great enablers of electronic systems, a synonym to modern-day convenience. Personal computers and cell phones, almost indispensable personal items these days, are good examples. Figure 1.1 shows a simplified block diagram of a personal computer. It is seen that VLSI chips such as a microprocessor [1–3], and semiconductor memories [4], e.g., RAM (Random Access Memory) and NVM (Nonvolatile Memory), are the most important parts among others. Important peripheral devices such as HDD (Hard Disk Drive), communications control, and monitoring display have built-in processors as well. The PC (Personal Computer) is a typical general-purpose computer where users run various different application programs. High-performance (Super-) computers are at the highest end of general-purpose computers.

Figure 1.2 depicts the power train (power generation and transmission) in a hybrid electric-gasoline-engine vehicle which uses a number of ECUs (electronic control units). Each ECU has at least one microprocessor "embedded" and is thus an electronic system in its own right. The automobile these days is a typical embodiment of embedded computing [5]. A high-end car these days uses as many

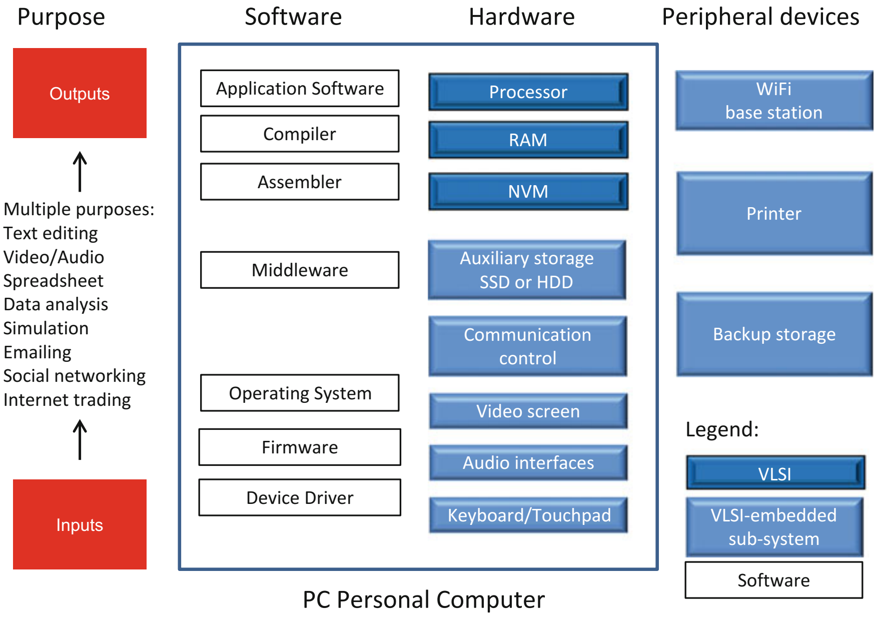


Fig. 1.1 A simplified block diagram of a PC (Personal Computer) to illustrate the use of VLSIs as key components

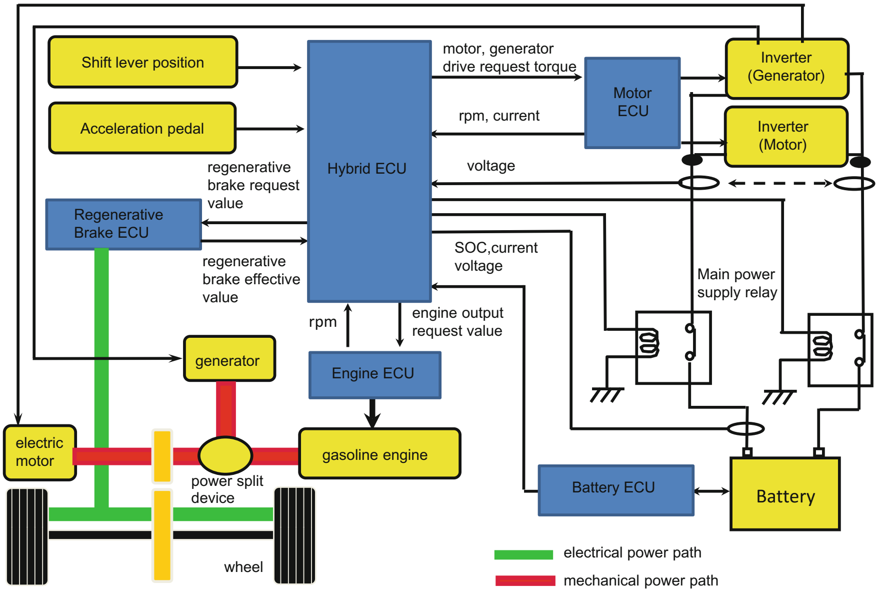


Fig. 1.2 Electronic control units in the power train of a hybrid electric and gasoline-engine vehicle to illustrate use of VLSI-powered ECUs (Electronic Control Units). Courtesy, Toyota Motor Corporation

as 80 microprocessors for various subsystem and module-level control [6]. Actually, the VLSI has provided the biggest momentum to improve the quality and reduce the cost of products or services of electronic systems. This is true with most of complex systems products, which may be mechanical (stationary or mobile), aerodynamic, electrical, electromechanical, electromagnetic, optical, electro-optical, or chemical. Because these systems generally need control for precision and throughput, which is hard to achieve were it not for the VLSI and program control. Automobiles, aircrafts, rockets, robots, chemical plants, utilities, medical devices, ATMs (Automatic Teller Machines), data storages, and agricultural plants of today are good examples of computer-embedded systems. They would not have existed without the VLSI as their key components for smart control. It is almost funny that we are accustomed to call these computer-embedded electronic systems "dedicated systems." Although the purpose of the system is certainly "dedicated", for example, to automotive control, computers (microprocessors) have actually found far more general and voluminous applications in embedded control than in "general-purpose" computing by PCs and HPCs (High-Performance Computers).

The more the benefits are drawn out of these systems and the more extensive their uses become over the population, the more heavily the human life depends on them. It is necessary therefore to see to it that these systems are available whenever they are needed. Because the VLSI is at the core of these systems as the workhorse, it is necessary to understand what the VLSI does in electronic systems, what would happen if it fails to function as expected, what could be done to prevent serious failures from happening, and what we can innovate further in realizing more dependable systems technologies. Actually, these are the subjects discussed in this book. (Let us call the systems that use VLSIs as key components "electronic systems" hereafter. The term VLSI systems may be used interchangeably.)

1.1.2 Necessity of Dependability

Dependability is never a single quality merit of a system. Central to the merit is rather the "performance" or "performance/cost," in other words, "better fulfillment of the primary purpose" it is intended for. Table 1.1 shows the factors that would affect the decision a user would make in the procurement of a product or service offered in the marketplace. During early stages of market introduction, cost and or performance may be the most influential factors, but as a product category and its market mature, increased attention is paid to dependability for increased social and economic implications, and this is true now with all kinds of electronic systems. These days, dependability of an electronic system is an interest shared among all those concerned: producers, users, and service providers alike.

The requirements for dependability have been discussed in and among various government regulatory agencies, global/regional/national standards bodies, mission-oriented agencies, industrial associations, and academic societies. Figure 1.3 shows such organizations along with the documents they have published. It will be

Table 1.1 Factors affecting the decision-making for procurement of a product or service

decision-affecting factors		index
cost (total cost of ownership)	cost of acquisition	initial price (plus NRE when applies)
	operational cost	cost of consumables
		cost of power, water, etc.
		maintenance/service cost
	cost of diposal	disposal of consumables
		cost of retirement
performance	speed (throughput)	product units/hour, GBPS, MIPS, etc.
	accuracy, resolution	accuracy/resolution (in units of time, length, etc.), measurement repeatability, etc.
	ease of use	unquantifiable
dependability	availability	MTTF, MTBF, regular maintenance/service time, network connentivity, etc.
	maintainability	MTTR
	maintenance support	unquantifiable (availability of service, parts, help desk, etc.)
	safety and security	unquantifiable (functional safety, tamper resistance, availability of encryption, etc.)
	integrity	unquantifiable (tamper resistance, accountability, etc.)

NRE: non-recurrent engineering, MIPS: Million Instructions Per Second, GBPS: Giga Bits Per Second,
MTTF*: Mean Time To Failure, MTBF*: Mean Time Between Failures, MTTR*: Mean Time To Repair
*: Statistical quantities available only after operation for a certain length of time

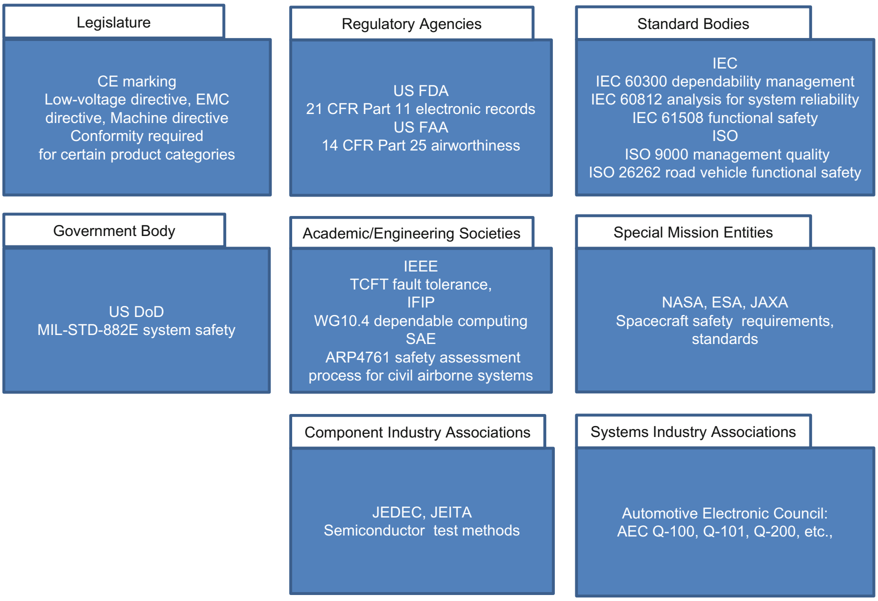

Legislature
CE marking
Low-voltage directive, EMC directive, Machine directive
Conformity required for certain product categories
Regulatory Agencies
US FDA
21 CFR Part 11 electronic records
US FAA
14 CFR Part 25 airworthiness
Standard Bodies
IEC
IEC 60300 dependability management
IEC 60812 analysis for system reliability
IEC 61508 functional safety
ISO
ISO 9000 management quality
ISO 26262 road vehicle functional safety
Government Body
US DoD
MIL-STD-882E system safety
Academic/Engineering Societies
IEEE
TCFT fault tolerance,
IFIP
WG10.4 dependable computing
SAE
ARP4761 safety assessment process for civil airborne systems
Special Mission Entities
NASA, ESA, JAXA
Spacecraft safety requirements, standards
Component Industry Associations
JEDEC, JEITA
Semiconductor test methods
Systems Industry Associations
Automotive Electronic Council:
AEC Q-100, Q-101, Q-200, etc.,

Fig. 1.3 Organizations engaged in regulations, standards, and guidelines for dependability as part of product quality

relevant to refer in particular to IEC 60300 [7] for dependability management, IEC 61508 [8] for functional safety in industrial process measurement, control and automation, and ISO 26262 [9] for the functional safety for road vehicles, since these will be frequently cited throughout this book.

1.2 Background and Motivation for the Program

1.2.1 What VLSI Has Brought About—A Historical Perspective

The VLSI has contributed to the progress in electronic systems in so many ways, which may be summarized as follows.

#1 Great number of devices integrated on a chip

As first observed by Gordon Moore and later named as Moore's Law that has held up until very recently, the number of transistors integrated on a chip of VLSI silicon has doubled every 18 months [10]. It is interesting to review the progress that the VLSI made following what Gordon Moore predicted [11]. I will not go into that here, however, since there already are abundant references available for this history

[12]. It is worthwhile to note here, however, that there is a very solid theoretical background to the scaling down the sizes (other physical parameters and operating voltages as well) of the transistor, the most basic element of VLSI that has underlain its progress [13]. The number of transistors in a microprocessor has actually increased from the mere 2300 of Intel 4004 in 1971 to the billions today [14]. The same is true with memory chips. In no other technologies has it ever been possible to integrate uniformly performing, reliable components the way VLSI has enabled, which has provided the most powerful driving force for the complex electronic systems [15].

#2 Variety of circuit functions realized on silicon

The VLSI rapidly evolved from the early days of chips with a few logic gates into a variety of circuit functions covering arithmetic, logic, memory, analog, and more. Memories include SRAM (Static Random Access Memory), DRAM (Dynamic Random Access Memory), ROM (Read-Only Memory), EPROM (Electrically Programmable ROM), EEPROM (Electrically Erasable and Programmable ROM), and Flash Memory [4]. The analog and analog–digital tier of the silicon circuitry is capable of small-signal and high-power amplification, and analog-to-digital and digital-to-analog conversion [16]. A very important type of products of VLSI called FPGA (Field Programmable Gate Array) emerged during the course of the development [17, 18]. Image sensors with billions of pixels have been used in cameras [19]. Micro-Electro-Mechanical (MEMS) is another direction the VLSI has taken to develop [20].

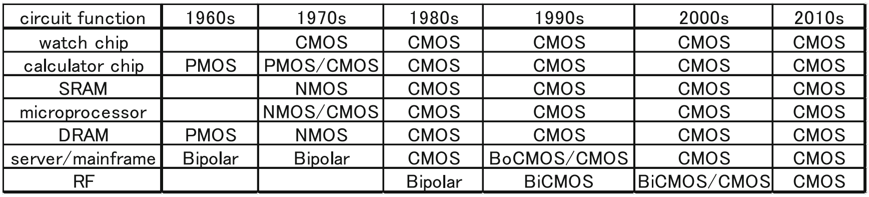
#3 Single-chip implementation of multiple circuit functions

Almost all the circuit functions described in #2 have actually been integrated in chips by now in the form of microprocessors used for personal computers, mobile communication devices, and computer-embedded electric, electronic, and software-controlled systems. The CMOS (Complementary Metal-Oxide Semiconductor), which emerged originally as low-power but low-speed integrated circuit technology, has since been exploited fully to realize all of the logic, memory, and coupled analog–digital functions, taking over the roles played by ECL, TTL and NMOS, and Bi-CMOS (hybrid bipolar and CMOS), realizing the highest density of integration by virtue of low power (virtually no power consumption when idle) inherent in that technology. This history is very well captured in Table 1.2 compiled by Makimoto et al. [21].

#4 Application functions and accelerated processing

During the course of evolution in VLSI, what is now called the ASIC (Application-Specific Integrated Circuit) [22] has evolved. The ASIC contrasts to general-purpose integrated circuits such as standard memories and microprocessors. ASICs with specific system- or subsystem-level functions have often been developed in-house at a systems house, or at a semiconductor house to the order of a systems house, for signal processing in telecom, image-processing applications (routers and switches, data compression, data correction, display control), for example.

Table 1.2 Evolution of CMOS to encompass broader applications over time. CMOS has gradually outperformed other circuit technologies and enabled the integration of various different circuit functions on a single chip of VLSI [21]



circuit function	1960s	1970s	1980s	1990s	2000s	2010s
watch chip		CMOS	CMOS	CMOS	CMOS	CMOS
calculator chip	PMOS	PMOS/CMOS	CMOS	CMOS	CMOS	CMOS
SRAM		NMOS	CMOS	CMOS	CMOS	CMOS
microprocessor		NMOS/CMOS	CMOS	CMOS	CMOS	CMOS
DRAM	PMOS	NMOS	CMOS	CMOS	CMOS	CMOS
server/mainframe	Bipolar	Bipolar	CMOS	BoCMOS/CMOS	CMOS	CMOS
RF			Bipolar	BiCMOS	BiCMOS/CMOS	CMOS

Some of these application functions that were originally developed for ASICS such as efficient display control, encryption, and decryption for secure data transmission have been integrated in a general-purpose microprocessor. There are other types of VLSIs that evolved into high-performance, dedicated computation to complement microprocessors. In this category are DSP (Digital Signal Processor) [23] and GPU (Graphic Processing Unit) [24].

#5 Abundance of on-chip resource

The availability of an abundance of circuit resource has been exploited to introduce fault tolerance to the VLSI. The use of redundant bits for error correction was first used in DRAMs and SRAMs, easily accommodating a few defective bits to the effect of salvaging partially defective chips and thus drastically lowering the average memory prices. The introduction of error correction dramatically improved the tolerance of semiconductor memories against radiation-induced soft errors. (Please refer to paragraphs below). The fault-tolerant technology is used in flash memories in a more sophisticated fashion to optimize the memory retention and write–erase endurance. Error-correcting codes and encoding techniques are used to avoid physical interference of charges in the neighboring cells [25, 26]. Recent multiple-processor chips as well as FPGAs are capable of performing redundant concurrent calculation and then having a vote for the correct result to be robust against faults in a part of the chip. Two of most advanced VLSI architectures are shown in Figs. 1.4 and 1.5 for illustrative purposes. Figure 1.4 shows a powerful integration of a multi-core processor and an FPGA which includes security features such as AES (Advanced Encryption Standard), SHA (Secure Hash Algorithm), and RSA (Rivest–Shamir–Aldeman encryption) [27]. Figure 1.5 is a microprocessor for automotive applications. Security features to support ISO 26262 have been integrated [28].

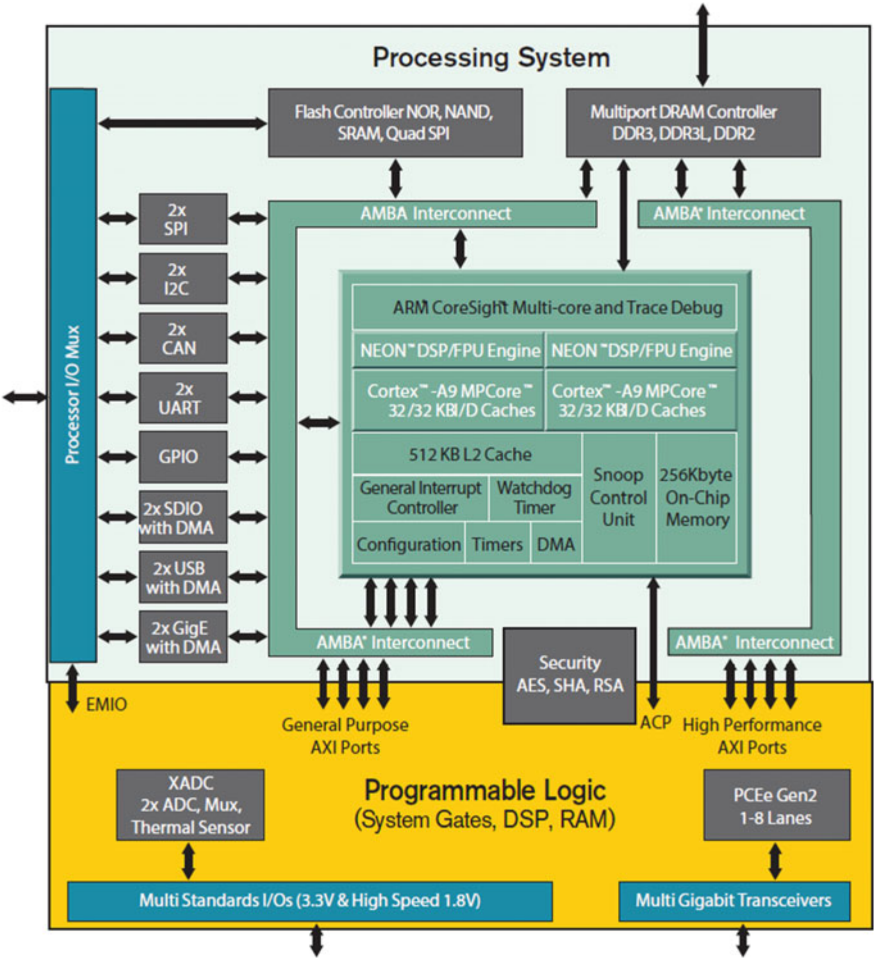

Processing System
Flash Controller NOR, NAND, SRAM, Quad SPI
Multiport DRAM Controller DDR3, DDR3L, DDR2
AMBA Interconnect
AMBA Interconnect
2x SPI
2x I2C
2x CAN
2x UART
GPIO
2x SDIO with DMA
2x USB with DMA
2x GigE with DMA
Processor I/O Mux
ARM CoreSight Multi-core and Trace Debug
NEON DSP/FPU Engine
NEON DSP/FPU Engine
Cortex-A9 MPCore 32/32 KB I/D Caches
Cortex-A9 MPCore 32/32 KB I/D Caches
512 KB L2 Cache
General Interrupt Controller
Watchdog Timer
Configuration
Timers
DMA
Snoop Control Unit
256Kbyte On-Chip Memory
AMBA Interconnect
Security AES, SHA, RSA
AMBA Interconnect
EMIO
General Purpose AXI Ports
ACP
High Performance AXI Ports
XADC 2x ADC, Mux, Thermal Sensor
Programmable Logic (System Gates, DSP, RAM)
PCEe Gen2 1-8 Lanes
Multi Standards I/Os (3.3V & High Speed 1.8V)
Multi Gigabit Transceivers

Fig. 1.4 A functional block diagram of an integration of a multi-core processor and an FPGA. Courtesy, Xilinx Corporation

#6 Stable manufacturing and sourcing

The remarkable progress in the precision manufacturing technology for semiconductors and its rapid proliferation amongst players throughout the world in a competing as well as collaborating business environment has brought about high quality and stability in the sourcing of the VLSI, contributing tremendously to the build, maintenance, and maintenance support of the electric and electronic systems in terms of cost and availability. This has allowed systems houses to use multiple sources to secure procurement of key components.

CPU	7-Stage 2-issue Pipeline, FPU	2.8DMIPS/MHz, 320MHz
Instruction Cache	8KB, 4WAY	Optimized for low power
Local RAM	64KB	128bits low latency access, Register Push/Pop instruction
Global RAM	192KB	64bits access
Safety	ECC, Parity, MPU, Access Guard	ISO26262 support

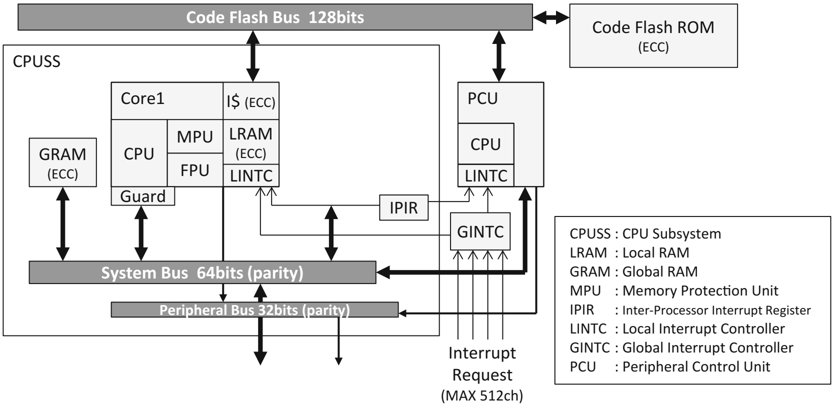

Code Flash Bus 128bits
Code Flash ROM
(ECC)
CPUSS
Core1
I$ (ECC)
CPU
MPU
FPU
LRAM
(ECC)
LINTC
Guard
GRAM
(ECC)
PCU
CPU
LINTC
IPIR
GINTC
System Bus 64bits (parity)
Peripheral Bus 32bits (parity)
Interrupt
Request
(MAX 512ch)
CPUSS : CPU Subsystem
LRAM : Local RAM
GRAM : Global RAM
MPU : Memory Protection Unit
IPIR : Inter-Processor Interrupt Register
LINTC : Local Interrupt Controller
GINTC : Global Interrupt Controller
PCU : Peripheral Control Unit

Fig. 1.5 A functional block diagram of a multiple-core microprocessor for automotive applications. Various safety and security features such as redundancy and access guard are integrated to support ISO 26262 for road vehicles. Courtesy, Renesas Electronics

#7 Distribution of reusable IPs

It has been made possible by the development of commercial practice in the semiconductor industry to distribute the rights to use the whole or parts of the design of an existing VLSI. Commerce of rights to use a semiconductor design (IP, Intellectual Property as it is called) that has proven to work has enabled reuse and helped realize more complicated chips in shorter time and with less cost of development. The last two items (#6 and #7) are a socioeconomic rather than technical phenomenon, which is worth noticing here discussing the impact of VLSI. Figure 1.5 in which a microprocessor IP and an FPGA IP are integrated is a good example.

The progress in VLSI technologies described above has been the contributors to progress in electronic systems, providing ever higher performance at ever lower prices, as well as dependability in compact, integral packages.

1.3 Threats and Opportunities for the VLSI Systems

Great many ingenuities and tremendous efforts in engineering and associated sciences have been put in to accomplish the colossal tower of VLSI technology as it stands, which has impacted electronic systems with so much socioeconomic momentum.

1.3.1 Threats Arising from Miniaturization

Suppose the precision printing and other manufacturing technologies continue to progress making the transistor and other device features even smaller, the VLSI engineering will be left with a pile of problems as follows to solve. Engineering has negotiated these problems of generic nature so far, but they will be much tougher to cope with in the future.

#1 Ionizing radiations and electromagnetic interference

There are the issues of various radiations in the environment that causes errors in the VLSI circuits. If a neutron from the outer space hits a VLSI chip, the electronic charges resulting from ionization in the semiconductor could cause errors in the VLSI circuits that could give rise to a system-level failure. This problem will be dealt with in Chap. 3 of this book. Electromagnetic interference is another persistent radiation issue. The voltage change induced by the alternating electromagnetic field generated off-chip (e.g., by an automotive engine igniter) or fed through the power line are a hazard that needs continued attention in the design of the VLSI. This problem will be handled in Chap. 4.

#2 Variations and degradation in device characteristics

The variation in sizes and other parameters of the transistor, which become more pronounced as it is scaled down, leads to variation in transistor characteristics, which in turn could cause deviation in delay times in the circuits. The latter could result in a system failure. This problem is addressed in Chap. 5. There are also multiple, persistent mechanisms that cause degradation in the characteristics of transistors and other components in VLSI over time and/or under the stress of operating voltage/current, temperature, etc. The time-dependent degradation mechanisms are the topic of Chap. 6.

1.3.2 Threats Arising from Scale and Complexity

Another aspect of problems in VLSI design for dependability is complexity-increasing scale and integration of different functions. A system consists of subsystems and modules with various different characteristics: processor, SRAM, flash memory, analog–digital components in hardware; and commands and sequences in software; some being offered as existing, already-proven parts, and some being newly developed and left to be proven. The complexity arises from the interactions of various objects such as these, consuming the time and human resource to make sure that they work in coordination in practical use cases.

#1 Connectivity

Interconnects and communications between subsystems are sources of system problems. Users of wireless telecommunications often experience loss of connection. Importance of securing minimal connectivity even under disaster conditions has been pointed out. It will be a challenge to mitigate or perhaps eliminate this problem in a wireless system with VLSIs with new functionalities. This is the topic of Chap. 7. Chapter 8 addresses connectivity in electronic systems and handles the challenges of wireless signal interconnects and wireless power supply for VLSI or system-level packaging.

#2 Responsiveness

A response within a certain specified length of time is often required in real-time systems. A soft real-time control is such that a late response is permissible to a certain extent as in the case of ATM as the user can wait for a second or two. A hard real-time control is such that this requirement is critical as in the case of robotics or automatic drive assistance. Meeting with the hard real-time response requirements in robotic applications and assuring synchronicity over the system-to-system handover in wireless applications are examples. This issue is dealt with in Chap. 9.

#3 Malicious attacks

Electronic systems are often the target of malicious attack of hackers who attempt to steal information, disrupt operation, etc., which poses a threat to systems security and reliability. Consideration for security and safety is adding more tasks for the VLSI systems design recently. This issue, which is becoming one of the greatest social concerns, is handled in Chap. 10.

#4 Design errors and test coverage

Complexity has to be dealt with in designing a VLSI system, but it tasks the process of verification, test, and validation of the systems as well. The mere number such as billions of transistors and ten million lines of source codes (operating systems alone) creates complexity, because experience tells that humans make an error in every 100 line of codes. Making certain that the design of an electronic system reflects the requirements specification has increasingly become a challenging task as complexity increases. Test coverage is therefore another important topic, which is undertaken in Chap. 11.

#5 Unknown threats and provisions

No design is perfect, particularly in light of changing threats, changing uses and changing use environments. Requirements specification, even though it will be prepared with utmost care may not be perfect. Unknown threats and provisions are discussed in Chap. 12.

1.3.3 Opportunities: Changing Markets and Increased Demands for Systems Dependability

Changes in the market environment that happened during the past 10 years are opening up new opportunities for VLSIs. First of all, certain types of electronic system products are receiving increasing requirements in privacy. Personal information stored in PCs, cell phones, or credit cards are prone to criminal plots and malicious attacks. Safety is an utmost requirement in robots in assistance of the handicapped or for hazardous mission in hostile environment. The same is true with automatic driving or drive assistance in road vehicles. Conformity to new safety standards such as described in Sect. 1.1.2 is now a must for the electronic systems design. These changes in markets and growing demands for safety and security pose great opportunities for VLSIs.

1.3.4 A Summary of Objectives

The threats and opportunities described in this section are mapped out in Fig. 1.6, which shows origins of threats to the dependability of electronic systems in terms of generation of faults and their escalation. Origins of faults are manifold. For example, noise charges generated in the semiconductor (bottom left) by a neutron of cosmic origin may lead to flipping in a logic or memory state, which may give rise to a failure of the system level, resulting in consequences with different levels of severity. Tampering of VLSI may also result in damages of varied severity. Bugs in circuit, logic, or program design could also cause failures to similar effects. Technological challenges therefore lie in the mitigation and containment of the threat by the design and test of VLSI. Opportunities for VLSI lie in realizing new functional features which could facilitate integration and enhance dependability of increasingly more complex systems.

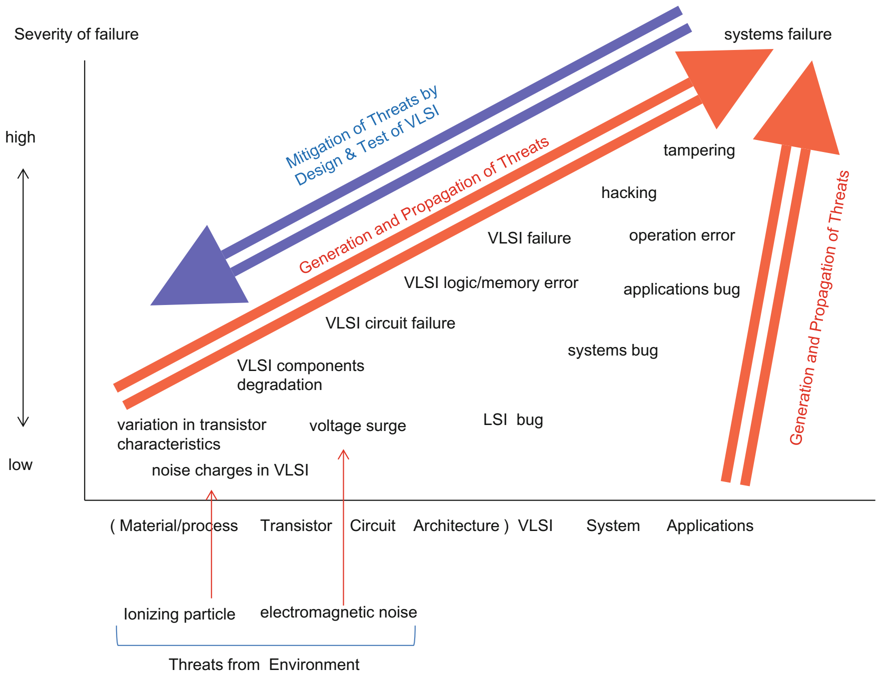


Fig. 1.6 Propagation and containment of threats that could cause systems failure vertical positions of events or bugs are relative and arbitrary

1.4 The DVLSI Program

1.4.1 Vision, Scope, and Mission Statement

From what has been discussed in Sect. 1.3, we now arrive at a vision, scope, and mission statement for the DVLSI Program as follows [29]:

- To work on technologies that would help contain the threats against dependability within VLSI.
  New designs for dependability in physical, circuit, logic, and architectural aspects of VLSI will be explored. New methods of verification and test will be pursued as well to complement from a different angle. The VLSI, which has proven to work as most integral, most dependable parts of systems, needs further development to further improve dependability.
- To come up with ideas of new functionalities for VLSI which contribute to enhancing dependability at the system level.

Systems in their most advanced form today as those used in electronic commerce, public telecommunications, management, robots, sensor networks, or so-called Internet of Things place challenges as described in Sect. 1.3.

- To provide a method for measuring the dependability of systems.

1.4.2 Program Start and Project Selection

The DVLSI program started with the appointment of the author to Research Supervisor in March 2007. In an arrangement customary to the CREST programs, we had the privilege of having distinguished advisors [30] from industry and academia shown in Table 1.3 join the Program Management to assist the Research Supervisor.

The first RFP (Request For Proposals) was issued from JST in March 2007, the deadlines for submission set in May. The selection from the submitted proposals was conducted by the VLSI Program Management (Research Supervisor and Advisors), considering the relevance of the proposal from the following perspectives:

- If the proposal has captured essential problem(s) being experienced and/or overarching in practical VLSI design for dependability;
- What original and distinctively competitive ideas are presented to solve the problem(s) raised;
- If a target is set at a challengeable level and described as clearly and hopefully as quantitatively as possible with respect to the state of the art and on-going competing efforts throughout the world;

Table 1.3 DVLSI Program Advisors from industry and academia

Adviser	Affiliation	Term Engaged	
		Start	End
Masatoshi Ishikawa	The University of Tokyo	Oct. 2007	Mar. 2015
Tohru Kikuno	Osaka Gakuin University	Oct. 2007	Mar. 2015
Tadayuki Takahashi	Japan Aerospace Exploration Agency	Oct. 2007	Mar. 2015
Koichiro Takayama	Fujitsu Ltd.	Oct. 2012	Mar. 2015
Naoki Nishi	NEC Corp.	Oct. 2007	Mar. 2015
Koki Noguchi	Renesas Semiconductor	Oct. 2007	Mar. 2009
Atsushi Hasegawa	Renesas Electronics Corp.	Oct. 2009	Mar. 2015
Yoshio Masubuchi	Toshiba Corp.	Oct. 2007	Mar. 2015
Kazuo Yano	Hitachi Ltd.	Oct. 2007	Mar. 2015

Table 1.4 Project subjects and PIs (Principal Investigators) in the DVLSI program

Principal Investigator	Position	Affiliation	PJ Term		PJ Subject
			Start	End	
Hidetoshi Onodera	Professor	Kyoto University	Oct. 2007	Mar. 2014	Dependable VLSI Platform Using Robust Fabrics
Shuichi Sakai	Professor	Univ. Tokyo	Oct. 2007	Mar. 2013	Ultra Dependable VLSI by Collaboration of Formal Verifications and Architectural Technologies
Kazuo Tsubouchi	Professor	Tohoku University	Oct. 2007	Mar. 2015	Development of Dependable Wireless System and Device
Hiroto Yasuura	Professor	Kyushu University	Oct. 2007	Mar. 2013	Modeling, Detection, Correction and Recovery Techniques for Unified Dependable Design
Seiji Kajihara	Professor	Kyushu Institute of Technology	Oct. 2008	Mar. 2014	Circuit and System Mechanisms for High Field Reliability
Masahiko Yoshimoto	Professor	Kobe University	Oct. 2008	Mar. 2014	Dependable SRAM Techniques for Highly Reliable VLSI System
Tomohiro Yoneda	Professor	National Institute of Informatics	Oct. 2008	Mar. 2014	Development of Dependable Network-on-Chip Platform
Takeshi Fujino	Professor	Ritsumeikan University	Oct. 2009	Mar. 2015	The Design and Evaluation Methodology of Dependable VLSI for Tamper Resistance
Mitsumasa Koyanagi	Professor	Tohoku University	Oct. 2009	Mar. 2014	Three-Dimensional VLSI System with Self-Restoration Function
Ken Takeuchi	Professor	Chuo University	Oct. 2009	Mar. 2015	Dependable Wireless Solid-State Drive (SSD)
Nobuyuki Yamasaki	Professor	Keio University	Oct. 2009	Mar. 2015	Fundamental Technology on Dependable SoC and SiP for Embedded Real-Time Systems

- What the likelihood of success in terms of PoC (Proof of Concept) demonstration and expected successive industrial implementation is.

The selection process took a few months after the submission of proposals and was completed by August 2007. The same process of RFP, proposal submission, and project selection was repeated in 2008 and 2009 to finalize the selection. The eleven projects led by the Principal Investigators were awarded with the JST CREST funds over the 3 years between 2007 and 2009 as shown in Table 1.4 [31]. Table 1.5 is the list of Co-Investigators.

During the 3 years of selection process, it was fortunate to have the projects in the DVLSI Program cover key aspects of the problem of dependability rather comprehensively if not exhaustively. The projects address the aspects of functionality, design/verification tools, and test tools in most of the hierarchical layers from the physics, circuit to architecture, as shown in Fig. 1.7. The vertical axis of Fig. 1.7 is the systems hierarchy from the physical layer at the bottom to application at the top. On the horizontal axis are the segments of research products ranging from the design tools, test tools, and concepts in chips/circuits up to proposed solutions for dependable systems. Figure 1.8 is another roughly sketched project portfolio of the Program compiled from the project documents positioning the projects relative to the applications areas envisioned such as aerospace, plant control, transportation, automobiles, robots, information, telecommunications, medical, finance, and consumer appliances.

1.4.3 Program Management

In view of the object of the CREST framework, in which technology innovations as a result of collaborative efforts within project teams are envisioned, and with

Table 1.5 Project teams consisting of the Principal Investigators and Co-Investigators

Principal Investigator	Co-Investigator	Affiliation	Term Engaged	
			Start	End
Hidetoshi Onodera (Kyoto University)	Takao Onoe	Osaka University	Oct. 2007	Mar. 2014
	Hiroyuki Kanbara	Advanced Scientific Technology & Management Reserch Institute of Kyoto	Oct. 2007	Mar. 2014
	Kazutoshi Kobayashi	Kyoto Institute of Technology	Apr. 2009	Mar. 2013
	Hajime Shimada	Nagoya University	Apr. 2009	Mar. 2013
	Yukio Mitsuyama	Kochi University of Technology	Apr. 2011	Mar. 2014
	Kazutoshi Wakabayashi	NEC Corp.	Apr. 2011	Mar. 2014
	Hiroyuki Ochi	Ritsumeikan University	Apr. 2013	Mar. 2014
Shuichi Sakai (The University of Tokyo)	Masahiro Fujita	The University of Tokyo	Oct. 2007	Mar. 2013
	Kenji Kise	Tokyo Institute of Technology	Oct. 2007	Mar. 2013
	Kazutoshi Wakabayashi	NEC Corp.	Apr. 2010	Mar. 2013
Kazuo Tsubouchi (Tohoku University)	Akira Matsuzawa	Tokyo Institute of Technology	Oct. 2007	Mar. 2015
	Makoto Iwata	Kyoto Institute of Technology	Oct. 2007	Mar. 2015
	Minoru Fujishima	Hiroshima University	Oct. 2007	Mar. 2015
	Hiroshi Fukumoto	Mitsubishi Electric Corp.	Oct. 2007	Mar. 2015
	Hiroshi Oguma	Toyama National College of Technology	Apr. 2012	Mar. 2015
Hiroto Yasuura (Kyusyu University)	Toshinori Sato	Fukuoka University	Oct. 2007	Mar. 2013
	Yusuke Matsunaga	Kyusyu University	Oct. 2007	Mar. 2013
Seiji Kajihara (Kyushu Institute of Technology)	Michiko Inoue	Nara Institute of Science and Technology	Oct. 2008	Mar. 2014
	Satoshi Otake	Oita University	Oct. 2008	Mar. 2014
	Yukiya Miura	Tokyo Metropolitan University	Oct. 2008	Mar. 2014
Masahiko Yoshimoto (Kobe University)	Makoto Nagata	Kobe University	Oct. 2008	Mar. 2014
	Koji Nii	Renesas Electronics Corp.	Oct. 2008	Mar. 2014
	Yasuo Sugure	Hitachi Ltd.	Oct. 2008	Mar. 2014
	Shigeru Oho	Nippon Institute of Technology	Oct. 2008	Mar. 2014
Tomohiro Yoneda (The National Institute of Informatics)	Masashi Imai	Hirosaki University	Oct. 2008	Mar. 2014
	Takahiro Hanyu	Tohoku University	Oct. 2008	Mar. 2014
	Hiroshi Saito	The University of Aizu	Oct. 2008	Mar. 2014
	Kenji Kise	Tokyo Institute of Technology	Apr. 2012	Mar. 2014
Takeshi Fujino (Ritsumeikan University)	Yohei Hori	Advanced Industrial Science and Technology	Oct. 2009	Mar. 2015
	Masaya Yoshikawa	Meijyo University	Oct. 2009	Mar. 2015
	Daisuke Suzuki	Mitsubishi Electric Corp.	Oct. 2009	Mar. 2015
Mitsumasa Koyanagi (Tohoku University)	Hiroaki Kobayashi	Tohoku University	Oct. 2009	Mar. 2014
	Takafumi Aoki	Tohoku University	Oct. 2009	Mar. 2014
	Toshinori Sueyoshi	Kumamoto University	Oct. 2009	Mar. 2014
	Tadashi Kamada	Denso Co.	Oct. 2009	Mar. 2014
	Makoto Motoyoshi	ZyCube Co.	Oct. 2009	Mar. 2014
Ken Takeuchi (Chuo University)	Tadahiro Kuroda	Keio University	Oct. 2009	Mar. 2015
	Hiroki Ishikuro	Keio University	Oct. 2009	Mar. 2015
Nobuyuki Yamasaki (Keio University)	Masayuki Inaba	The University of Tokyo	Oct. 2009	Mar. 2015
	Kikuo Wada	NEC Corp.	Oct. 2009	Mar. 2015

ever-accelerating advancement in technology and realization in products taking place worldwide, the program management that consisted of the Research Supervisor and the Advisors adopted the following practice to help the projects effectively carry out the mission.

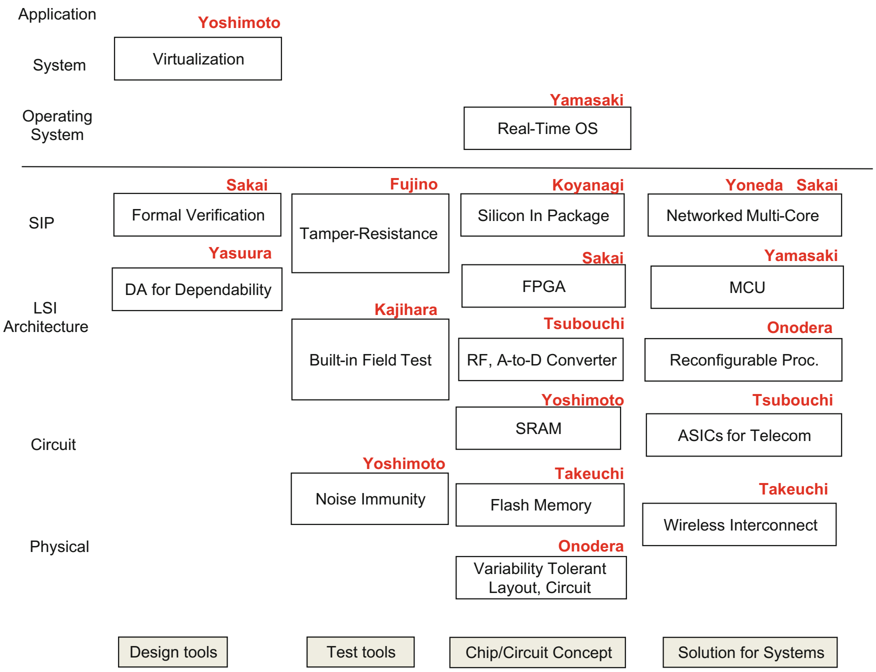


Fig. 1.7 Areas of technologies that the projects in the DVLSI program have covered in a plane defined by systems hierarchy on the vertical axis, from the physical layer to application, and segments of research products on the horizontal axis, from the design tools, test tools, through concepts in chips/circuits and up to proposed solutions for dependable systems. The names of the PIs heading up the projects are indicated in red

- Start out and keep interacting with industry to identify/refine the problems and objectives and have shared interest between the Program and industry if that has not been done enough (Actually this often was the case.),
- Come up with methods to solve the issues that compete favorably among similar efforts worldwide,
- Keep specifying and narrowing down possible applications or opportunities of PoC (Proof of Concept) demonstration,
- Keep interacting with industry to enable research results to get the concept proven and exited to the real world,
- Get the ideas patented and standardized.

The relationship between the Program and the outside world was envisioned as depicted in Fig. 1.9. It was always kept in mind to have a vertical (radial in Fig. 1.9), cross-layer interactions happening exchanging ideas and collaborating with each other. In the innermost core are the teams of Projects in the VLSI Program represented by the PIs (Principal Investigators). The layer surrounding the core is the semiconductor industry and EDA (Electronic Design Automation)

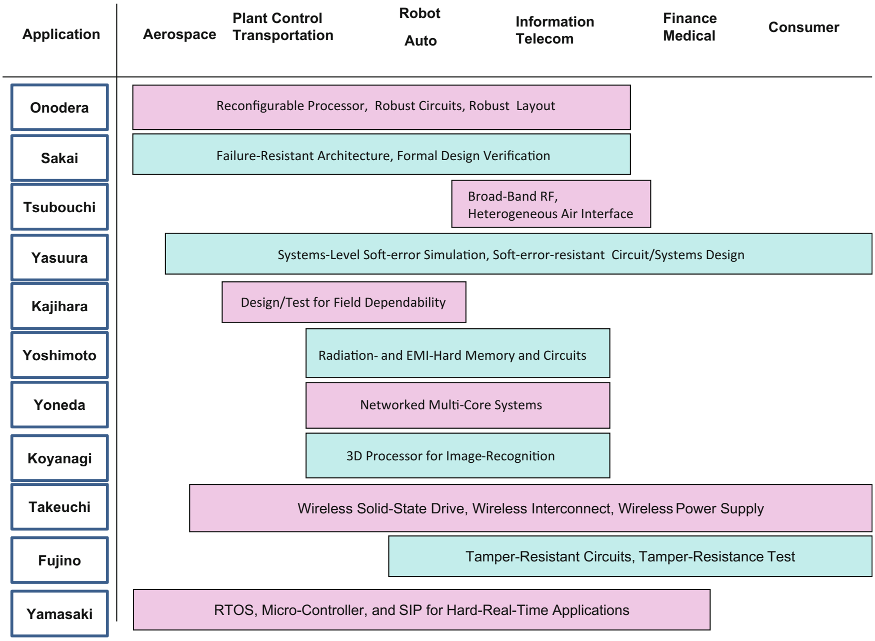

Application
Aerospace
Plant Control
Transportation
Robot
Auto
Information
Telecom
Finance
Medical
Consumer
Onodera
Reconfigurable Processor, Robust Circuits, Robust Layout
Sakai
Failure-Resistant Architecture, Formal Design Verification
Tsubouchi
Broad-Band RF,
Heterogeneous Air Interface
Yasuura
Systems-Level Soft-error Simulation, Soft-error-resistant Circuit/Systems Design
Kajihara
Design/Test for Field Dependability
Yoshimoto
Radiation- and EMI-Hard Memory and Circuits
Yoneda
Networked Multi-Core Systems
Koyanagi
3D Processor for Image-Recognition
Takeuchi
Wireless Solid-State Drive, Wireless Interconnect, Wireless Power Supply
Fujino
Tamper-Resistant Circuits, Tamper-Resistance Test
Yamasaki
RTOS, Micro-Controller, and SIP for Hard-Real-Time Applications

Fig. 1.8 Applications envisioned and approaches taken by the projects in the DVLSI program. The projects with their distinctive research focuses are positioned roughly relative to the broad spectrum of applications that range from aerospace, plant control/utilities/transportation, robot/automobile, information processing, wireless/telecom, finance/medical, to consumer electronics

industry. The semiconductor manufacturer layer is in turn enclosed in the systems industry layer, which is then to provide the products for the service provider industry (and mission-oriented government bodies) in the outer adjacent layer. The outermost space is the consumer or the general public.

The DVLSI Program (center oval) had invited speakers, panelists, and commentators from the external organizations indicated in the outer shells attend the Program meetings to interact with the DVLSI Program. These organizations in effect formed special interest groups shown with elongated ovals in blue with the PIs indicated in red as the primary window of contacts. Some of these interactions have materialized into collaborative technology/product development and implementation. It was intended throughout the Program to have active interactions between the Program and the outside world first to obtain inputs in from, and then to promote exiting the research results back out into, the real world.

People outside the Program were invited from industries and mission-oriented government bodies such as JAXA (Japan Aerospace eXploration Agency) to participate in discussions and collaborate with the teams throughout the term of the Program. It was intended that those invited form groups of special interest as

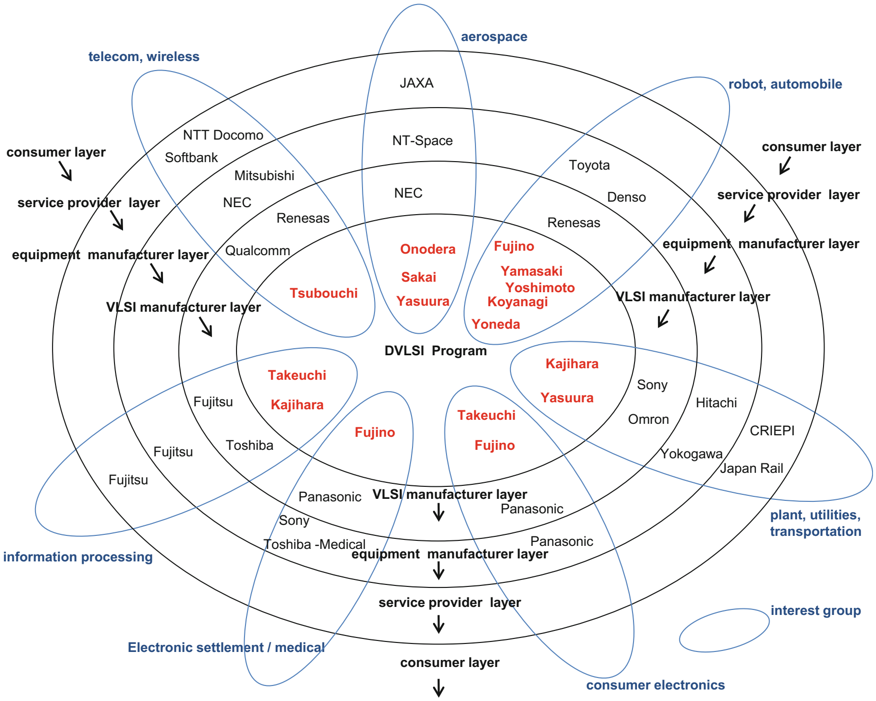


Fig. 1.9 The DVLSI program and its intended cross-layer interactions with external partners

depicted in long ovals as depicted in Fig. 1.9 with project teams of matching research topics.

1.5 A Summary of Results

1.5.1 What Has Been Accomplished

#1 Fundamental study of threats against VLSI dependability and means to mitigate them

There have been many important results obtained in the DVLSI Program out of the fundamental work of studying the nature of “threats” against the dependability of VLSI systems and means to mitigate/cope with them. Detailed account is given by Program researchers in the chapters and sections of Part II in this book, which is entitled, “The VLSI Issues in Systems Dependability.” Much of the fundamental, physical-/circuit-layer research work have been transferred to industry, or being engineered for products.

It is due here to comment that Part II was contributed by many distinguished authors from outside the VLSI Program as well, who participated in the activities of the Program in the interactive way described in Fig. 1.9, and also kindly agreed to write succinct reviews for some of the chapters in PART II to identify the overarching issues and notable engineering efforts that had been made in the relevant area. Readers are referred to the papers in Part II for more elaborate account of the topics.

#2 Systems-/Solution-oriented results

The Program also brought forth several interesting innovative ideas for dependability at the systems and/or solutions layer. These are discussed in chapters of Part III in this book, which is entitled, “Design and Test of VLSI for Systems Dependability.” Many of them have been brought to the stage of demonstration in proof of concept (PoC) experiments, or preliminary implementation by the time of publication of this book. There are continued efforts being made on these proposals to have them implemented in practical systems. A survey conducted by the management of DVLSI Program on its closing in March 2015 said that about a dozen “exit” efforts were being undertaken between the DVLSI project teams and corporations exploiting the ideas and their demonstrations that had resulted from the Program research. It is hoped that we will see them materialized in tangible products and services in the not too distant future.

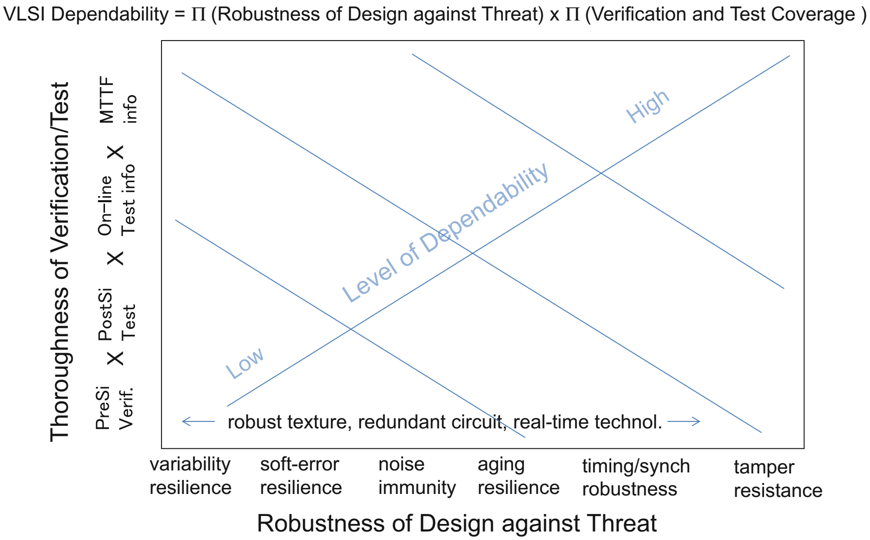

VLSI Dependability = Π (Robustness of Design against Threat) x Π (Verification and Test Coverage)
Thoroughness of Verification/Test
PreSi Verif.
X
PostSi Test
X
On–line Test info
X
MTTF info
High
Level of Dependability
Low
← robust texture, redundant circuit, real-time technol. →
variability resilience
soft-error resilience
noise immunity
aging resilience
timing/synch robustness
tamper resistance
Robustness of Design against Threat

Fig. 1.10 Qualitative levels of VLSI systems measured from the robustness of design against threats and the thoroughness of verification and test

#3 Measurement of dependability

It was on the agenda for the DVLSI team since the beginning of the Program if it will ever be possible to establish quantitative metric(s) of dependability of a VLSI system. This subject was brought up to group discussions from time to time. However, we were not able to come up with a good result for quantitative metrics. Probably closest we have come to this topic is Fig. 1.10, which shows a Cartesian diagram. The horizontal axis is the robustness of the technologies built-in by design and represented by a product of technology "robustness factors" comprising variability resilience, soft-error resilience, noise immunity, aging resilience, timing/synchronicity robustness, and tamper resilience. The vertical axis shows the thoroughness of verification and test, and comprises of pre-silicon verification, post-silicon test, availability of field-test data, and MTTF information. By diagonally sectioning the Cartesian quadrant, it will be possible to categorize a design into a few different levels of dependability, which could be useful for auditing the design practice for dependability.

Same sort of idea may be used for assessing the dependability at the systems level. In fact, it is attempted in Chap. 2 of this book to describe risk analysis and engineering for dependability [6]. For systems, subsystems, or systems components that have been used for a considerable period of time well into their expected full lifetime with a good record of random failure/fault events archived, it would be possible to assess their dependability in terms of MTTF (Mean Time to Failure), MTTR (Mean Time To Repair), or FIT (Failure In Time), and use this knowledge to assess the dependability of the next generation of product.

Not only the above time measures, but other measurable dependability indexes such as rates of packet loss, bit errors, etc., at systems- or subsystems-level will be considered in the dependability. It is essential that archives of failure events and their analyses are built and made accessible for basic engineering researchers as those from the DVLSI Program. It is hoped that future project teams will be able to more effectively address the subject of dependability by having access to knowledge of actual failures and practice of dependability design in industry.

1.5.2 Outreach

Since the DVLSI program started in 2007, a project with objectives quite close to that of DVLSI started in Germany in 2012 [32] and then another in the United States [33]. DVLSI program extended invitation for scholars and engineers from outside Japan as well, including those who participated in the German and US programs to attend meetings of DVLSI, the 2012 JST International Symposium on Dependable VLSI Systems [34] and 2nd International Symposium in Dependable VLSI Systems [35], in particular. The DVLSI program had a number of other events of discussions to promote exchanges of ideas between the DVLSI researchers and people from industry and mission-oriented national organizations, e.g., JAXA, in Japan.

1.5.3 Conclusions

The ideas borne in the DVLSI program to mitigate threats and provide solutions to dependable systems presented in this book are abundant. They may still need more brush up and further engineering, but are believed to form part of foundation for dependable design and test of the VLSI and help improve the dependability of electronic systems of the future.

References

1. J. Hennessy, D. Patterson, *Computer Architecture*, 5th edn. (Morgan Kaufmann, Waltham, 2012)
2. Univ. Wisconsin, "Processors Guide 2012," A good list of commercial microprocessors can be found at this university website. https://kb.wisc.edu/showroom/page.php?id=4927
3. Manufactures are the best sources of information about the working of microprocessors including dependability. Visit the websites of Intel, AMD, ARM, Renesas, etc
4. Memory chip manufacturers are the best sources of information about the working of DRAMs, SRAMs and NVMs including their dependability. Visit the websites of Micron, Cypress, Intel, Toshiba, for example
5. D. Patterson, J. Hennessy, Computer Organization and Design: The Hardware/Software Interface, ARM Edition, Morgan Kaufmann, Cambridge, 2017. A companion piece to Hennessy and Patterson [5] and best textbook available on embedded microprocessors
6. S. Asai, Design and Development of Electronic Systems for Quality and Dependability, Chapter 2 of this book
7. International Standard, IEC 60300, Dependability management. https://webstore.iec.ch/publication/1293, 1294, etc
8. International Standard, IEC 61508, Functional safety of electrical/electronic/programmable electronic safety-related systems, pp. 5515–5516. https://webstore.iec.ch/publication
9. International Standard, ISO 26262, Road vehicles—Functional safety. http://www.iso.org/iso/catalogue_detail?csnumber=43464, etc
10. Gordon E. Moore, Cramming more components onto integrated circuits. Electron. Mag. 19 4 (1965)
11. For actual trend in the speed of integration, refer, for example, to: Intel Website, "50 years of Moore's Law." http://www.intel.com/content/www/us/en/silicon-innovations/moores-law-technology.html
12. Brook, David, "Understanding Moore's Law, Four Decades of Innovation," Chapter 4 (The Future of Integration), p. 39, CHF Publications, Philadelphia, 2006
13. For scaling down the sizes of transistors, refer to: Dennard, Robert H. et al., Design of Ion-implanted MOSFETs with very small physical dimensions. IEEE J. Solid State Circ. **SC-9**, 256–268 (1974)
14. Computer history museum, "Intel's microprocessor." http://www.computerhistory.org/revolution/digital-logic/12/285

15. For the most recent account of what is happening to the Moore's law, readers are referred to: Tom Simonite, "Intel puts brakes on Moore's Law," MIT Technology Review, March 23, 2016. https://www.technologyreview.com/s/601102/intel-puts-the-brakes-on-moores-law/
16. Refer to manufacturer's websites for analog or analogue-digital VLSIs: Texas Instruments, Analog Devices, etc
17. FPGA Manufacturer Websites: Xilinx, Altera, Intel
18. Rodríguez-Andina, J. Juan et al. Features, design tools, and application domains of FPGAs. IEEE Trans. Indust. Electron. **54**, 1810–1823 (2007)
19. Refer to a Wikipedia site, "Active Pixel Sensor." https://en.wikipedia.org/wiki/Active_pixel_sensor
20. As a good reference, visit MEMS & Sensor Industry Group Website. http://www.memsindustrygroup.org/?page=WhatIsMEMS
21. Makimoto, Tsugio and Sakai, Yoshio (2003), "Evolution of Low-Power Electronics and Its Future Applications," Proceedings of the 2003 International Symposium on Low Power Electronics and Design, Seoul, Korea, August 25–27, pp. 2–5
22. Refer to a Wikipedia page, "Application-Specific Integrated Circuit." https://en.wikipedia.org/wiki/Application-specific_integrated_circuit
23. Please refer to manufacturers' website, for example: Texas Instruments, "Digital Signal Processors." http://www.ti.com/lsds/ti/processors/dsp/overview.page
24. Please refer to manufacturers' website, for example: NVIDIA, "What is GPU-Accelerated Computing?" http://www.nvidia.com/object/what-is-gpu-computing.html
25. Tanakamaru, "Degradation of Flash Memories and Signal Processing for Dependability," Section 6.2 of this book
26. Tanakamaru, "Design and Applications of Dependable Non-volatile Memory Systems," Chapter 18 of this book
27. Xilinx, "Zinq-700, All-Programmable SoC." https://www.xilinx.com/products/silicon-devices/soc/zynq-7000.html
28. Renesas web page, "RH 850 Family." https://www.renesas.com/en-sg/products/microcontrollers-microprocessors/rh850.html
29. The DVLSI website is found at the following URL: http://www.dvlsi.jst.go.jp/english/index.html
30. Refer to the DVLSI Webpage. http://www.dvlsi.jst.go.jp/english/adviser/index.html
31. Refer to the DVLSI Webpage. http://www.dvlsi.jst.go.jp/english/list/index.html
32. Priority Programme "Design and Architectures of Dependable Embedded Systems" (SPP 1500) sponsored by DFG (Deutsche Forschungs Gemeincschaft) http://www.dfg.de/foerderung/info_wissenschaft/2012/info_wissenschaft_12_06/index.html Started in 2011 and still running as of 2016 Also refer to: http://spp1500.itec.kit.edu/
33. "Failure-Resistant Systems (FRS)," sponsored by NSF (National Science Foundation) and SRC (Semiconductor Research Corporation) in the United States; http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=504754, http://www.nsf.gov/awardsearch/advancedSearchResult?ProgEleCode=8081&BooleanElement=ANY&BooleanRef=ANY&ActiveAwards=true&#results. Started in 2013 and still running in 2017, participated by about 30 teams
34. Refer to the DVLSI Webpage. http://www.dvlsi.jst.go.jp/english/topics/smpe121201index.html
35. Refer to the DVLSI Webpage. http://www.dvlsi.jst.go.jp/english/topics/smpe131206index.html

Chapter 2
Design and Development of Electronic Systems for Quality and Dependability

Shojiro Asai

Abstract In this chapter, we quickly walk through the development process of electronic systems that use VLSIs as key parts to provide a background and introduction to the rest of this book. Setting a good goal for a development is not simple to begin with, and the task to get there is often more demanding than it appears at the beginning. The importance of project management and role played by the project manager is first pointed out along with the need to clearly define and document the system requirements specification. Besides the performance and dependability, other aspects of the design goal such as cost, timeline, and compliance are discussed as well, in recognition of the reality of product development. After all, the one who heads up the development is in a position to account for the quality of product throughout its life and return on the investment in the development as well. The multiple phases of the life of an electronic system are described: design, verification, prototyping, test, validation/certification, operation in the field, and finally, retirement. Among these, the specific process in the design of risk analysis and dependability engineering is highlighted as the central topic of this book. Simultaneous assessment of the outcome of possible systems failures and economic viability of the product being pursued is elaborated. Some of the specific technologies developed in the present work, CREST DVLSI Program sponsored by JST, are referred to as possible solutions to problems encountered in designing dependability in future electronic systems to address immediate market needs as well as far-reaching issues such as the IoT (Internet of Things) and system of systems.

Keywords Systems requirements specification · Risk analysis
Dependability engineering · Internet of things · System of systems

S. Asai (✉)
Rigaku Corporation, Tokyo, Japan
e-mail: asai@rigaku.co.jp

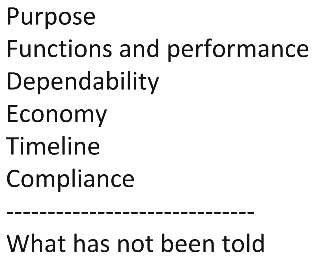
S. Asai (ed.), *VLSI Design and Test for Systems Dependability*,
https://doi.org/10.1007/978-4-431-56594-9_2

2.1 Core Considerations in Designing an Electronic System Product

2.1.1 Purpose and Requirements

Think of an electronic system product—one of a kind that has fascinated and/or inspired you most recently. It could be the electronic payment, Mars Explorer, Toyota Prius, bullet train, or perhaps Apple i-phone. We are sometimes fascinated by these things and intrigued as to how one can complete the task of designing an electronic system as complex as these to perform beautifully with expected dependability, and how they are built and tested to be able to satisfy critical mission purposes or gain general public acceptance in the marketplace. It is amazing as well to recognize that all of these products are enabled by VLSIs playing their critical roles in layers of system hierarchy from the component level as high up to as the top level. In this chapter, we have tried to put together some thoughts on the design and development of complex electronic systems for quality and dependability to lay a ground for later chapters. Particularly for those readers who have basic understanding of electrical engineering and semiconductor technologies and are interested in dependability engineering, this chapter presents a meaningful collection of basic principles, worth sticking to in the design and development of electronic systems and thus will be helpful for those who want to undertake electronic systems design for profession. It is meant to be an introduction to the chapters that follow where technologies for dependability in VLSI and VLSI systems are extensively discussed.

Figure 2.1 is a summary of items where attention is required in designing a system. They include: purpose, functions, dependability, economy, timeline, and compliance. The most fundamental among these items is the purpose, or what the user intends to do using the system being designed. It is often useful to come back and think what the purpose was whenever we need to disambiguate the requirements or make a decision on possible engineering options. The next item is the functions, i.e., the capabilities the system is given by design to be able to fulfill its purpose. Dependability, the third item, is basically availability of functions throughout the expected lifetime of the system. Since this is the central topic of this



Purpose
Functions and performance
Dependability
Economy
Timeline
Compliance

What has not been told

Fig. 2.1 Basic considerations underlying systems design

book, it will be discussed in detail in what follows. Product economy is an issue that needs to be addressed from both angles: performance/cost from the user's perspective or profitability over the product life from manufacturer's perspective. The manufacturer has to recover the (i) initial cost of development (sometimes referred to as NRE (nonrecurrent engineering), (ii) direct (materials and labor) and indirect (supervising) cost of manufacturing, and (iii) SG&A (selling, general, and administrative) overhead expense, with sufficient profit margins that enable capital reinvestment for growth as well as paying out dividends for investors. The product economy from user's perspective is the product value for him contrasting his costs that include initial product price and spending for maintenance and services throughout its life (TCO, or total cost of ownership). In the timeline consideration, it is always a good idea to start from the delivery date demanded by the customer or the predicted market window and work back to the present with time needed for shipping, test, production, and design which is the immediate future task; not to start from the present and move forward without a good grasp of how long each of these steps would take. Compliance to regulations and standards is another "must" that needs close attention. Safety is a priority issue in product compliance and can be one of the most basic functions of the system. Last but not least, there are items the designer may not be explicitly told, which will be addressed in a little more detail in the following subsections.

2.1.2 Design for X

The next consideration goes to product life management, which is summarized in Fig. 2.2 as the "Design for X." Design gives birth to a system as indicated by the leftmost bold arrow on the top half of the diagram. The system is then fabricated, tested, and shipped to the user. The user often benefits from the help of the producer in maintenance and support. When the system comes to the end of life, it needs to be disposed of with safety and permissible negative impact on the environment. It is important to notice that all the collective quality of the system exhibited in its whole life goes back to the design as its origin: performance, ease of use, maintainability, manufacturability, testability, and disposability at the end of its life.

The lower half of this chart tells that the designer needs to have a good grasp of the lifecycle of the system before undertaking the task. It goes without saying that the performance of the system is the central attention for the designer. As indicated by the thin arrows pointing toward left in the lower half of Fig. 2.2, the above thought underlies such important notions as design for fabrication, design for testability, design for mortality, etc. The designer is expected to pay attention to these "Design for X" issues or think back from the future, while shaping the product concept for success.

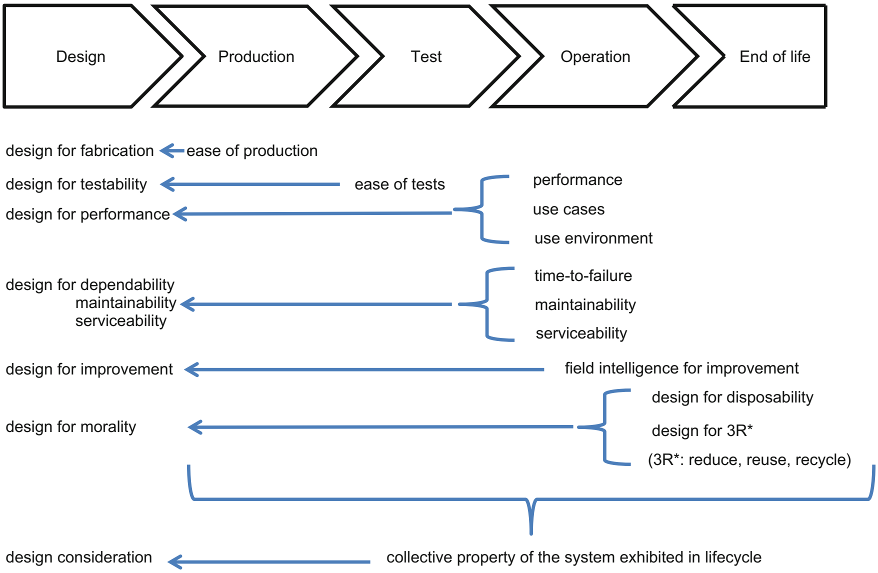


Fig. 2.2 Design for X; look "back from the future"

2.1.3 *Look from Outside*

Another useful look at the design of a system is the one from outside, which is depicted in Fig. 2.3. A system being designed (Let it be called system *A*) could be meant to be used as part of another system (system *B*). The system *B* may actually be just another electronic system in which System *A* is used as a subsystem, or it

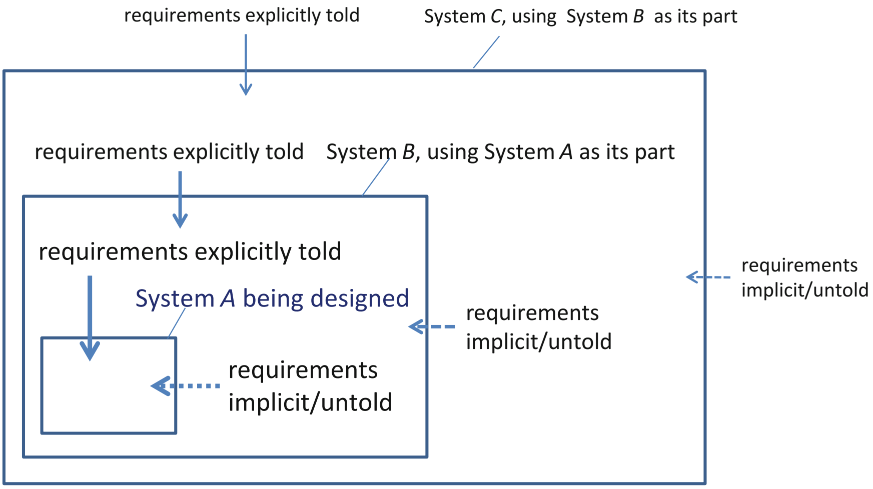

requirements explicitly told
System *C*, using System *B* as its part
requirements explicitly told
System *B*, using System *A* as its part
requirements explicitly told
System *A* being designed
requirements implicit/untold
requirements implicit/untold
requirements implicit/untold

Fig. 2.3 Look from outside—a hierarchical "food chain" of systems. System *A* being designed at its bottom may be used as part of *B*, and so forth

could be a workflow in which *A* is used in a series of related jobs in its owner organization. Requirements for *A* that originates from *B* may in some cases come explicitly from the user but frequently be implicit or untold, especially if *A* is supposed to be, or in fact not quite, a stand-alone system. Likewise, system *B* may be used in yet another system *C*, and so forth. The message that Fig. 2.2 carries is that it is a good useful practice for the project manager to find out about such implicit requirements by going out and listening to the voices of the user and user's user from outside. This practice is part of what is sometimes called "Go to Market."

2.2 Design and Development of an Electronic System Product

2.2.1 Design to Manage the Product Lifecycle

Figure 2.4 depicts a life of an electronic system product designed and built to order and related design activities from conception to retirement. (The cycle for mass-produced products may differ a bit but not very much). At the very beginning,

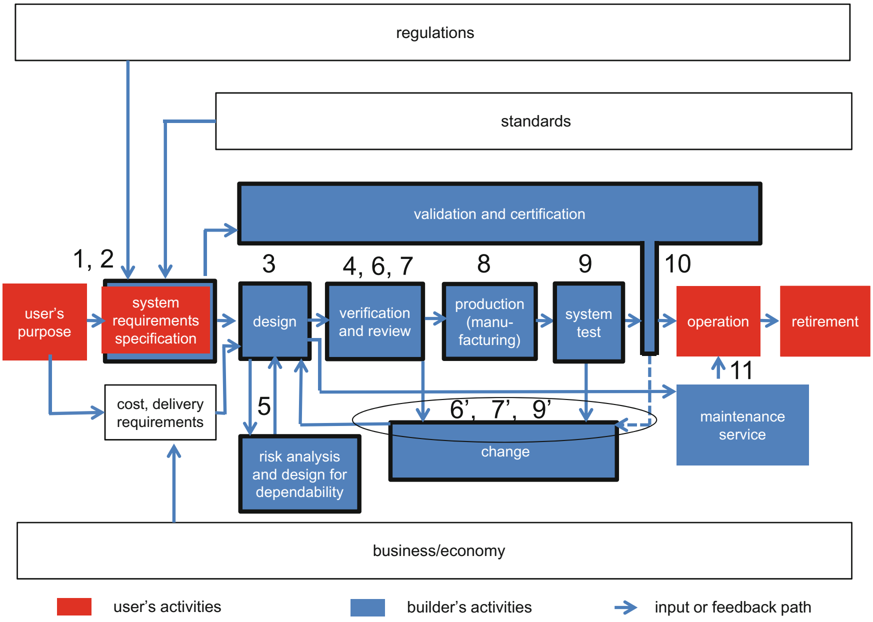
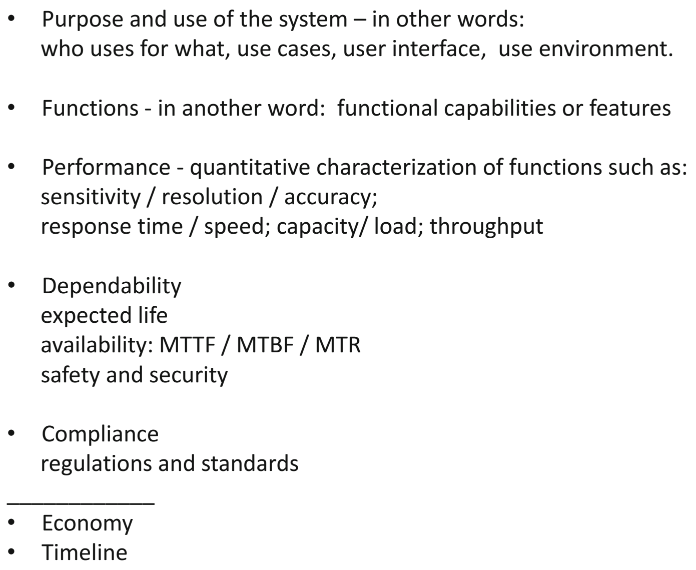


Fig. 2.4 Major stages in the life of an electronic system. The scope of design encompasses the entire lifecycle of the product. Key processes at the builder's house from design to qualification are highlighted with broad black frames surrounding the boxes. The sequential number in the chart corresponds to the process step number in Table 2.1

a set of business objectives at the user's firm is determined, and, to pursue it, a decision is made to procure an electronic system from a systems house. Then, a document is materialized at the user's house that describes the user's purpose (red box in the left end). A design team at the builder's house takes over the user's purpose and starts to work out a more detailed document of the SRS (system requirements specification). Blue boxes are the producer's activities and red boxes are the user's. It is necessary that the user and builder agree on the SRS, which is symbolized in Fig. 2.4 by the second box in blue embracing a red one.

2.2.2 System Requirements Specification

An outline of a model SRS is sketched in Fig. 2.5. It includes the purpose, functions, performance, dependability, and compliance. The purpose and use of the system specify who the user is; what specifically the user uses it for (what objectives, what applications); when (in what situation), where (what use environment), and how (in what user interfaces). Use environment may be specified by the ambient temperatures, humidity, atmospheric pressures, vibrations, line power conditions, electromagnetic noises, ionizing radiations, etc. Electronic systems are generally sensitive to these conditions so that environmental conditions constitute potential hazards that affect its dependability. In an automobile, a very typical electronic system, for example, three basic functions are driving, steering, and



- Purpose and use of the system – in other words:
  who uses for what, use cases, user interface, use environment.
- Functions - in another word: functional capabilities or features
- Performance - quantitative characterization of functions such as:
  sensitivity / resolution / accuracy;
  response time / speed; capacity/ load; throughput
- Dependability
  expected life
  availability: MTTF / MTBF / MTR
  safety and security
- Compliance
  regulations and standards

- Economy
- Timeline

Fig. 2.5 An outline of system requirements specifications (SRS)

stopping. Occupant safety has been added as an important function relatively recently. Automatic driving is being pursued as an ultimate integration of these functions, where the safety becomes the utmost requirements. Every one of the functional items is usually associated with quantitative performance description or characteristic metrics of functions. Performance is typically specified in terms of quality measures such as speed, capacity (load), throughput (speed multiplied by capacity), response time (latency), and accuracy (or sensitivity or resolution). The next item in the SRS listed in Fig. 2.5 is dependability, which comprises an important part of systems requirement specifications and is the central topic of this book. Compliance, economy, and timeline are also issues that need continuous and consistent attention. All of these items are fed into the design as indicated in Fig. 2.4.

2.3 Process and Management of Product Development

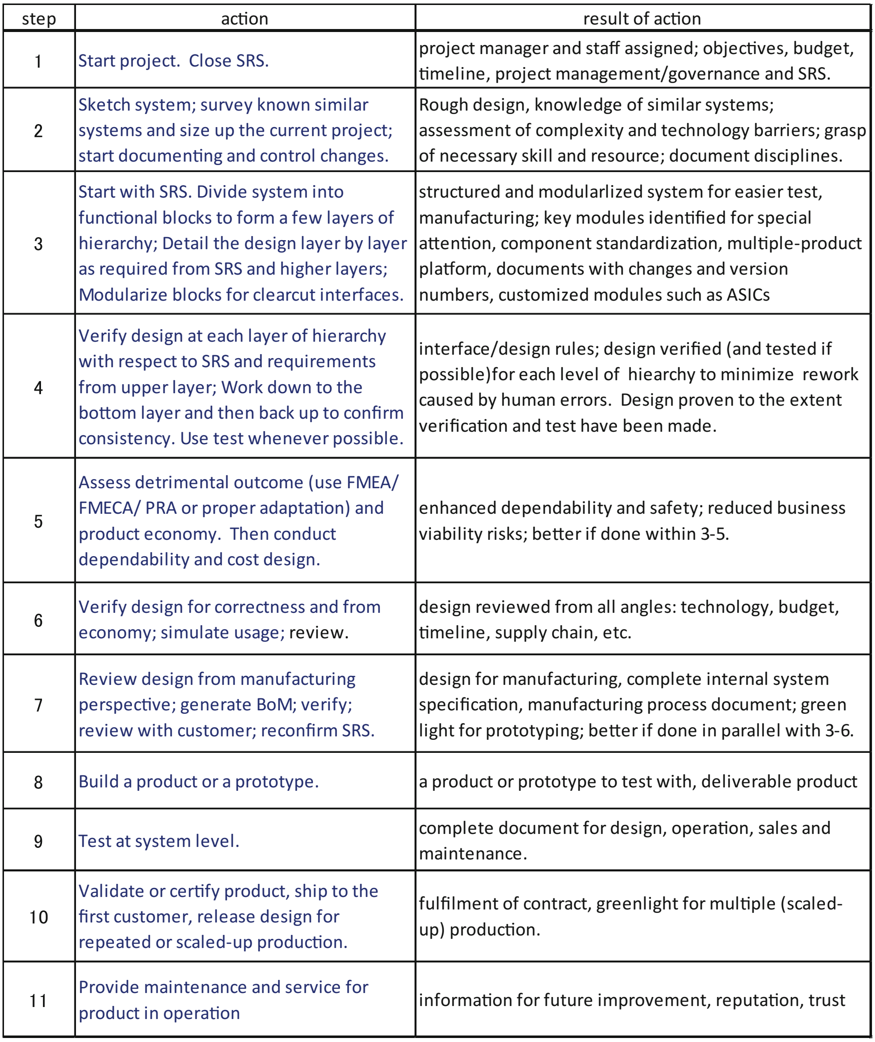
2.3.1 Launching a Project

The process of designing and developing an electronic system product will take a sequence of steps as shown in Table 2.1, which will be described below referring back to Fig. 2.4 as well. Each of these steps is given the same sequential number in Fig. 2.4 and Table 2.1 for the readers' convenience. The inception of the project (Step 1) is marked by the assignment of a project manager. For a custom-built product, the project manager sees to it that his team interacts with the user as intensively as needed to have an SRS documented correctly, exhaustively, and unambiguously in all aspects listed in Fig. 2.1. It is the project manager's responsibility to put together the SRS and to make sure it is implemented in the end product in such a way to serve its intended purpose throughout its life. With the project manager and team members assigned, SRS and accompanying information such as delivery date and product economy put together, at least roughly and agreed on in writing,[1] the project is underway.

It is a good idea to introduce at this stage a method of project management and establish it as a practice of the project. Project management is a mechanism of managing and controlling a project in terms of time, human, and other resources to help achieve the goal. It helps the project manager deploy the work of the project into various necessary tasks, coordinates tasks to meet the milestones (specific

[1] It is customary to conduct the development of a custom-built system under a business contract between the user and the builder. The contract covers SRS, price (for the system, NRE, warranty, maintenance and services, parts supply), delivery, payment conditions, compliance, provisions for the breach of contract terms, and so forth. Such contracts often address the ownership of intellectual properties that underlie or arise/derive from the development. Those who want to be engaged in product development are strongly advised to learn about the management of contractual development project.

Table 2.1 System development process steps



step	action	result of action
1	Start project. Close SRS.	project manager and staff assigned; objectives, budget, timeline, project management/governance and SRS.
2	Sketch system; survey known similar systems and size up the current project; start documenting and control changes.	Rough design, knowledge of similar systems; assessment of complexity and technology barriers; grasp of necessary skill and resource; document disciplines.
3	Start with SRS. Divide system into functional blocks to form a few layers of hierarchy; Detail the design layer by layer as required from SRS and higher layers; Modularize blocks for clearcut interfaces.	structured and modularlized system for easier test, manufacturing; key modules identified for special attention, component standardization, multiple-product platform, documents with changes and version numbers, customized modules such as ASICs
4	Verify design at each layer of hierarchy with respect to SRS and requirements from upper layer; Work down to the bottom layer and then back up to confirm consistency. Use test whenever possible.	interface/design rules; design verified (and tested if possible)for each level of hiearchy to minimize rework caused by human errors. Design proven to the extent verification and test have been made.
5	Assess detrimental outcome (use FMEA/ FMECA/ PRA or proper adaptation) and product economy. Then conduct dependability and cost design.	enhanced dependability and safety; reduced business viability risks; better if done within 3-5.
6	Verify design for correctness and from economy; simulate usage; review.	design reviewed from all angles: technology, budget, timeline, supply chain, etc.
7	Review design from manufacturing perspective; generate BoM; verify; review with customer; reconfirm SRS.	design for manufacturing, complete internal system specification, manufacturing process document; green light for prototyping; better if done in parallel with 3-6.
8	Build a product or a prototype.	a product or prototype to test with, deliverable product
9	Test at system level.	complete document for design, operation, sales and maintenance.
10	Validate or certify product, ship to the first customer, release design for repeated or scaled-up production.	fulfilment of contract, greenlight for multiple (scaled-up) production.
11	Provide maintenance and service for product in operation	information for future improvement, reputation, trust

timings during the project to review the progress of work), making necessary changes and adjustments among different tasks. It also helps enhance the visibility of the progress to the general management and other stake holders of the project.

The US military was the first to put the project management into an organized form during the World War II. It has since been applied to the design and development of systems with varied complexity to cope with increasing complexity. There has been significant progress made with the project management since particularly regarding the difficulty of managing software (program) development, which has become dramatically more important in systems development. A systematic method has been put together by the PMI (Project Management Institute) in association with the CMU (Carnegie-Mellon University) in what is called Project Management standards and procedures it publishes [1]. There are great many commercial project management tools that run on computer these days as well that allow stakeholders either participate or monitor the progress [2].

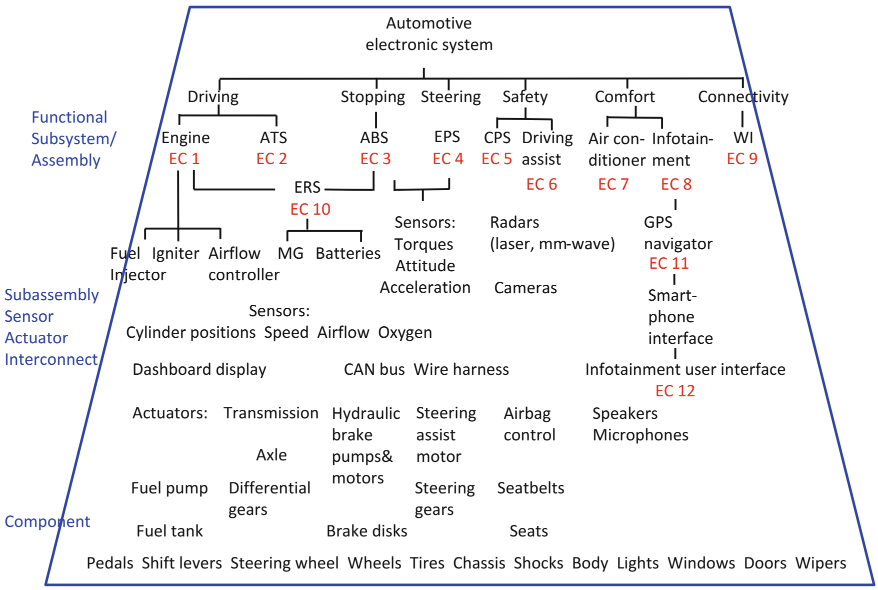
A great deal can be learned by conducting a survey in the next stage (Step 2) looking at the design and working of similar systems which were built in the past and successful (or unsuccessful). The most important thing such a survey will bring is information of what level of complexity the current project team is taking on and/or what new technology problems it is confronted with, relative to what has been experienced in similar projects in the past. Another thing such a survey will provide is information of the performance and availability of parts (software as well as hardware) that can be reused from the past designs. It is necessary for the project manager and the upper management to make sure that people with necessary skills, time, and money are allocated to solve the problems. The worst scenario is that deficiency in the ability of the project team goes unnoticed while on the surface the project moves on.

2.3.2 Breaking Down to Parts and Detailing the Design

The subsequent Step 3 in Table 2.1 is to break or divide the system into parts to form a few layers of hierarchy; major functional blocks in the top layer, subassemblies in the middle layers, and discrete components at the bottom layer. The result of this step is illustrated in Fig. 2.6 for an automobile as an electronic system, which will be described in the subsequent few paragraphs.

The three major automotive functions are driving, stopping, and steering. Other important functions that have been added are safety, comfort, and connectivity. The driving function, for example, is broken down into the engine, transmission, and others that comprise the powertrain. A part marked with a red “EC” sign followed by a serial number in Fig. 2.6 is equipped with an ECU (Electronic Control Unit) with a control microprocessor. The driving function is further broken down into the engine and transmission assemblies. Further down the layers, the driving function comprises subassemblies which consist of sensors and actuators such as fuel injector, igniter, airflow sensor, and many more parts in the component level. It is noted that at least a dozen microprocessors, dozens of them in reality, are used in an automobile.

As seen in Fig. 2.6, a functional block typically consists of a mechanical (or electromechanical) part such as the engine or a fuel injector with its electronic control provided by a microprocessor. It is a good idea to partition the system by allocating an electronic control to each of these functional blocks, making them as independent from each other as possible. Sometimes, however, multiple functional blocks may be required to work in coordination. For example, automatic antilock



ABS: Anti-lock Braking System, CAN: Controller Area Network, CPS: Collision Prevention System, EPS: Electric Power Steering, ERS: Energy Recovery System, MG: Motor/Generator, WI: Wireless Interface

Fig. 2.6 Sketchy hierarchical breakdown of an automotive electronic system. The trapezoidal envelope is to indicate that the key functions of the system are fanned out into increasing number of parts in lower layers. An "EC" with a serial number denotes an embedded computer in subsystems/assemblies and subassembly-level parts. Even component-level parts may have small embedded microcontrollers

braking is a function that can be realized by rendering the steering mechanism as well as the four brakes to a single controller. It does not make sense, in contrast, to have a microprocessor oversee both steering and air conditioning. It is important to partition and modularize the blocks to make the system easy to configure, test, service, and modify for upgrading. Diagrams and charts such as block diagrams of parts, process flow charts, state transition tables, and timing charts are used extensively to describe the working and relationship between the parts.

The software in the system forms a hierarchy similar to that of hardware. The application program for controlling the automobile, which is above the hierarchy shown in Fig. 2.6, written in high-level functional description languages such as C and C++ has been compiled and assembled into machine-language programs, and downloaded onto a microprocessor (any one of the EC1, EC2, etc. in Fig. 2.6) which has an instruction set designed to efficiently execute the assembler language program. For the architecture of microprocessors and software in microprocessor-embedded electronic systems, readers are referred to an excellent book by Patterson and Hennessy [3].

It is worthwhile to think about using an ASIC (Application-Specific Integrated Circuit) in the system. It could comprise a processor core, application software encoded and stored in a flash memory, analog circuits, and an I/O interface that enables performing specified functions. An ASIC can greatly enhance the system performance but yet its cost can be significant particularly for small and/or middle-volume system products. Such an ASIC will be an electric system of its own, and may have to be designed from scratch for specific purposes beginning with the requirements specification and going through hierarchical deployment of functions, logic-level and circuit-level design, all the way down to the physical (transistor) level at the bottom.

Powerful logic synthesis tools are available on the market for ASIC or FPGA design to generate logic at the RTL (Register Transfer Level) description, and from the RTL description the gate-level implementation [4]. When the gate-level description is obtained, circuit simulators such as SPICE [5] are used to make sure that the circuits perform the required logic/arithmetic operation within predetermined delay time margins, satisfying overall speed requirement. Circuit simulator is used also in the design of analog or mixed analog–digital circuits as found in telecommunications or instrumentation systems to achieve the needed accuracy within power consumption and other constraints.

In designing electromechanical systems as in the case of automotive control shown in Fig. 2.6, an analysis of coupled electrical and mechanical systems, often with feedback links, is indispensable for hard real-time (must-respond-in-time) control. A block diagram consisting of electrical/mechanical units and transfer functions of the effects being transmitted in between is analyzed. Tools are available for such purposes [6]. The management of power consumption and heat dissipation is also an important issue that calls for the designer's attention. Heat dissipation is simulated considering the generation of heat from components to make sure that the temperature will not run too high. Mixed-mode simulations of electric and thermal dissipations, for example, are used extensively and are sometimes called "multi-physics" simulators [7].

2.3.3 Design Verification

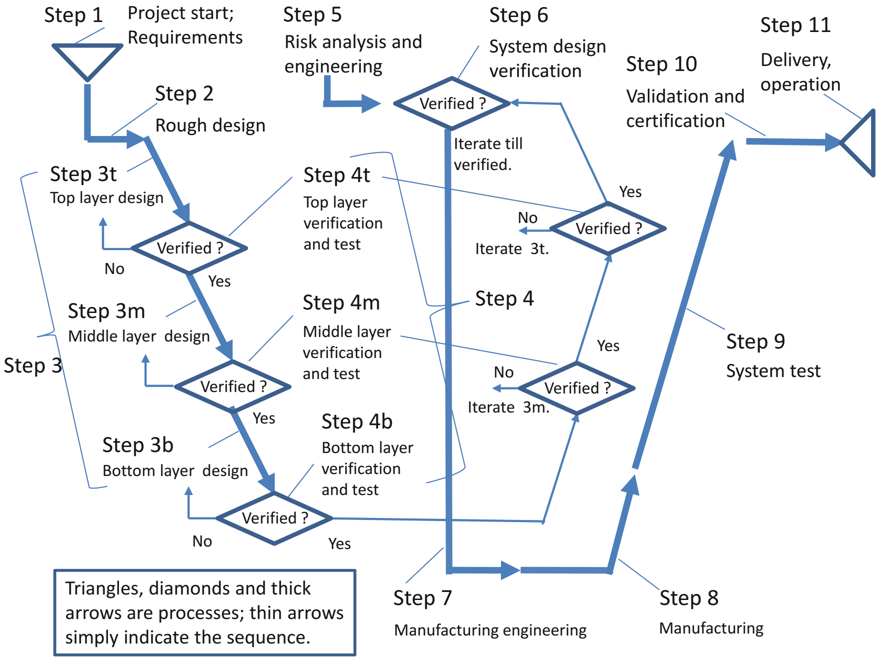
Design verification is a process to prove the correctness of the design and is absolutely necessary because a design of a complex system inevitably includes faults and errors that could arise from mistakes in writing software, inadequate assessment of design margins to accommodate manufacturing variations, environmental conditions, external noises, etc. Verification is conducted in all levels in the hierarchy of the system.

Though complicated it seems, verification process can be structured by using the system structure delineated using hierarchical layers, functional partitioning, and modularization. Actually, it is suggested that the design and verification be done stepwise following the hierarchy as shown in Fig. 2.7. The design in the top layer of hierarchy, Step 3t, is verified in the verification Step 4t, to prove that the functional requirements are fulfilled by the topmost functional hardware blocks and a basic set of primary functional commands and their sequences to drive them. When the design in the top layer has been verified, the design in the middle layers is undertaken (Step 3m), and verified (Step 4m).

The working of the design needs to be verified from all aspects of functional, logical, electrical, and physical (mechanical, thermal, etc.) design. Most tools used for verification are basically the same as those used for design. Input data and operating conditions given to the simulators when used in verifications, however, are in general more extensive and often more extreme to cover the use cases assumed in requirements specification. Some of the more advanced methods of verification such as formal verification and systems-level virtualization will be discussed in Sect. 2.4.3. The layer-by-layer process of design and verification is conducted until the bottom layer design (Step 3b) has been verified (Step 4b).

The letters t, m, and b that follow step numbers indicate top, middle, and bottom layers, respectively, of the system hierarchy. Risk analysis and engineering (Step 5) and manufacturing design and engineering (Step 7) may be conducted within Steps 3 through 4, but are picked out here to emphasize their importance.

A good practice of completing the design and verification is to go the hierarchical layers back up as shown in the right arm of the V-curve in Fig. 2.7 until it is confirmed at Step 6 that all the changes, which may have been made as the results of verifications and test at lower layers so far, are consistent with the requirements



Triangles, diamonds and thick arrows are processes; thin arrows simply indicate the sequence.

Fig. 2.7 The V-model of systems engineering steps. Step numbers correspond to those in Fig. 2.4 and Table 2.1

in the upper layer. Step 6 is the final step of verification to confirm that, though much is still on paper (or on computer) yet, everything fits together at the system level to perform up to the specification. Step 5 that appears in Fig. 2.7 (also in Table 2.1 and Fig. 2.4) is the important process of risk assessment and dependability engineering, which is intentionally singled out and discussed in Sect. 2.4, so that we will skip this subject for now. If Step 5 and 6 are completed, we will have reached Step 7 in Table 2.1 or Fig. 2.4, when the design is now reviewed from manufacturing (production) perspective.

2.3.4 Building a Prototype, Testing, Validation, and Certification

Prototyping

When the design has been verified, the development goes into a next phase of implementation, Step 7 in Table 2.1 (or Figs. 2.4 and 2.7). What is done here is to review the design documents and to generate instructions as to how to build (manufacture) it. Major output of this step is a document called BoM (Bill of Materials). A BoM is a list of hardware materials that constitute a system, from the subsystem/assembly level, module level, component level, all the way down to the subcomponent materials level [8]. It provides not only a useful description of the structure of the product but also how it is procured from whom at what costs and lead-times. Combined with the information of production process steps, what is called the M-BoM (Manufacturing BoM) is generated to describe the production steps and their sequence in terms of standard time, direct labor attended, what part is needed when, and so forth [9]. With the prescription of M-BoM, the first product or prototype is built (Step 8 in Table 2.1). Whether actual prototype building may be done in house or outsourced to an OEM manufacturer, the M-BOM is a key document that interfaces the design team and manufacturing team. It is a good idea to have a joint design review with the customer at this stage before the prototyping gets started.

Test

When the prototype is built, it is subjected to product test at the system level (Step 9). Test is conducted on the prototype or on the final product after it has been built and before it is shipped to the user/market to prove the correctness of the design. A final product deliverable to the customer may be built after all the design changes on the prototype has been introduced and verified. The test is to see if the product performs as specified. First of all, test is often conducted under various use and environmental conditions to find out about the defects that the system under test may exhibit in use. Temperature, humidity, radiation, and vibration are among parameters of the environment. Accelerated reliability or endurance test conducted in extreme operation conditions is used to find out about expected lifetime and life-limiting failure modes. Changes that have been found necessary as the result of verification and test are implemented in the design and recorded in documents (the arrows marked 5', 7', and 9' in Fig. 2.4).

Validation and Certification

Validation and Certification which appears in Step 10 Fig. 2.7, (Fig. 2.4 and Table 2.1 as well) is a step that follows the actual product manufacturing and a thorough system-level test to confirm that the design meets the purposes it is intended for. Validation is to guarantee that the product satisfies the requirements, compliant with regulations. Certification is issued after the product is validated and the confirmation that all documents are in place to account for the product design and to support its users as well as maintenance/service work. Certification is the basis of the assurance that the manufacturer gives on the quality of the product in use in the hands of the user. It is important that the process of certification be in the hands of a quality assurance team that is independent of the design team.

After completion of qualification, the product can then be delivered to the first customer and put into operation to the fulfillment of the contract in the case of a custom-ordered product, or it is turned over to scaled-up production in the case of a mass-manufactured product. Extending maintenance and service to the products in the field (Step 11) provides the design team with the most valuable feedback such as actual reliability information.

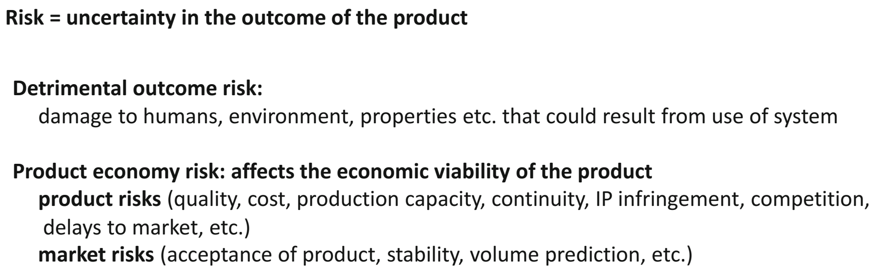
2.3.5 Software and Systems Engineering Practice

For software and systems engineering, there are a number of useful references in addition to those from PMI [1], which has already been referred to. It is useful referring to the voluminous and generic ISO/IEC standards [10] regarding topics such as systems and software engineering and information technology. FDA (United States Food & Drug Administration) also has reference materials that are very useful for those interested in developing medical systems or software for medical purposes [11, 12].

2.4 Risk Assessment and Refinement of Design Against Risks

2.4.1 Risk Assessment

When a rough design has been done, it is time to conduct risk assessment, which will then be followed by refinement of design to mitigate risks (Step 5 in Fig. 2.4 and Table 2.1). This actually is integral part of design, but we have opted to single



Risk = uncertainty in the outcome of the product

Detrimental outcome risk:
damage to humans, environment, properties etc. that could result from use of system

Product economy risk: affects the economic viability of the product
product risks (quality, cost, production capacity, continuity, IP infringement, competition, delays to market, etc.)
market risks (acceptance of product, stability, volume prediction, etc.)

Fig. 2.8 Risks associated with electronic systems as industrial products. Risk is defined as uncertainty in the outcome of product. Two risks considered are detrimental outcome of systems failure and economic viability of the product

out and highlight this issue in this section as the central topic of this book. Risk is defined here as *uncertainty in the outcome of product*. Two risk factors considered are detrimental outcome of systems failure and economic viability of the product as shown in Fig. 2.8.

There are two ways in risk analysis; one starts from the causes and work toward the consequences, while the other conversely starts from the consequences and work back to the causes. The former, inductive, analysis has been very well established as FMEA (Failure Mode and Effects Analysis) or FMECA (Failure Mode, Effects and Criticality Analysis). Both were created for the US military in the 1940s and later enhanced by NASA. These methods have been adopted by aviation and automotive industries. Contrarily, FTA (Fault Tree Analysis) is a deductive analysis that was first developed in Bell Telephone Laboratories in 1962 for US military rocket development and extensively used later in aircraft and other industry sectors as well. A good comprehensive document of FMEA, FMECA, and FTA is available from IEC/ISO [13]. More recently, a more advanced statistical method called PRA (Probabilistic Risk Assessment) has been introduced in the US organizations such as NNC (National Nuclear Council), NASA, and EPA (Environment Protection Agency) [14, 15]. PRA provides a method to quantitatively assess the severity of possible damages and its likelihood.

Figure 2.9 describes sequential steps in risk assessment and mitigation. The step RE 1 (Risk assessment and mitigation Engineering Step 1) is a step to use FMEA/FMECA/PRA or a proper adaptation of these to assess the severity levels of the consequence of a failure in a system. It is worthwhile to note here on “functional safety” (air bag is one of such functions in an automobile) that has recently been introduced to enhance the dependability of systems. IEC (International Electrotechnical Commission) has worked out international standards on this important subject [16]. It is worthwhile for anyone interested in dependability engineering to go through these documents: the general requirements (IEC 61508-1), requirements for electrical/electronic/programmable electronic safety-related systems (IEC 61508-2), software requirements (IEC 61508-3) and techniques and measures (IEC 61508-7), in particular. Using severity levels to quantify the consequence of a failure event is discussed in IEC 61508-5 [17]. It is a good practice to use different alert levels and allocate appropriate dedicated functions to reduce the risks in design as well as production and testing.

Industrial standards concerned specifically with system-level functions for safety of automobiles have also been introduced [18]. The probability of failures in each safety functions supposed to kick in the event of an initial failure is a key factor in determining the probability of detrimental consequence levels using PRA.

The next step, RE 2, is assessing the product economy. The manufacturer will need to obtain ROI (Return on Investment) for the product. ROI is the profit (after all direct costs and overhead) divided by investment (fixed assets and working capital) [19]. The ROI has to exceed the cost of capital, which is a simple rule of capitalism. Costs are always the factor that calls most attention in this analysis so that BoM and M-BoM are key elements. Weighing in-house manufacturing against outsourcing is an important consideration. It is useful to assess ROI from the user's perspective as well: the benefit of the product the user will enjoy against investment (initial price and cost of maintenance and supply).

After all the above consideration with a certain allowance for the choice of key parts, conclusion will be reached about the acceptable levels of detrimental risks and ROI, which will accompany realistic numbers for such things as product life, MTTF, MTBF, error rates, latencies, and narrowed-down ranges of costs (RE 3). These numbers will guide the refinement of design that follows. It is important to note that the plan may have to be aborted if no compromise can be made between the cost and level of detrimental outcome that have to be avoided.

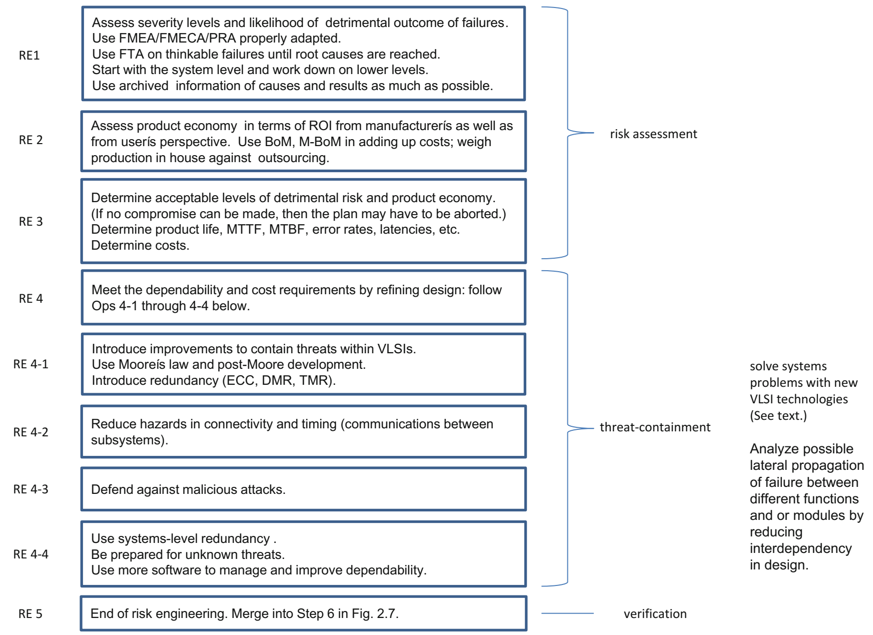
2.4.2 *Refining Design for Risk Mitigation in View of the Dependability and Economy of the Product*

The work in the following step RE 4 in Fig. 2.9 is to satisfy the dependability and cost requirements in the refinement of design. We shall focus here on dependability engineering, and defer elaborating on product economy to another opportunity. The system mean time to failure is determined by:

$$1/MTTF_{system} = \sum_{i=0} 1/MTTF_i, \tag{2.1}$$

where $MTTF_i$ is the MTTF of the i-th component of the system. The system can have a total life of:

$$\text{System Life} = \sum_{j=0} MTTFsystem_j + idle\,time\,for\,service,\ maintenance,\ repair,\ etc. \tag{2.2}$$



RE1 Assess severity levels and likelihood of detrimental outcome of failures.
Use FMEA/FMECA/PRA properly adapted.
Use FTA on thinkable failures until root causes are reached.
Start with the system level and work down on lower levels.
Use archived information of causes and results as much as possible.

RE 2 Assess product economy in terms of ROI from manufacturerís as well as from userís perspective. Use BoM, M-BoM in adding up costs; weigh production in house against outsourcing.

RE 3 Determine acceptable levels of detrimental risk and product economy.
(If no compromise can be made, then the plan may have to be aborted.)
Determine product life, MTTF, MTBF, error rates, latencies, etc.
Determine costs.

RE 4 Meet the dependability and cost requirements by refining design: follow Ops 4-1 through 4-4 below.

RE 4-1 Introduce improvements to contain threats within VLSIs.
Use Mooreís law and post-Moore development.
Introduce redundancy (ECC, DMR, TMR).

RE 4-2 Reduce hazards in connectivity and timing (communications between subsystems).

RE 4-3 Defend against malicious attacks.

RE 4-4 Use systems-level redundancy .
Be prepared for unknown threats.
Use more software to manage and improve dependability.

RE 5 End of risk engineering. Merge into Step 6 in Fig. 2.7.

risk assessment
threat-containment
verification
solve systems problems with new VLSI technologies (See text.)
Analyze possible lateral propagation of failure between different functions and or modules by reducing interdependency in design.

FMEA: Failure Modes and Effects Analysis; FMECA: Failure Mode and Effect Analysis; PRA Probabilistic Risk Assessment; FTA Fault-Tree Analysis; ROI: Return on Investment. Design is refined by implementing dependability and product economy considerations. RE on the left stands for Risk Engineering steps.

Fig. 2.9 Risk assessment and engineering for risk mitigation

where *MTTFsystem$_j$* is the system's MTTF after it has received the *j*-th service, maintenance, and repair work which takes a certain length of (non-operational) time. The useful lifetime is of course the first term of Eq. (2.2). Serviceability, maintainability, and repairability are thus important consideration in dependability engineering to make total system life long enough. Equation (2.1) tells that system MTTF is affected most by the most vulnerable parts with short MTTFs. It is therefore very important to make sure each and every key part has accompanying MTTF information provided by its supplier as part of its qualification. The microprocessor is a key part of the system that its time-to-failure data is very useful. One of the microprocessor manufacturers, Intel, used to make the MTTF of their products publicly available on the Internet. Strictly speaking, the data was not MTTF but MTBF. Even so, it but can be used initially as a good guess for *MTTF$_0$*. It is said that Intel no longer provides the data through the Internet but the company's customer support can be contacted for this information [20].

Any other part of the system that could affect the dependability needs to be verified as its legitimate constituent during RE 4 in Fig. 2.9. If the part happens to be a VLSI, the first thing to be done (RE 4-1) is to see if all the already known dependability-threatening issues inherent in VLSIs as discussed in chapters of Part II of this book have been properly addressed in its design, verified, and tested as well. The VLSI issues discussed in Part II range from tolerance against radiation-induced soft errors [21–25], resilience against electromagnetic interference [26–29], variability tolerance [30–34], and degradation-aware designs [35–39]. The key to RE 4-1 is how to fully exploit the Moore's law [40–42], and post-Moore development in VLSI technologies such as 3-D integration [43, 44]. RE 4-1 also involves the use of technologies which exploit abundant VLSI resource available on chip. For example, redundant memory cells with ECC (Error Correcting Codes) [45] for NVMs (Non-Volatile Memory) [36, 46], duplicate-cell SRAM [38, 47, 48], DMR (Dual Modular Redundancy) [49], and TMR [50] are useful in VLSI, and are discussed throughout this book [24, 39].

RE 4-2 is to address and reduce the effects of hazards that could happen in connectivity and timing requirements in "regional" communications between on-chip cores, across chips, or between subsystems. Wireless interconnect [51, 52] and wireless power supply [53, 54] across chips or modules have been proposed as very promising solutions to replace wired interconnect to cope with problems of vibration and connector reliability, one of the major hazards to dependability in automotive and air-/spacecraft electronics. On-chip and off-chip wired networks with [55, 56] and without [57] using GALS (globally asynchronous locally synchronous) scheme have been discussed as ways to provide redundant interconnect between multiple cores [58]. Noise-tolerant off-chip communications, standardized as the Responsive Link (ISO/IEC 24740:2008), can be an attractive solution [29]. A review of increasing requirements for hard real-time, i.e., "must-respond-in-time (before-the-deadline)," control is given in Sect. 9.1 [59]. A new microprocessor architecture for real-time processing called RMTP (Real-time Multi-Thread Processor) is presented in Sect. 9.2 [60] and Chap. 24 [61]. Another notable work is a reconfigurable processor architecture called FRRA (Flexible Reliability Reconfigurable Array), which is described in two separate papers in this book [24, 62]. The latter describes why this architecture suits the needs of diverse real-time applications for the IoT.

RE 4-3 is to defend the system against malicious attacks. A series of papers in Chap. 10 of this book address vulnerability of VLSIs, especially those used for cyphering/deciphering, and discuss methods to strengthen their tamper resistance. A leading paper that raises the issue [63] is followed by a discussion of tampering methods [64], a tamper-resistant cryptographic circuit [65], verification of tamper-resistant circuit design [66], physical unclonable signature [67], scan-based attacks [68], and evaluation of tamper resistance [69]. A self-contained co-processor for challenge–response authentication is proposed [70].

RE 4-4 is conducting systems-level dependability engineering. Three possible approaches are briefly discussed in the rest of this section: systems-level redundancy, preparedness for unknown threats, and using more software for managing and improving dependability. The so-called "System of systems" which consists of multiple systems is a reality these days and exemplified in multiple government and enterprise systems which operate in different levels of coupling. Some may consist of rather closely coupled systems, while others may include multiple distributed systems in a network that work more or less autonomously exchanging data as needed. One is the use of systems-level redundancy or allowing heterogeneous systems to work interoperably. An interesting proposal made in this book has to do with wireless communications. After a review which highlights the issue of connectivity [71], a series of papers follow discussing various issues relating to this topic—the concept of heterogeneous air interface [72], analog/digital signal processing [73], broadband rf (radio frequency) circuits [74], all-Si CMOS front-end IC [75], versatile A-to-D converter design [76], a frequency-domain equalizer [77], and network management [78]. The original concept of heterogeneous air interface has been expanded into inclusion of satellite communications for message exchange in emergency [79], and use of global clock signal distributed via satellites to better manage heterogeneous handover [80]. Heterogeneous wireless interconnect is only an example of system-level redundancy. The emerging IoT will consist of a variety of systems of systems, where use of systems-level redundancy for back-up dependability will be a standard.

Figure 2.10 summarizes some of the contributions to dependable VLSI systems made in the present work with relevant implications to this section. The listing in Fig. 2.10 has been chosen considering the uniqueness, priority, and importance of the work and has been categorized into technology at the system-of-systems level, system level, assembly or package level, chip level, circuit level, and device level. We will not elaborate on each entry, because that would be redundant with what has been described in the above paragraphs. It is worth noting also that the topic of

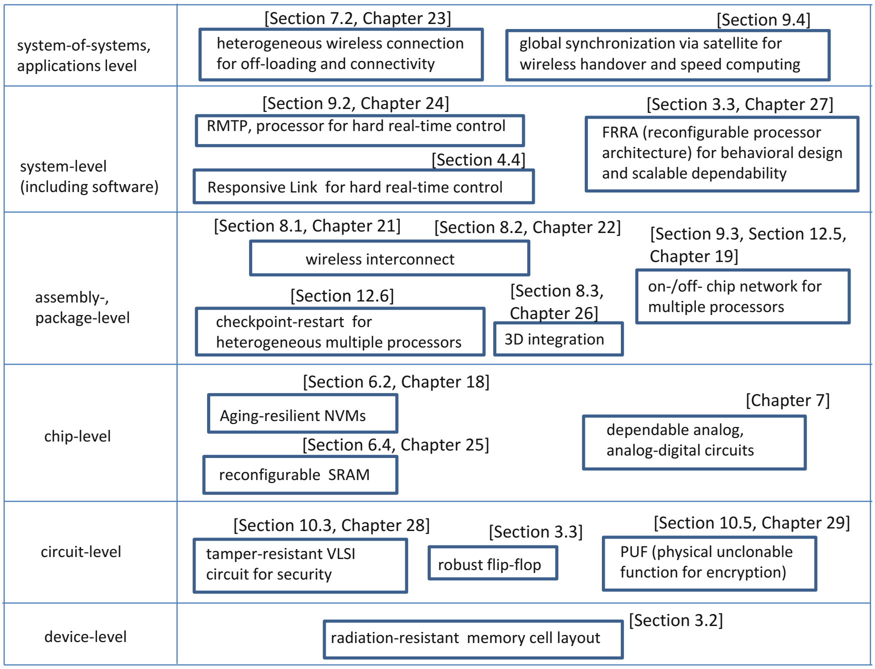

system-of-systems, applications level
[Section 7.2, Chapter 23]
heterogeneous wireless connection for off-loading and connectivity
[Section 9.4]
global synchronization via satellite for wireless handover and speed computing
system-level (including software)
[Section 9.2, Chapter 24]
RMTP, processor for hard real-time control
[Section 4.4]
Responsive Link for hard real-time control
[Section 3.3, Chapter 27]
FRRA (reconfigurable processor architecture) for behavioral design and scalable dependability
assembly-, package-level
[Section 8.1, Chapter 21]
[Section 8.2, Chapter 22]
wireless interconnect
[Section 9.3, Section 12.5, Chapter 19]
on-/off- chip network for multiple processors
[Section 12.6]
checkpoint-restart for heterogeneous multiple processors
[Section 8.3, Chapter 26]
3D integration
chip-level
[Section 6.2, Chapter 18]
Aging-resilient NVMs
[Section 6.4, Chapter 25]
reconfigurable SRAM
[Chapter 7]
dependable analog, analog-digital circuits
circuit-level
[Section 10.3, Chapter 28]
tamper-resistant VLSI circuit for security
[Section 3.3]
robust flip-flop
[Section 10.5, Chapter 29]
PUF (physical unclonable function for encryption)
device-level
radiation-resistant memory cell layout
[Section 3.2]

Fig. 2.10 Technologies for enhanced dependability discussed in this book

unknown threats and preparedness against them is addressed Chap. 12 of this book with suggestions meaningful to this section. Led by an introductory section that gives a historical review of faults [81], sections cover the dependability of data centers [82], patchable hardware as provisions to post-silicon changes [83], logging of field test data for improved dependability [84], fault-detection and reconfiguration in response to it [57], and checkpoint-restart for multiprocessor systems [85].

When all the steps (RE 1 through 4) of risk assessment and mitigation engineering shown in Fig. 2.9 have been completed, the next step (RE 5) is to get back to the original flow of final design verification at Step 6 in Fig. 2.7.

2.4.3 Final Verification and Test

During the final iteration of design verification (Step 6), all useful conventional verification and test methods as described in Sects. 3.3.3 and 3.3.4 can be used. In addition, some of the new methods that have been proposed in the present work, CREST DVLSI, as summarized in Fig. 2.11 may be found useful, some offering new angles in these processes in which coverage becomes increasingly more difficult as system becomes more complex [86] One is formal verification [87, 88], in which logical/mathematical approach is made to prove equivalence of a design to another. The second is a cross-layer simulation in which abstraction of behavior in a lower

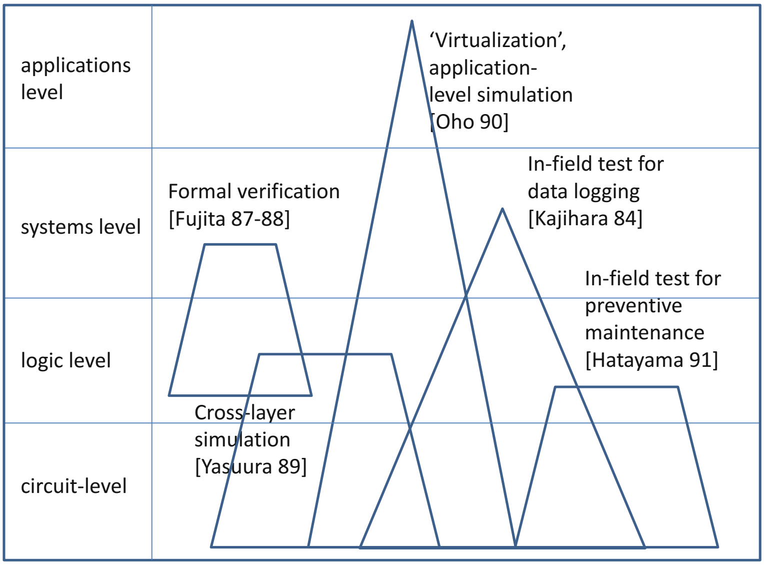

applications level
systems level
logic level
circuit-level
'Virtualization', application-level simulation [Oho 90]
Formal verification [Fujita 87-88]
In-field test for data logging [Kajihara 84]
In-field test for preventive maintenance [Hatayama 91]
Cross-layer simulation [Yasuura 89]

Fig. 2.11 New approaches for verification and test discussed in this book are shown in triangles and trapezoids. The height and breadth of a figure are to roughly indicate the scope of the proposed methods

layer is used to allow simulation of failures at higher levels of hierarchy in the system [89]. An attempt to evaluate the systems-/applications-level failure in an automotive ECU that could result from an error in a SRAM has been successfully demonstrated [90] by using cloud computing. In-field test of VLSI components [37, 91] can be very useful for preventive maintenance of large-scale systems. Technologies for on-chip test circuits for this purpose are discussed in several different sections [32, 33, 37, 92, 93]. In-field test with data logging will be useful for post-failure analysis and archival for future improvement as described in Sect. 12.4 [84].

Step 6 will subsequently be followed by manufacturing engineering (Step 7), actual manufacturing implementation (Step 8) and then the final system test (Step 9), as we have already gone through in Sect. 2.3.

2.5 Conclusion and Future Work

2.5.1 Summary of Chapter 2

Development of electronic systems using VLSI as key parts has been described with a focus on the design process. We have enumerated and elaborated on the items the designer has to keep on mind in developing the product for successful delivery and appreciation. Dependability is clearly among those items and is becoming increasingly more important with systems to be built as they are getting more and more complex. Risk analysis has been outlined and followed by a description of dependability engineering. New technologies proposed in the DVLSI Program were discussed as possible design options for dependability.

2.5.2 Optimistic Outlook—Notable Potential Game Changers from the DVLSI Program

The FRRA (Flexible Reliability Reconfigurable Array) [24, 62] stands out among the VLSI architectures that resulted from the DVLSI program. Truly innovative feature of this architecture is that the description of its functions in a high-level language allows the chip to be automatically configured [24]. It obviously has the speed at least as fast as FPGA and will play a major role in real-time embedded system. The versatility of FRRA will be indispensable in the era of the IoT. Tighter real-time control and assuring data synchronicity between separately running computing elements will become more important. Hard real-time control of automated machines will be enabled by dependable processors such as the RMTP (Real-time Multi-Threaded Processor) [60, 61].

Heterogeneous wireless telecommunications [72, 78–81] will undoubtedly provide more dependable connectivity. It will be a must in the next generation, 5G

(Five-G), or Fifth-Generation, public wireless [94]. Wireless for public safety (police, firefighting) will also be using concepts described in the relevant Chapters [79] and Sections [72, 78, 80]. The heterogeneous air interface is quite innovative because it is a most typical system of systems. It can also be a game changer because the user terminal has a decisive role selecting the connection.

Wireless also provides contactless broadband interface as well as contactless power supply between modules in electronic systems and could be revolutionary for electronic packaging [51–54], replacing bulky connectors and flexible wiring sheet.

Dependability of an electronic system is user experience, which can be shared effectively with the designer by logging and then having the designer analyze degradation and failure modes [84].

There are many other interesting, potential game-changers among the results of the DVLSI program described in this book. Some of the technologies presented here have already proven useful in a proof-of-concept demonstration with realistic electronics systems. Some are still in early phases of conception and in the process of implementation. Further work needs to be continued to make the outcome widely visible and available in either form of systems, components, or test tools.

2.6 Appendix to Chapter 2: The Case of a Scientific Instrument System—An Example Electronic System

This chapter is intended to present an X-ray diffractometer as an example of electronic systems design. Admittedly this is quite a peculiar example, given that the analysis of X-ray diffraction is a very special branch of scientific analysis of materials and therefore most readers will not be familiar with it, though it is a must-have tool for the development of electronic devices including VLSIs. Nonetheless we hope that the readers will better understand the key aspects of design of computer-embedded systems by having this example. The information in this section was made available by the courtesy of Rigaku Corporation [95].

Figure 2.12 is a schematic of X-ray diffraction measurement, a method used to measure the diffraction of X-rays in a material, in which an instrument called X-ray diffractometer as shown in Fig. 2.13 is used. Simply stated, a beam of collimated X-rays is shone on a sample to obtain an image of X-rays on a two-dimensional image sensor, which contains information of the atom-scale structure of the material.

The measurement of X-Ray diffraction is programmed for the windows PC at the top of hierarchy in Fig. 2.13 in C++ or C# language. The program file consists of a sequence of commands, which is linked and compiled into a program in assembler language, and has been downloaded onto the flash memory of the embedded SH-2A computer. A PC is used to initiate the measurement under the control of SH-2A, collect the diffraction image, and analyze them to obtain information of the atomic

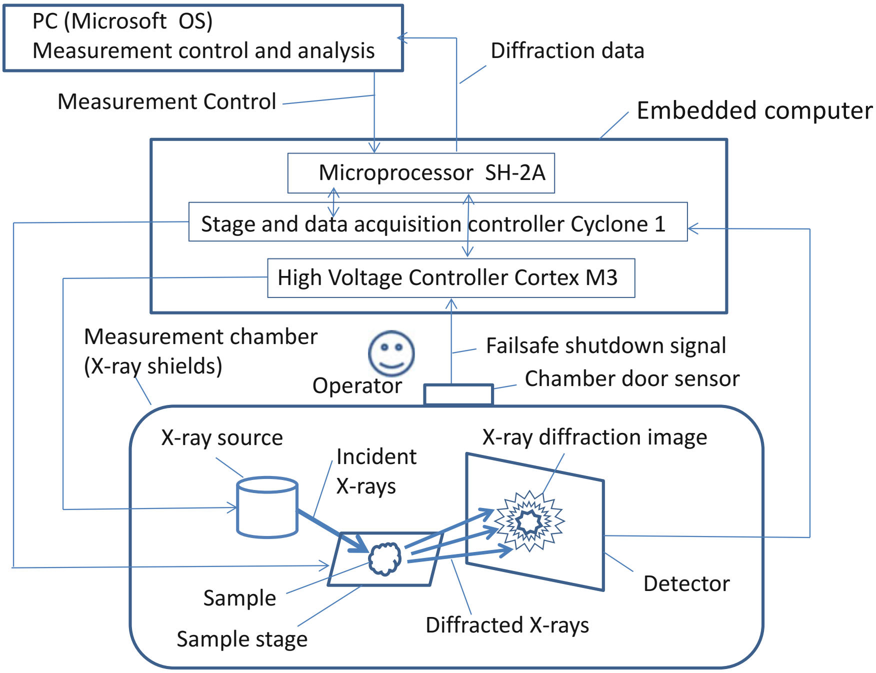


Fig. 2.12 A simplified schematic of an X-Ray diffractometer. The X-ray image that results from the physical phenomenon called “diffraction” of the incident X-rays contains the signature of microscopic structure and composition of substances the sample consists of

structure of the sample. (It is to be noted here that in most embedded systems the PC, on which the embedded software is developed and compiled, is detached from the embedded system at this point in time. The embedded system runs on its own except during the upgrading of software or servicing for maintenance.) The SH-2A running on the iTRON real-time operating system switches over a few different tasks on the priority basis accepting interrupt requests from the instrumentation hardware, including the X-ray source, sample stage, and detector, and reports the measurement result to the PC. The SH-2A, having a multiple interrupt controller with 16 interrupt ports, is convenient for use in a hard real-time environment such as the X-ray diffraction measurement, in which the gating for the detector has to be precisely synchronized with the motion of the 3-D sample stage within less than 0.1 ms. Tasks are dispatched through the fast 50 MHz data bus to the Cyclone FPGA. The SH-2A can take care of instructions that can take time longer than 10 ms to respond to through its various I/O ports such as UART and SPI. The rationale for the choice of an SH-2A as the processor for this system is the capacity and the speed (>100 MHz) to run the real-time iTRON OS and the sufficient I/O capabilities. Figure 2.14 shows photographs of printed circuit boards for an X-ray diffractometer. The motherboard (a) contains a microprocessor SH-2A 7201 from Renesas that runs the iTRON real-time operating system, an FPGA Cyclone-1 from

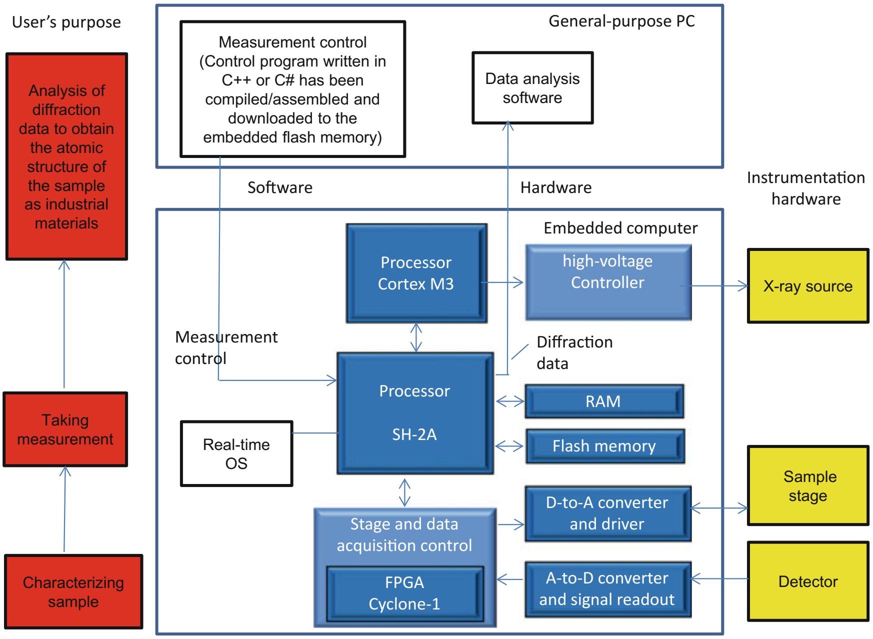

User's purpose
Analysis of diffraction data to obtain the atomic structure of the sample as industrial materials
Taking measurement
Characterizing sample
General-purpose PC
Measurement control (Control program written in C++ or C# has been compiled/assembled and downloaded to the embedded flash memory)
Data analysis software
Software
Hardware
Instrumentation hardware
Embedded computer
Processor Cortex M3
high-voltage Controller
X-ray source
Measurement control
Diffraction data
Processor SH-2A
RAM
Flash memory
Real-time OS
Stage and data acquisition control
FPGA Cyclone-1
D-to-A converter and driver
A-to-D converter and signal readout
Sample stage
Detector

Fig. 2.13 A simplified block diagram of an X-ray diffractometer. User's purpose is to have the intended measurement done automatically and analyze its results as he/she pleases. The embedded system automates the instrumentation using the source, optics, movable stages, etc. The general-purpose computer is used to give macroscopic commands for the embedded computer to execute the measurement and collect data, and then to analyze the data by using the software of his/her liking. Medical imaging and simple robotic systems have a similar structure

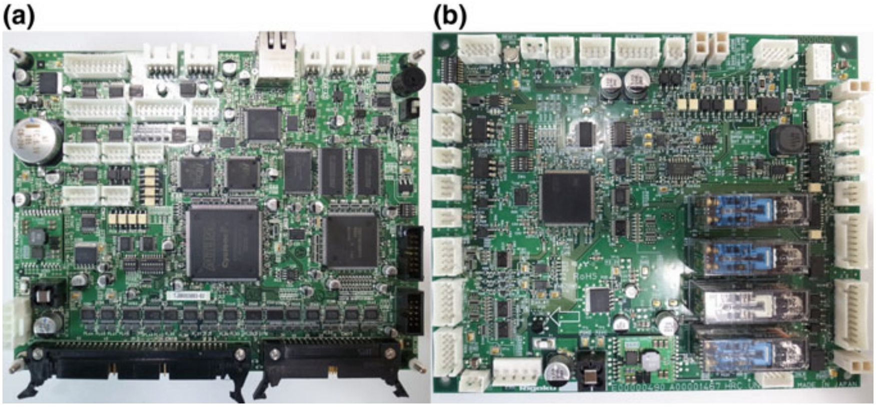


Fig. 2.14 Photographs of an embedded computer system for a scientific instrument called X-ray diffractometer. The motherboard (**a**) contains a microprocessor SH-2A from Renesas that runs the iTRON real-time operating system, an FPGA from Altera, and memory chips. The daughterboard (**b**) is for motor-control contains four safety relays (bottom right) mandated by the regulation to prevent inadvertent exposure to the X-rays (health hazard). Pictures courtesy of Rigaku Corporation

Altera, 14 MB flash NOR memory chip from Spansion, two 32 MB SDRAM chips. The daughterboard (b) contains an ARM Cortex M3 microprocessor from ST Microsystems and four safety relay mechanisms as major components, and is used for the following two purposes; one is controlling the X-ray generator including the vacuum tube, high-voltage power supply, cooling waters, etc., and the other is preventing inadvertent X-ray exposure from happening. The latter may thus be called a functional safety feature of the system. Other safety mechanisms are installed to comply with CE marking directives (low-voltage, electromagnetic and mechanical).

References

1. Project Management Institute, "What is Project Management?" http://www.pmi.org/, https://www.pmi.org/about/learn-about-pmi/what-is-project-management
2. Microsoft Store URL: "Microsoft Project," https://www.microsoftstore.com/store/msusa/en_US/cat/Project/categoryID.69407700
3. D. Patterson, J. Hennessy, *Computer organization and design, the hardware/software interface*, ARM edn. (U.S.A, Morgan Kauffman, Cambridge, 2016)
4. Refer to EDA (Electronic Design Automation) tool vendor websites, for example: Synopsis, Cadence, Mentor Graphics, for example
5. SPICE, A circuit simulator that originates at the University of California at Berkeley and has disseminated by firms specializing in design tools. Tools are available from vendors [4]
6. Refer to the websites of Mathworks, for example, for 'model-based' design tools: https://www.mathworks.com/products/matlab.html?s_tid=hp_products_matlab
7. Refer to the websites of 'multi-physics' simulator vendors, ANSYS, COMSOL, for example: http://www.ansys.com/products/multiphysics https://www.comsol.jp/multiphysics
8. Wikipedia, "Bill of Materials," https://en.wikipedia.org/wiki/Bill_of_materials
9. There is abundant information available on the internet net about this topic. Please throw key words such as "manufacturing bom" at a search engine. Most are offered commercially
10. ISO Website, "Standards Catalogue, ISO/IEC JTC 1/SC 7- Software and systems engineering" http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_tc_browse.htm?commid=45086
11. FDA, "General Principles of Software Validation; Final Guidance for Industry and FDA Staff," FDA website: http://www.fda.gov/RegulatoryInformation/Guidances/ucm085281.htm
12. FDA, "Software As a Medical Device (SAMD): Clinical Evaluation, FDA Website"; http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM524904.pdf
13. International Standards, IEC/ISO 31010, "Risk management -Risk assessment techniques," http://www.iso.org/iso/catalogue_detail?csnumber=51073
14. For example, Dr. Michael Stamatelatos, "Probabilistic Risk Assessment: What is it and Why is it worth performing?" http://www.hq.nasa.gov/office/codeq/qnews/pra.pdf. The internet provides rich reference to PRA which is worth for anyone who is interested in building dependability in electronic products to take time going over. A lot of consultancy firms offer help in risk analysis as well. FDA
15. International Standards, ISO 11231:2010, "Space Systems—Probabilistic risk assessment—PRA," http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=50302
16. International Standard, IEC 61508, "Functional safety of electrical/electronic/programmable electronic safety-related systems," http://www.iec.ch/functionalsafety/

17. International Standard, IEC 61508-5 "Functional safety of electrical/electronic/programmable electronic safety-related systems—Part 5: Examples of methods for the determination of safety integrity levels," https://webstore.iec.ch/publication/5519
18. International Standard, ISO 26262, Road-vehicles—Functional safety,"
19. T. Grossman, J.L. Livingstone, The portable MBA in finance and accounting, 4th edn, Wiley, New York, Sept 2009; see also: R.C. Higgins, Analysis for Financial Management, 10th ed., McGraw-Hill Education, December, 2011 for return-on-investment performance indexes similar but with different definitions
20. Refer to the Intel product support website at the following. http://www.intel.com/content/www/us/en/support/processors/000007093.html
21. E. Ibe et al., Radiation-Induced Soft Errors, Section 3.1 of this book
22. H. Kawaguchi, Soft-Error Tolerant SRAM Cell Layout, Section 3.2 of this book
23. K. Kobayashi, Radiation-Hard Flip-Flops, Section 3.3 of this book
24. Y. Mitsuyama, Soft-Error-Tolerant Reconfigurable Architecture, Section 3.4 of this book
25. M. Sugihara, Simulation and Design Techniques for Memory Systems, Section 3.5 of this book
26. M. Nagata et al., "Electromagnetic Compatibility of CMOS ICs," Section 4.1 of this book
27. M. Nagata, "Electromagnetic Noise Immunity in Memory Circuits," Section 4.2 of this book
28. M. Nagata, "Power Noise of IC Chips in Assembly and Its Mitigations," Section 4.3 of this book
29. N. Yamasaki, "Responsive Link for Noise-tolerant Real-time Communications," Section 4.4 of this book
30. H. Onodera, "Overview of Device Variations," Section 5.1 of this book
31. H. Onodera, "Monitoring and Compensation for Variations in Device Characteristics," Section 5.2 of this book
32. Y. Miura et al., "Highly Accurate Delay-Time Measurement by an On-Chip Circuit," Section 5.3 of this book
33. T. Sato et al., "Timing-Error-Sensitive Flip-Flop for Error-Prediction," Section 5.4 of this book
34. K. Nii et al., "Fine-Grain Assist Bias Control for Dependable SRAM," Section 5.5 of this book Discussed in this chapter are general review of the topic (Sections 5.1 and 5.2), on-chip delay-time measurement (Section 5.3), timing-error-sensitive flip-flop for error prediction (Section 5.4) and fine-grained voltage assist for SRAM that works against variations (Section 5.5)
35. T. Sato et al., "Time-Dependent Degradation in Device Characteristic," Section 6.1 of this book
36. S. Tanakamaru et al., "Degradation of Flash Memories and Signal Processing for Dependability," Section 6.2 of this book
37. Y. Sato et al., "In-Field Monitoring of Device Degradation for Predictive Maintenance," Section 6.3 of this book
38. M. Yoshimoto et al., "A Reconfigurable SRAM Cache Design for Wide-Range Reliable Low-Voltage Operation," Section 6.4 of this book
39. H. Shimada et al., "Runtime Self Reconstruction for Soft/Hard Fault Toleration," Section 6.5 of this book
40. G. Moor, Cramming More Components onto Integrated Circuits. Electron. Mag. **19**, 4 (1965)
41. For actual trend in the speed of integration, refer, for example, to: Intel Website, "50 years of Moore's Law," http://www.intel.com/content/www/us/en/silicon-innovations/moores-law-technology.html
42. B. David, Understanding Moore's Law, Four Decades of Innovation, Chapter 4 The Future of Integration, p. 39, CHF Publications, Philadelphia (2006)
43. M. Koyanagi et al., "Connectivity Issues in 3D Packaging," Section 8.3 of this book
44. M. Koyanagi et al., "A 3-D VLSI Architecture for Future Automotive Visual Recognition," Chapter 26 of this book

45. On-chip error correction in DRAM from Intelligent Memory is said to be capable of correcting single-bit errors on the fly, “ECC DRAM,” http://www.intelligentmemory.com/ECC-DRAM/DDR3/
46. S. Tanakamaru, “Design and Application of Dependable Non-Volatile Memory Systems,” Chapter 18 of this book
47. M. Yoshimoto, “Design of SRAM Resilient against Dynamic Voltage Variations,” Chapter 17 of this book
48. M. Yoshimoto, “A Low-Latency DMR Architecture with Efficient Recovery Scheme Exploiting Simultaneously Copiable SRAM,” Chapter 25 of this book
49. Refer, for example, to; Wikipedia, “Dual Modular Redundancy,” https://en.wikipedia.org/wiki/Dual_modular_redundancy
50. Refer, for example, to; Wikipedia, “Triple Modular Redundancy,” https://en.wikipedia.org/wiki/Triple_modular_redundancy
51. T. Kuroda et al., “Connectivity in Electronic Packaging,” Section 8.1 of this book
52. T. Kuroda et al., “Wireless Interconnect in Electronic Systems,” Chapter 21 of this book
53. H. Ishikuro et al., “Connectivity in Electronic Packaging,” Section 8.2 of this book
54. H. Ishikuro et al., “Wireless Power Delivery Resilient against Loading Variations,” Chapter 22 of this book
55. T. Yoneda et al., “Asynchronous Network on Chip,” Section 9.3 of this book
56. T. Yoneda et al., “Dependable Network-on-Chip Platform for Safety-Critical Automotive Applications,” Chapter 19 of this book
57. M. Imai et al., “Fault Detection and Reconfiguration in NoC-Coupled Multiple CPU Cores for Deadline-Specified Periodical Tasks,” Section 12.5 of this book
58. K. Kise, “An On-Chip Router Architecture for Multicore Processor,” Chapter 20 of this book
59. Y. Nakabo, “Responsiveness for Hard-Real Time Control,” Section 9.1 of this book
60. N. Yamasaki et al, “Microprocessor Architecture for Real-Time Processing,” Section 9.2 of this book
61. N. Yamasaki et al, “Responsive Multithreaded Microprocessor for Hard-Real Time Robotic Applications,” Chapter 24 of this book
62. H. Hihara et al., “A Re-Configurable Processor Architecture for Space Applications,” Chapter 27 of this book
63. T. Fujino et al., “The tamper resistance against Malicious Attacks on Security VLSIs,” Section 10.1 of this book
64. Y. Hori, “Methods for Tampering Cryptographic VLSIs,” Section 10.2 of this book
65. M. Shiozaki, “Tamper-Resistant Symmetric-Key Cryptographic Circuits,” Section 10.3 of this book
66. M. Yoshikawa et al., “Verification Methods for Tamper-Resistant VLSI Design,” Chapter 10.4 of this book
67. K. Nii et al., “A SRAM-Based Physically Unclonable Function for Authentication and Encryption,” Chapter 29 of this book
68. M. Yoshimura, “A Method for Evaluating Vulnerability to Scan-Based Attacks,” Section 10.6 of this book
69. Y. Hori, “Evaluation of Tamper Resistance of VLSI, “Section 10.7 of this book
70. D. Suzuki, “Security Components for Systems-Level Authentication,” Chapter 28 of this book
71. F. Adachi et al., “Challenges for Dependable Public Wireless Telecommunications,” Section 7.1 of this book
72. K. Tsubouchi et al., “Challenges for Dependable Air,” Section 7.2 of this book
73. T. Takagi, “Challenges in Wireless Signal Processing,” Section 7.3 of this book
74. M. Fujishima, “Broad-Band RF Circuit for Versatile, Dependable Wireless Telecommunications,” Section 7.4 of this book
75. R. Inagaki et al., “All-Si CMOS Front-End ICs for Multi-Band Micro-/Millimeter-Wave Communications,” Section 7.5 of this book
76. A. Matsuzawa et al., “Dependable Analog-to-Digital Converter,” Section 7.6 of this book

77. K. Tsubouchci, “Multimode Frequency-Domain Equalizer for Heterogeneous Wireless System,” Section 7.7 of this book
78. S. Kameda, “Network Technology for Heterogeneous Wireless System,” Section 7.8 of this book
79. K. Tsubouchi et al., “Connectivity in Wireless Communications,” Chapter 23 of this book
80. S. Kameda, “Timing Dependability for Wireless Network,” Section 9.4 of this book
81. N. Kanekawa, “Historical Review of Faults and Unidentified Future Threats,” Section 12.1 of this book
82. T. Miyoshi, “Challenges to Dependability at Data Centers,” Section 12.2 of this book
83. M. Fujita et al., “Post-Silicon Validation and Patchable Hardware for Rectification,” Section 12.3 of this book
84. S. Kajihara et al., “Logging and Using Field-Test Data for Improved Dependability,” Section 12.4 of this book
85. H. Takizawa et al., “Checkpoint-Restart in Heterogeneous Multiple-Processor Systems,” Section 12.6 of this book
86. K. Takayama at al., “Verification and Test Coverage,” Section 11.1 of this book
87. M. Fujita et al., “Design Errors and Formal Verification,” Section 11.2 of this book
88. M. Fujita, “Formal Verification and Debugging of VLSI Logic Design for Systems Dependability: Experiments and their Evaluation,” Chapter 14 of this book
89. H. Yasuura, “Design Automation for Reliability,” Chapter 13 of this book
90. S. Oho et al., “Virtualization: System-Level Fault Simulation of SRAM Errors in Automotive Electronic Control System,” Chapter 15 of this book
91. K. Hatayama et al., “Circuit and System Mechanisms for High Field Reliability - DART Technology,” Chapter 16 of this book
92. M. Inoue et al., “High Quality Delay Testing for In-Field Self-Test,” Section 11.3 of this book
93. T. Yoneda et al., “Temperature- and Voltage-Variation-Aware Delay Test,” Section 11.4 of this book
94. L. Young, Telecom Experts Plot a Path to 5G, in *IEEE Spectrum IEEE*. http://spectrum.ieee.org/telecom/wireless/telecom-experts-plot-a-path-to-5g. Accessed 6 Oct 2015
95. Refer to Rigaku Corporation website for information regarding X-ray diffraction and X-ray diffractometer. http://www.rigaku.com/en

Part II
VLSI Issues in Systems Dependability

Chapter 3
Radiation-Induced Soft Errors

Eishi H. Ibe, Shusuke Yoshimoto, Masahiko Yoshimoto, Hiroshi Kawaguchi, Kazutoshi Kobayashi, Jun Furuta, Yukio Mitsuyama, Masanori Hashimoto, Takao Onoye, Hiroyuki Kanbara, Hiroyuki Ochi, Kazutoshi Wakabayashi, Hidetoshi Onodera and Makoto Sugihara

Abstract We will begin by a quick but thorough look at the effects of faults, errors and failures, caused by terrestrial neutrons originating from cosmic rays, on the terrestrial electronic systems in the variety of industries. Mitigation measures, taken at various levels of design hierarchy from physical to systems level against neutron-induced adverse effects, are then introduced. Challenges for retaining robustness under future technology development are also discussed. Such challenges in mitigation approaches are featured for SRAMs (Static Random Access Memories), FFs (Flip-Flops), FPGAs (Field Programmable Gate Arrays) and computer systems as exemplified in the following articles: (i) Layout aware

E. H. Ibe (✉)
Exapalette, LLC., Tokyo, Japan
e-mail: eishi_h_ibe@exapalette.com

S. Yoshimoto · M. Yoshimoto · H. Kawaguchi
Kobe University, Kobe, Japan

K. Kobayashi · J. Furuta
Kyoto Institute of Technology, Kyoto, Japan

Y. Mitsuyama
Kochi University of Technology, Kochi, Japan

M. Hashimoto · T. Onoye
Osaka University, Osaka, Japan

H. Kanbara
Advanced Science, Technology & Management Research Institute of KYOTO (ASTEM), Kyoto, Japan

H. Ochi
Ritsumeikan University, Kyoto, Japan

K. Wakabayashi
NEC, Tokyo, Japan

H. Onodera
Kyoto University, Kyoto, Japan

M. Sugihara
Kyusyu University, Kyusyu, Japan

S. Asai (ed.), *VLSI Design and Test for Systems Dependability*,
https://doi.org/10.1007/978-4-431-56594-9_3

neutron-induced soft-error simulation and fault tolerant design techniques are introduced for 6T SRAMs. The PNP layout instead of conventional NPN layout is proposed and its robustness is demonstrated by using the MONTE CARLO simulator PHITS. (ii) RHBD (Radiation-Hardened By Design) FFs hardened by using specially designed redundant techniques are extensively evaluated. BCDMR (Bistable Cross-Coupled Dual Modular Redundancy) FFs is proposed in order to avoid MCU (Multi-Cell Upset) impacts on FF reliability. Its robustness is demonstrated thorough a set of neutron irradiation tests. (iii) CGRA (Coarse-Grained Reconfigurable Architecture) is proposed for an FPGA-chip-level tolerance. Prototype CGRA-FPGA chips are manufactured and their robustness is demonstrated under alpha particle/neutron irradiation tests. (iv) Simulation techniques for failures in heterogeneous computer system with memory hierarchy consisting of a register file, an L1 cache, an L2 cache and a main memory are also proposed in conjunction with masking effects of faults/errors.

Keywords Terrestrial neutron · Soft-error · Simulation · SRAM
BCDMR · Flip-Flop · ALU · CGRA · Heterogeneous computer system
Register file · Cache · Mitigation measures

3.1 Fundamentals and Highlights in Radiation-Induced Soft-Errors

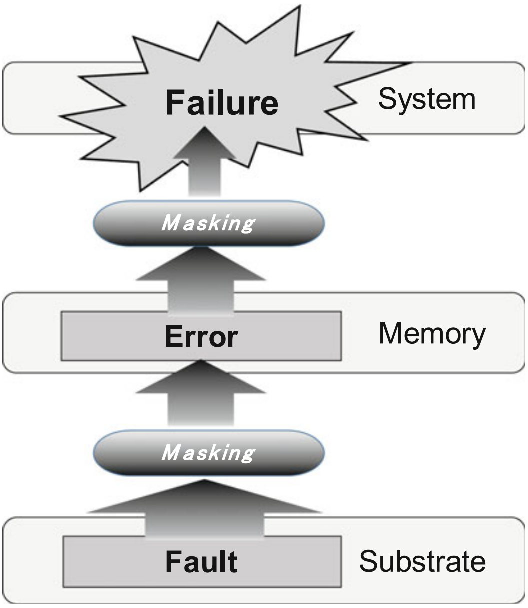
Eishi H. Ibe, Exapalette, LLC

3.1.1 Hierarchy of Faulty Conditions of an Electronic System

Reliability is gaining monumental spotlights as the foremost property that is indispensable for the overall worth of electronic products, in particular, with respect to radiation hardness at the ground [1–3]. Once failures take place in electronic systems in the market, the news is spread over the world immediately though the internet and massmedia and the products or even the vender companies may, in the worst case, lose their business chance for a long period of time.

It is believed that the failures should have some sequential steps of symptoms to result in failures in almost all the troubles. In the most electronic systems, the symptom starts with a simple fault in the substrate of a circuit board in the system. Before the fault would grow the fatal failure, there should be many kinds of symptoms towards failures in a variety of situations. In many cases, a substantial

Fig. 3.1 Hierarchy of faulty conditions: fault-error-failure



part of faults may be disappeared or eliminated during propagation by a certain logical/timing masking effects as illustrated in Fig. 3.1, but some may be captured and fixed in memory elements such as SRAM, DRAM, flash memory, flip-flops, and so on. Once these faults are fixed in the memory elements, they have a lot more chance to cause the system failed.

It is important, therefore, to detect the faults, errors, and onsets of the failure, and eliminate them at the early stage to prevent fatal failure.

In the present chapter, we will show the basic understandings and examples of countermeasures against evolving threat of soft-error in electronic systems induced by terrestrial neutrons in VLSI devices and systems.

3.1.2 Sources of Neutrons in the Field and Fundamentals of Terrestrial Neutrons

In space applications, primary cosmic-ray (electrons, protons, and heavy ions)-induced soft-errors and hard-errors (permanent errors by which the device is mechanically destructed) are major concerns in reliability, which may cause failures and eventually determine the life of a space craft [4].

Meanwhile, when energetic cosmic ray protons enter into the atmosphere (troposphere and stratosphere) of the Earth, some protons undergo *nuclear spallation* *reaction* with nuclei (mainly nitrogen and oxygen nuclei) in the atmosphere to produce a number of light particles or secondary cosmic rays including neutrinos, photons, electrons, muons, pions, protons, and neutrons. As the cosmic rays are deflected by Heliomagnetic field or the Sun's activity whose intensity has about 11-year cycle, strength of neutrons at the ground has also about 11-year cycle [5]. The neutron flux at the ground is the lowest, during the *solar maximum* (states when the Sun is the most active), while it is the highest at the *solar minimum* (states when the Sun is the least active).

Since a secondary neutron causes a cascade of spallation reactions in the atmosphere, it produces a *shower* of secondary particles and radiations that reaches the ground of the Earth. As the thick air layer over the ground can shield neutrons, strength (both of flux and energy) of neutrons depends upon altitude with slight dependency on atmospheric pressure [6]. Compared to neutron flux at the avionics altitude (about 10,000 m), therefore, the neutron flux at terrestrial altitude is much lower by a factor of 100–300.

The cumulative flux, which is the sum of total flux from the minimum neutron energy determined by some practical reason (in some standards like JESD89A [7] as below, for example) to the maximum neutron energy, is summarized in Fig. 3.2 with respect to of the terrestrial neutron flux estimated at the NYC sea level [1]. Figure 3.2a can be used for evaluation of the effects of thermal (about 25 meV) or low-energy (<1 MeV) neutrons, and Fig. 3.2b can be used for evaluation of the effects of high-energy (>1 MeV) neutrons. The total flux beyond 10 meV can be estimated 13 n/cm^2/h from Fig. 3.2b, which is consistent with JESD89A setting [7]. It is noteworthy that the energy of terrestrial neutrons ranges widely from thermal (25 meV) to high-energy (>1 GeV) and its total flux is about 50 n/cm^2/h at the ground including NYC sea level.

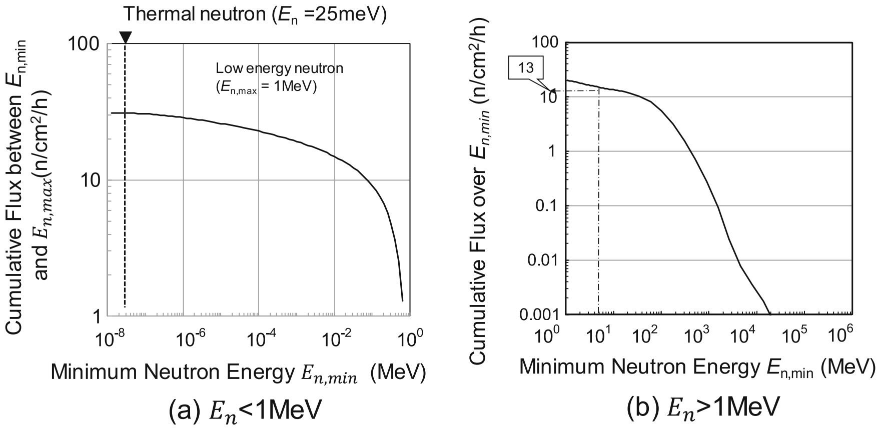


Fig. 3.2 Cumulative neutron flux at the NYC sea level. **a** Low-energy (<1 MeV) neutrons, **b** high-energy (>1 MeV) neutrons (2015©IEEE [1])

Table 3.1 Type of nuclear reactions that can be induced by terrestrial neutrons at the ground

Type	Neutron energy range	Target nucleus	Mechanism	Main secondary products	Relevance to the present book
(i) Fission	Thermal to epi-thermal	^{235}U, ^{238}U	The reactions are utilized for nuclear power plants thanks to its tremendous power generation. This reaction is not relevant to the present paper because the natural abundance of target nuclei are extremely low.	Any ions whose atomic number is equal to or les than the target nucleus, including ^{137}Cs, ^{131}I, and ^{90}Sr.	None
(ii) Neutron capture	Thermal to <1MeV	^{10}B, ^{112}Cd, ^{113m}Cd, ^{155}Gd,^{157}Gd	Only when the target nuclei are contained in the chips, this reaction has certain imoacts on the reliability of electronic systems. The target ^{10}B is of major concern.	^{10}B produces an alpha particle plus a residual excited ion.	Minor
(iii) Spallation	>1MeV	Any	Only when the energy of the incident neutron is high enough, this reaction takes place to produce a number of combination of secondary particles including pions,muons and neutrons. Major targets are Si and O.	Any ions whose atomic number is equal to or les than the target nucleus	Major

Neutrons themselves are not charged particles, thus do not interact directly with matters except for very limited cases such as nuclear reactions and as summarized in Table 3.1. Only some charged particles, which can be produced as a consequence of nuclear reaction depending on the type of reaction, may cause SEEs. Since the natural abundances of the target nuclei in (i) nuclear fission reaction (^{235}U/^{238}U) are negligibly low, the reactions (ii) neutron capture reaction and (iii) spallation nuclear reaction only matter in the terrestrial fields.

In particular, the reaction mechanism (iii) has major roles in SEEs in the terrestrial fields, and therefore, the neutron reaction (iii) is focused in the present chapter. Only when ^{10}B is contained in the matter, reaction mechanism (ii) may be of concern as explained in Sect. 3.1.6(iv).

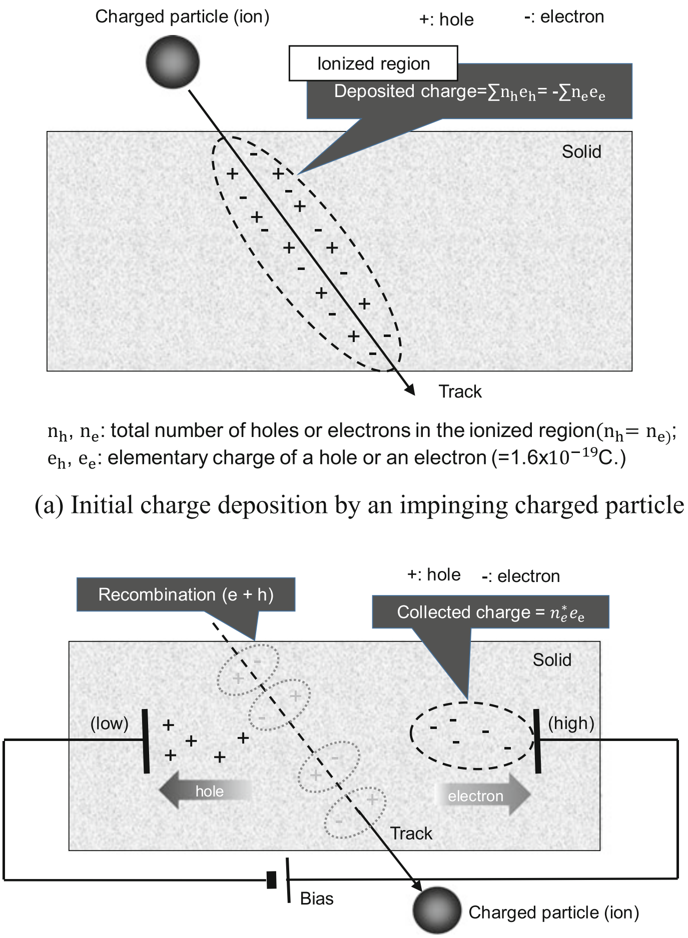
Energetic charged particles including secondary particles from the nuclear reactions above interact with matters via Coulomb interaction mechanism.

Namely, while an energetic charged particle passes through the material, an orbital electron (conduction-band electron in solid) is stripped from its orbit by Coulombic interaction with the impinging ion, leaving electron-hole pairs (deposited energy of 3.6 eV is required to produce one-pair of electron-hole pair in Si) along with the trajectory of the impinging ion as illustrated in Fig. 3.3a. This process is called “direct ionization” or “charge deposition”.

The original sum of charges of electrons or holes is called “deposited charge”.

Some or most parts of electrons and holes recombine to disappear in particular in metals and dielectrics because mobility of the carrier is very high (electrons in metals) or low (holes in dielectrics). Some part of electrons and holes can survive from recombination in semiconductor materials under a certain level of potential gradient. (This can take place even in dielectrics under very high potential field.)

Some part of the deposited charges generated in the semiconductor materials can be collected by applying a certain level of potential gradient as illustrated in Fig. 3.3b. This process is called “charge collection” (to the electrode).



n_h, n_e: total number of holes or electrons in the ionized region(n_h= n_e);
e_h, e_e: elementary charge of a hole or an electron (=1.6x10^{-19}C.)

(a) Initial charge deposition by an impinging charged particle

n_e^*: number of electrons escaped from recombination and reached to the (high) electrode.

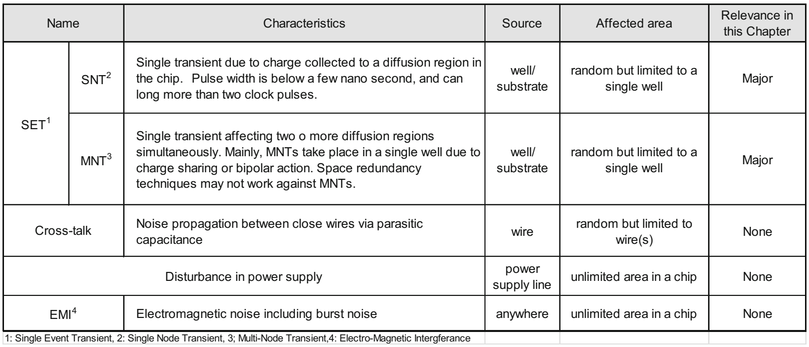
(b) Subsequent charge collection by potential field
(drift-diffusion process also takes place)

Fig. 3.3 Basic physical phenomena in matters by an energetic charged particle. **a** Charge deposition (direct ionization), **b** charge collection

3.1.3 Generation of Faults: Origin of Errors and Failure

There are number of sources of faults in electronic devices and circuits such as SET (SNT and MNT), power disturbances [3], and EMI [3] as summarized in Table 3.2 and they play very crucial roles in reliability in the electronic systems for the ground applications.

Table 3.2 General sources of faults in electronic devices/circuits



Name		Characteristics	Source	Affected area	Relevance in this Chapter
SET[1]	SNT[2]	Single transient due to charge collected to a diffusion region in the chip. Pulse width is below a few nano second, and can long more than two clock pulses.	well/ substrate	random but limited to a single well	Major
	MNT[3]	Single transient affecting two o more diffusion regions simultaneously. Mainly, MNTs take place in a single well due to charge sharing or bipolar action. Space redundancy techniques may not work against MNTs.	well/ substrate	random but limited to a single well	Major
Cross-talk		Noise propagation between close wires via parasitic capacitance	wire	random but limited to wire(s)	None
Disturbance in power supply			power supply line	unlimited area in a chip	None
EMI[4]		Electromagnetic noise including burst noise	anywhere	unlimited area in a chip	None

1: Single Event Transient, 2: Single Node Transient, 3; Multi-Node Transient,4: Electro-Magnetic Intergferance

SET is a single transient due to charge collected to a diffusion region in the chip by an energetic particle impingement. Pulse width is below a few nano-second, and can long more than two clock pulses, which may require special and additional design consideration [8].

When SETs take place in multiple diffusion regions, the phenomenon is called MNT (Multiple Node Transient) that may corrupt the protective functions in the redundant circuitries [9].

Cross talk is noise propagation between close wires via parasitic capacitance [10]. Disturbance in power supply [3], and EMI [3, 11] are very important fault sources in electronic systems.

The most important characteristics of faults caused by a single event effect compared to other fault sources mentioned above is that they are initially only localized in a single well or substrate. In other words, it can be said that SET has an internal origin in the transistor structure while other sources have external origins outside transistors. Keeping this difference in mind, we will focus only on faults caused by a single event effect in this book. Please have a look at [3] for details of the last two mechanisms, power disturbance and EMI.

3.1.4 Transformation of Faults to Errors and Failures

As an SET is a single rapid (pico- to nano- second order) pulse noise in the substrate or well so that it is very difficult, in general, to detect and locate it in the device. Suppression of them to low enough level is also very difficult, but they do not always transform to "error". Three important concepts of faulty conditions of a system are explained in [1].

An error is an incorrect state in a digital circuit node that could be caused by a data flip in a memory element like an SRAM (Static Random Access Memory)

[12], a DRAM (Dynamic Random Access Memory) [13], a flash memory [14], and an FF (Flip-Flop) [15] or an extra delay in a circuit [16]. When an error is caused by ionizing radiation, it is called SEU (Single Event Upset) or SE (Soft-Error) [7]. When an SEU causes randomly distributed multiple errors, it is also called an MCU (Multi-Cell Upset) [7]. Failure is a malfunction or dysfunction of a system. It is to be noted that a fault may or may not give rise to an error and an error may or may not result in a failure; A fault may or may not be strong enough to cause a memory bit to flip; An errors in a circuit may or may not reflect in the arithmetic results on a system. Furthermore, it is possible to reduce the probability of escalation of faulty conditions. It is therefore very important to characterize the nature of faulty conditions and their behavior in escalation from lower levels to higher levels of hierarchy.

Whether an error causes a failure or not depends on its location and the particular function that the system happens to be performing. Only when an error(s) propagates to the final output and cause malfunction of the system, we call this consequence as "*failure*". An error does not always cause a system failure, because it may disappear or may be *masked* during propagation in the chip or board by some masking effects. The real failure rate of a system, therefore, cannot be estimated from the total sum of memory SEUs or SERs (SE Rates) in the system. In order to estimate realistic failure rate of a computer system can be obtained through computer simulation and extended in Sect. 3.5. Some mitigation techniques like parity [17], ECC (Error Correction Code) [18], and interleaving techniques [19] may be applied to reduce SER. In the parity technique, one extra bit is added to a word (a set of bits) that expresses a character like numbers and alphabets. The data in the extra bit is set according to whether the number of "1" in the word is odd or even. When an SBU takes place in the word, the datum in the extra bit and the word become inconsistent and thus the SBU can be detected. In the ECC, more extra bits are added to a word to correct the error(s) in the word. To reduce speed, area and power penalties, the simplest scheme, Hamming code [18], where an SBU can be corrected based on the coding theory, is commonly applied. Two or more errors in the same word, which is called an MBU (Multi-Bit Upset) cannot be corrected by the Hamming code. Interleaving technique, by which the intervals between the bit in the same word are made wide enough compared to the penetrating ion range, is applied to reduce MBUs.

Failures include shut-down, abnormal operation of the system. Incorrect calculation by using supercomputers can also be categorized into failure. Failure is not recovered by system itself without physical or economic damages.

3.1.5 Fundamentals of CMOS Semiconductor Devices

In order in primary importance to understand the physical aspects of soft errors in relation to real MOSFET structure. A brief look at the structsure of CMOS (Complementary Metal Oxide Semiconductor) devices [20], which are commonly recognized as the most vulnerable semiconductor structure to neutron-induced soft-error, such as SRAMs, FFs and most logic circuits is given here. CMOS circuits are basically built on the identical striped structure of p and n- dual wells as illustrated in Fig. 3.4a for one bit of an SRAM or one OR gate. Unlike dual well structure (this structure is often called “bulk”) as illustrated in Fig. 3.4b, triple-well structure has an additional deep n-well to isolate Si-body from electrical disturbance in the substrate. It is recognized that the triple-well structure have some benefit for soft-error resilience because the volume of charge collection is limited and reduced above the deep n-well.

In SOI (Silicon On Insulator) devices [20], BOXs (Buried-OXides) [21] are made under the dual wells to isolate the Si-body vertically and completely from the substrate. Isolation oxides such as Shallow Trench Isolation (STI) oxides are also made to isolate each node in lateral direction for such a structure. The SOI structure, therefore, has more advantages in soft-error resilience than triple-well structure does.

Further challenges have been made on the SOI structure: When the thickness of the SOI layer is thinner than the depth of depletion region in the SD (Source-Drain) channel, the structure is called FD (Fully Depleted) SOI [22]. Meanwhile, when the thickness of the SOI layer is thicker than the depletion region, the structure is called as PD (Partially Depleted) SOI [23]. Since the upper surface of BOX in FDSOI is covered fully with the depletion region, parasitic capacitance can be largely reduced compared to bulk/PDSOI devices, resulting in steep sub-threshold characteristics, reduction in latency, and power consumption.

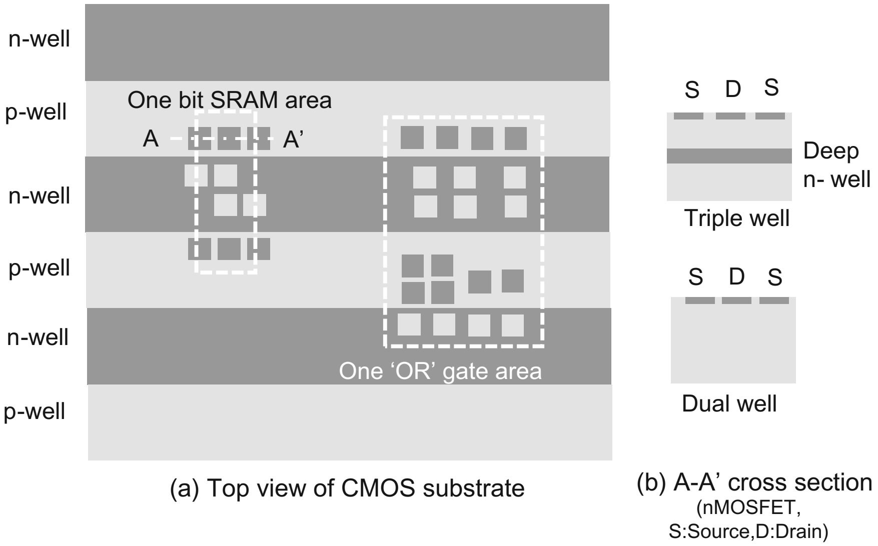


Fig. 3.4 Basic layouts of CMOSFET devices on **a** the striped structure of p- and n-wells and **b** cross sections of triple and dual wells

Sugii et al. develop Silicon on Thin BOX (SOTB) [24] structure by which backgate bias can be applied in Silicon substrate below the bottom of thin (about 10 nm thickness) BOX in order to control *V*th [24] (see Sect. 3.3 for more details). This structure is also called as *double-gate* structure because the Si-body is sandwiched by the conventional gate and the backgate.

The structure of Si-body has been changed continuously year by year as mentioned above, and will also be changed even drastically in the future. The challenges to enhance the resilience of CMOS devices, however, have to be started continuously and simply with Si-body structure because it is the initial condition of the failures regardless of the memory or logical origins.

3.1.6 Effects of Ionizing Radiation on Semiconductor Circuits

(i) Soft-Error

As first found in alpha particle-induced soft-error mechanism [25], a high-energy single charged particle that hits a semiconductor generates a number of electron-hole pairs along its trajectory as illustrated in Fig. 3.5a, which is similar to Fig. 3.2a used for general material. When a charged particle penetrates into a depletion region at the bottom of the storage node of semiconductor memory cell (diffusion region), electrons flow into the off-state storage node (with “high (1)” potential for an n^+ node, for example) in accordance with electromagnetic field there as illustrated in Fig. 3.5a. The mechanism shown in Fig. 3.5b is again called *charge collection* mechanism. The potential in the node is eventually lowered down by charge collection below the threshold potential between “1” and “0”, resulting in an SEU or a soft-error to flip the data from “1” to “0”. The flipped state can be recovered without any physical damages in the semiconductor device simply by rewriting data. This is why the phenomenon is called “soft”-error. In addition, charge collection is intensified by funneling effect [26], in which electrostatic field in the depletion region is elongated beneath the original depletion region by flowing electrons themselves and more electrons than initially contained in the depletion region are collected. Charge collection may cause SEU in both DRAM and SRAM [12] when the collected charge exceeds the critical charge Q_{crit}, which can be estimated by

$$Q_{crit} = \frac{C_s}{2} V_{cc}, \tag{3.1}$$

where,

C_{s} storage node capacitance;
V_{cc} supply voltage.

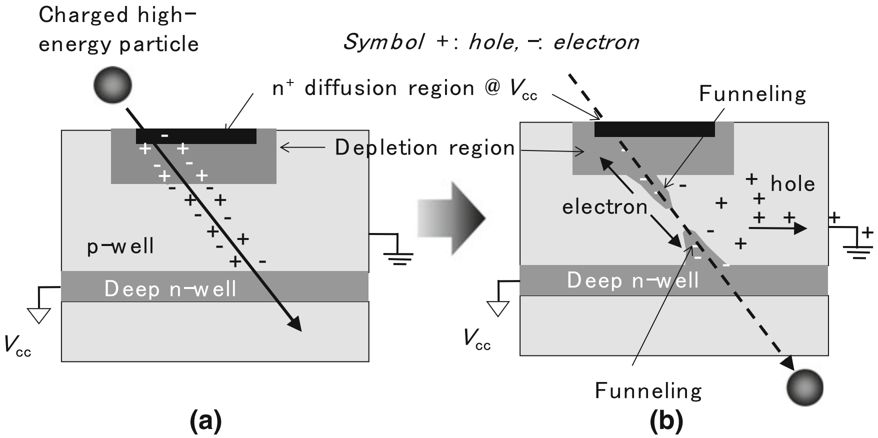


Fig. 3.5 Physical phenomena in basic nMOSFET structure with deep n-well induced by a high-energy particle. **a** Charged (secondary) particle penetrates through an n^+ diffusion region (storage node) and charge deposition. **b** Charge collection to the diffusion region

The principal metric that stands for the vulnerability of semiconductors is SER (Soft Error Rate), which is calculated by

$$\mathrm{SER} = \text{Number of events/time.} \tag{3.2}$$

The unit of SER is FIT (Failure In Time: number of events/10^9 h). Another unit, FIT/Mbit (of memories), is commonly used referring to the SER per memory bit capacity.

(ii) Error modes other than soft-error

Unlike soft-error, there are other error modes that cannot be recovered by rewriting.

SEFI (Single Event Functional Interrupt) is an error mode in logic circuits by data flips in FFs contained in the logic circuits [27]. State in an FF can be flipped in two ways by an ion hit. One is capture of an SET from the input of an FF. The other is data flip by direct hit into an FF storage node by ionizing radiation. An SEFI may be related to the FF behavior but is not understood fully. It is said that it cannot be recovered by rewriting of memory data, but can be recovered by resetting FF data to default values [1].

SEL (Single Event Latchup) is a phenomenon in which a pnpn switch is turned on resulting in an I_{dd} current increase accompanying a number of circuit errors [28]. SEL cannot be recovered by re-writing but can be recovered by power-cycling (power off and then power-on) [7]. SEB (Single Event Burnout) and SEGR (Single Event Gate Rupture) are permanent destructive modes of radiation effects in power devices [29–31].

(iii) The influence of scaling on radiation-induced faults or SER

Scaling (shrinking) the feature size (linewidth and spacing) has been the key to reduce power consumption, increase density and performance of LSIs, and, therefore intensely pursued for many decades [32]. From a viewpoint of SEE, however, there are some conflicting impacts by scaling

(1) The smaller a memory size becomes, the lower the probability to be hit by an energetic particle, resulting in reduction of SER.
(2) In addition, volume for charge collection become smaller, the amount of collected charge gets smaller compared to Q_{crit}, resulting in reduction of SER.
(3) Capacitance of a storage node C_{s} is, in principle, in proportion to the area of a storage node. Scaling of memory cell, therefore in general causes decrease in the capacitance and worsens susceptibility of a memory cell due to decrease in Q_{crit} ($\propto C_{\mathrm{s}} V_{\mathrm{cc}}$).
(4) The distance between adjacent storage nodes is shortened by scaling, which causes "charge-sharing" [33] between multiple nodes. This causes an increase in MCU ratio to total SEUs.
(5) The distance between pn-junctions is also shortened, which causes increase in susceptibility to bipolar effects including latchup. Such bipolar effects are becoming dominant in CMOSFET (CMOS Field Effect Transistor) circuits as a result of scaling (see Sect. 3.1.7 for more details).

The impacts (1) and (2) are beneficial for SER reduction. The impacts (3)–(5) are adverse effects. They are in a trade-off relation and, therefore, SER may increase or decrease depending on which mechanism is dominant.

Next we will discuss how SER at which errors occur in a device, is estimated. When a single particle penetrates into a device(s), it can cause multiple transients or multiple errors. By definition, physical consequence due to one single particle including neutron is called an SEE. When an SEE causes an error(s), we call this phenomenon SEU. Therefore, SEU can consist of multiple errors. *Important thing is that SER is defined by the number of SEUs, not by the number of errors.*

Another important quantity used in this chapter is *SEU cross section* σ_{seu} that is defined by

$$\sigma_{seu} = \frac{N_{seu}}{\Phi_p}, \tag{3.3}$$

where,

N_{seu} the number of SEUs (not errors!)/count;
Φ_{p} fluence of particles (neutrons)/(n/cm^2).

Fluence means the total number of particle passed through a unit area.

σ_{seu} can be measured in experiments using radio-isotopes or accelerators [1] and one can calculate SER by using the σ_{seu} as follows:

$$SER = \ < \sigma_{seu} > \times \phi_p \times 1 \times 10^9 / \mathrm{FIT}, \tag{3.4}$$

where,

$<\sigma_{\mathrm{seu}}>$ is an average of σ_{seu} over particle energies to adjust for actual field (or packaging) environment;
ϕ_{p} flux of the particle/(count h^{-1} cm^{-2});
FIT Failure In Time, SER in 10^9 h.

Flux means the number of particles that pass through a unit area per unit time.

3.1.7 Bipolar Action: A Newly Found Mode of Radiation-Induced Faults

As explained in Sect. 3.1.5, electron-hole pairs are produced along the trajectory of a high-energy particle when it passes through a semiconductor device. If the particle passes through the depletion region of the pn-junction under an off-state n-diffusion at the potential V_{cc}, electrons in the depletion region are collected to the n-diffusion region to cause a *single event fault* or a SEU and holes are repulsed out of the depletion region.

Ibe et al. pointed out that, in addition to the charge collection described so far, there is a novel soft-error mechanism, which they called Multi-Coupled Bipolar Interaction (MCBI) [34]. When a high-energy charged particle passes through the pn-junctions, not below the diffusion region, for example, in the side wall of the p-well in the triple-well CMOS structure as shown in Fig. 3.6a, direct ionization or charge deposition, by which electron-hole pairs are produced along with the track, similarly to Fig. 3.5a. Then, as illustrated in Fig. 3.6b electrons produced in the well flow out of the well by the same funneling mechanism as the conventional soft-error mechanism, leaving the holes in the well. These holes can make the well potential high enough to turn the parasitic npn transistor in the well "on" as illustrated in Fig. 3.6c. As a substantial number of nodes are contained and flipped in a single common well, the "high" nodes in the MCBI region can be flipped simultaneously to cause MNT or MCU.

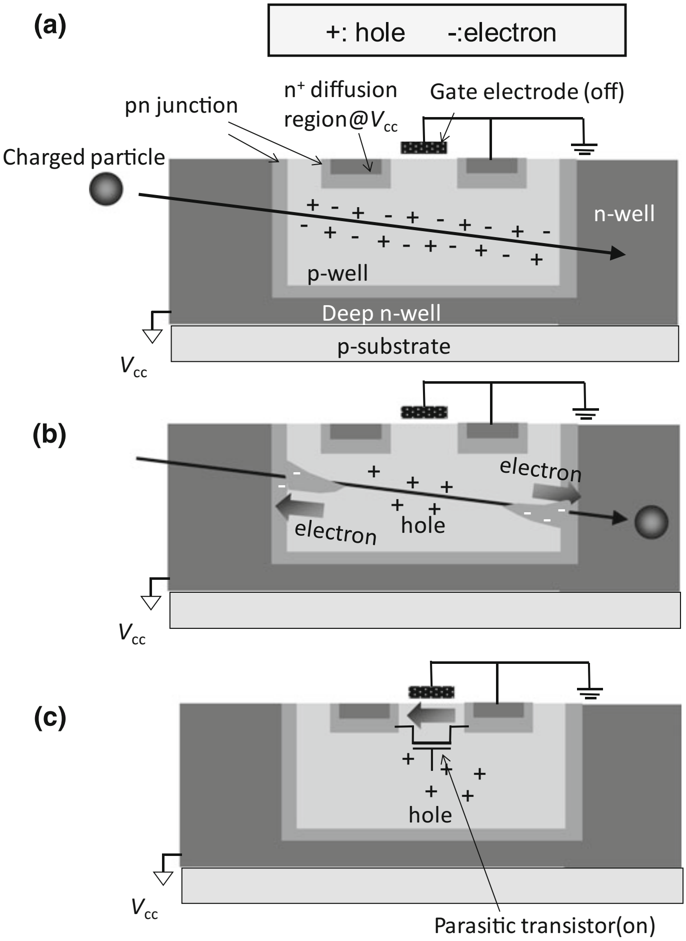


Fig. 3.6 Physical phenomena in basic nMOSFET structure induced by a high-energy charged particle. **a** Charged particle penetrates through pn-junctions on the side wall of the p-well and generate electron-hole pairs. **b** Electrons flow out of the p-well and holes remain in the p-well. **c** Holes elevate the potential in the p-well, resulting in turning the parasitic transistor on to cause soft-error

3.1.8 A Perspective of Progresses in Research and Engineering of Radiation-Induced Soft Errors

In this subsection, a historical review will be given regarding how technology challenges were encountered in the issue of radiation-induced soft-errors in LSIs and how engineering have solved them. Ever since alpha particle soft error was first discovered in DRAMs in 1979, a few distinctive *paradigm shifts* have been experienced.

(i) First paradigm (1979–1990s) where SRAM design rule and density are >250 nm and <64 kbits, respectively: It is well known that alpha particle-induced soft error in DRAM was discovered by May et al. in 1979 [25]. In the same year, the possibility of soft-error due to terrestrial neutron is pointed out by Ziegler and Lanford [35]. As the impact of alpha particles on DRAMs appeared to be most devastating at that time, engineering attention was focused on alpha particles. By the early 1990s, alpha particle soft error in DRAMs was overcome by several effective countermeasures such as stacked or trench capacitors to enhance storage capacitance [36], triple-well structure, usage of purified low-alpha materials, and shielding by package materials [37–39]. Thus, soft errors in LSIs for terrestrial applications did not get much attention until the late 1990s.

(ii) Second paradigm (late 1990s–2000) was experienced when SRAM design rule and density were around 130 nm and 128 k–4 Mbits, respectively: The terrestrial neutron-induced SER of SRAM was found to have become much higher than DRAMs [40]. It is understood that SER in DRAMs, which have embedded capacitors to keep high Q_{crit}, naturally has decreased thanks to the beneficial effects of scaling as mentioned previously in Sect. 3.1.3 (iii) (1) and (2). Meanwhile, SRAMs do not implement any artificial capacitor, and, therefore, SER in SRAMs has drastically increased by the adverse effect mentioned in Sect. 3.1.3 (iii)(3).

(iii) Third paradigm (2000–2005) was experienced when SRAM design rule and density were around 90 nm and 8 Mbits, respectively: Filing neutron irradiation data report to users was mandatory for memory venders, and this triggered discussions on neutron standard testing methods worldwide. As a consequence, JESD89 [41] for neutron, proton and α-ray SER testing method were issued as the de facto soft-error testing standard in 2001. In the third paradigm shift, concerns on neutron soft-error further spread over two directions from around 2004. One direction was concerns about MCU that emerged from about 130 nm process due to bipolar effects [42] and charge-sharing effects [43]. When a MCU takes place in more than two bits in the same word of SRAM, it cannot be recovered by using EDAC (Error Detection and Correction) or ECC (Error Checking and Correction) to result in system crash. EDAC or ECC can detect two-bit errors and correct one-bit error, but cannot correct two-bit errors in the same word (MBUs). It was found that almost all MCUs had taken place in one single MOSFET well and been aligned along with the only two adjacent bit lines. Based on this finding, newly found problem of neutron-induced MCUs in SRAMs was basically overcome by applying both ECC and interleaving with a small interval [34]. Another direction was to address concerns about single event transient (noise) in sequential and combinational logic devices. SERs (Soft-Error Rates) in flip-flops were predicted to be close to that in SRAM beyond 90 nm design rule [44], but there had been no effective detection and correction methods in logic devices except for redundancy techniques. Moreover, obvious threats of common-node failures or those due to MNT had been found in most space redundancy techniques, like TMR [45] and DICE (Dual-Interlocked storage Cell) [46]. If an MNT happens in two modules of TMR or two input nodes of DICE, recovery mechanism fails and may result in SDC (Silent Data Corruption) that cause unrecognizable system failure [47]. Uemura et al. [48] and Lee et al. [49] proposed ideas to harden DICE-like flip-flops by changing layout of nodes independently in 2010.

In addition to the two distinct directions described above, Baumann et al. pointed out soft-error caused by thermal neutron caption reaction by ^{10}B that has natural abundance of 19.9% in Boron contained in the BPSG (Boron Phosphor Silicate Glass) used for the planarization of wafer surface [50]. When a thermal neutron, mostly of cosmic origins, which has a typical energy of 25 meV in equilibrium with atmospheric molecules, is captured by a ^{10}B nucleus, a He ion (1.47 MeV) and a ^{7}Li ion (0.84 MeV) are released to cause soft-errors by ionization. This type of soft-error seemed to have been overcome by changing the planarization process from BPSG to CMP (Chemical Mechanical Polishing), which does not use Boron.

(iv) Fourth paradigm (2006–2009) was experienced where SRAM design rule and density were around 65 nm and 16 Mbits, respectively: Discussions on revision of JESD89 was started in 2003 because the original JESD89 had a number of limitations: the only testing facility assigned as the standard facility was the spallation neutron source in Los Alamos National Laboratory, for example. The new version JESD89A [7] was issued in 2006 with more practicable and reliable testing and analysis methods including *quasi-monoenergetic neutron* test method. Differential spectrum of terrestrial neutron was revised and a certain number of neutron irradiation facilities were added as the standard facilities. IEC60749-38 standard that is consistent with JESD89A was issued in 2008 as the de jure standard [51].

(v) Fifth paradigm (2010) was experienced when SRAM design rule and density were <40 nm and >32 Mbits, respectively: the impact of soft-errors spread over large electronic systems. For big data-centers [52] or exa-scale supercomputers [53], power reduction had been one of the most important design issues. The space redundancy techniques that require large areas and power overheads would not be therefore applied to such big systems, in principle. Real-time (safety critical) systems like avionics or micro-control units in automobiles are also becoming under serious concerns and in-depth studies were widely undertaken [54, 55]. AEC Q100 G [56] and ISO26262 [57] for automobiles were also issued in 2008 and 2011, respectively.

With a common recognition that soft-error-induced system failure cannot be suppressed to satisfactory level by applying mitigation techniques only to a single design stack layer (device, circuit, chip, board, firmware, OS, middleware, and so on), communications between and combined mitigation techniques among stack layers have been encouraged as unavoidable direction [58–61]. In reality, such collaboration has turned out to be very difficult since the basic engineering skills in each stack layer are essentially and significantly different. Most engineers/

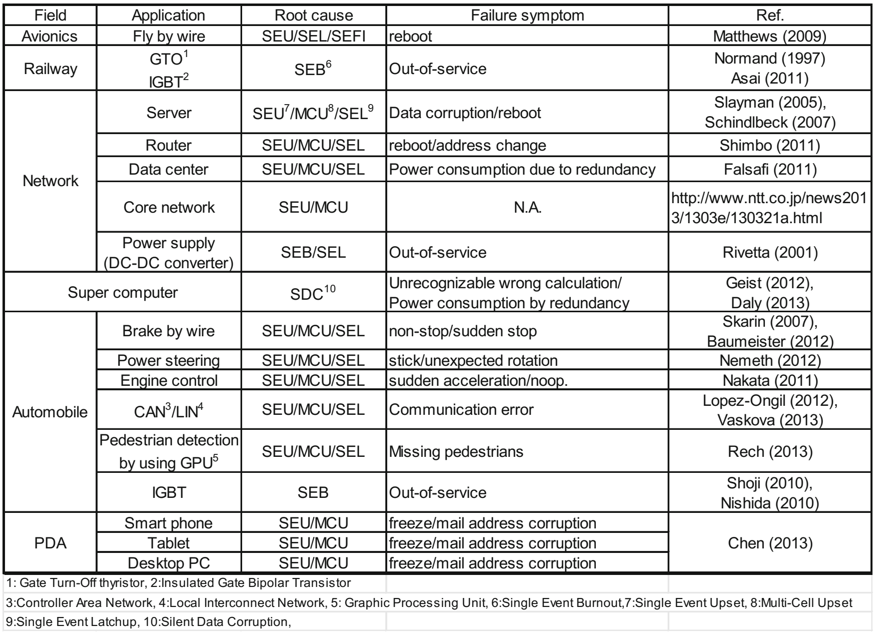
researcher cannot expand their specialties beyond their own stack layers. Novel strategies to overcome this situation are needed to be explored and being proposed. *Built-in* communication scheme among the stack layers has been proposed by Ibe et al. in their LABIR (inter-Layer Built-In Reliability) concept [62, 63]. Evans et al. have proposed the RIIF (Reliability Information Interchange Format) as common format or protocol to be used in system design among stack layers [64].

In the possible sixth paradigm shift, other terrestrial particles, like muons, low-energy neutrons, protons, are being pointed out as a possible SER threat at the ground [65]. Alpha particle with VLA (Very Low-Alpha)-level package can again cause soft-errors in SRAMs [66]. Sub-100 nm SRAMs have a substantial susceptibility for soft-error due to terrestrial muons [67]. Low (thermal) energy neutron causes soft-error due to neutron capture reaction of ^{10}B in device without BPSG processes [68, 69]. Concerns on electrons (beta rays) and gamma rays have been boosted after the severe accident in Fukushima-1 nuclear power plants [70, 71].

3.1.9 Spreading Concerns on Failures in Industries

Table 3.3 summarizes recent concerns in various fields of industry related to single event effects with applications, possible root causes, and observable failure symptoms [72–88].

Table 3.3 Status-of-the-art failure reports by terrestrial neutrons in various industries



Field	Application	Root cause	Failure symptom	Ref.
Avionics	Fly by wire	SEU/SEL/SEFI	reboot	Matthews (2009)
Railway	GTO[1] IGBT[2]	SEB[6]	Out-of-service	Normand (1997) Asai (2011)
Network	Server	SEU[7]/MCU[8]/SEL[9]	Data corruption/reboot	Slayman (2005), Schindlbeck (2007)
	Router	SEU/MCU/SEL	reboot/address change	Shimbo (2011)
	Data center	SEU/MCU/SEL	Power consumption due to redundancy	Falsafi (2011)
	Core network	SEU/MCU	N.A.	http://www.ntt.co.jp/news2013/1303e/130321a.html
	Power supply (DC-DC converter)	SEB/SEL	Out-of-service	Rivetta (2001)
Super computer		SDC[10]	Unrecognizable wrong calculation/ Power consumption by redundancy	Geist (2012), Daly (2013)
Automobile	Brake by wire	SEU/MCU/SEL	non-stop/sudden stop	Skarin (2007), Baumeister (2012)
	Power steering	SEU/MCU/SEL	stick/unexpected rotation	Nemeth (2012)
	Engine control	SEU/MCU/SEL	sudden acceleration/noop.	Nakata (2011)
	CAN[3]/LIN[4]	SEU/MCU/SEL	Communication error	Lopez-Ongil (2012), Vaskova (2013)
	Pedestrian detection by using GPU[5]	SEU/MCU/SEL	Missing pedestrians	Rech (2013)
	IGBT	SEB	Out-of-service	Shoji (2010), Nishida (2010)
PDA	Smart phone	SEU/MCU	freeze/mail address corruption	Chen (2013)
	Tablet	SEU/MCU	freeze/mail address corruption	
	Desktop PC	SEU/MCU	freeze/mail address corruption	

1: Gate Turn-Off thyristor, 2:Insulated Gate Bipolar Transistor
3:Controller Area Network, 4:Local Interconnect Network, 5: Graphic Processing Unit, 6:Single Event Burnout,7:Single Event Upset, 8:Multi-Cell Upset
9:Single Event Latchup, 10:Silent Data Corruption,

In avionics, TMR is applied to critical components to avoid fatal failures and faults can be found through error flags from TMRs [72]. IGBTs (Insulated Gate Bipolar Transistors) are used in trains [73], automobiles [29–31] and avionics for inverters. They are subject to destructive SEE mode, SEB, due to electron avalanche by a charged particle penetration in pnp structures. SEEs in servers [74, 75] and routers [76] have been main concerns in networks because they use a tremendous number of memories, in particular, SRAMs. Power supplies for network systems like DC–DC converters are also vulnerable to terrestrial radiation in the destructive mode [77].

In large-scale supercomputers like TITAN in ORNL (Oak Ridge National Laboratory), it has been reported that about 10 errors take place in a day [78]. In particular, SDC s by which wrong results are obtained without any error evidences after extremely massive and costly calculations [79, 80], is one of the most serious concern in resilience. DUEs (Detected Unrecoverable Errors) are also major concern in microprocessors, in particular, for the systems that are not allowed to stop. It is said that the rate of DUEs is higher than that of SDC in cache memory [81]. Capture and recovery of SDCs and DUEs impacts is top-priority issue in *real time*, safety critical systems.

Concerns about automobile systems reliability are spreading rapidly and widely, on the brake by wire [82], power steering [83], engine control [84], communication protocol in a car like CAN (Controller Area Network) [85] and LIN (Local Interconnect Network) [86]. GPUs (Graphic Processing Units) or GPGPUs (General-Purpose GPU) are being widely used for many purposes including nodes for supercomputers thank to its high ability in parallel computing. Rech et al. made a neutron beam testing at ISIS for 40 nm GeForce GTX480 and showed high susceptibility of GPUs to terrestrial neutrons [87]. Pedestrian detection at night is one of the most important safety requirements (“Five star” in Euro NCAP rating) where GPUs are used in future.

Even portable digital applications, like smartphones and tablet PCs, have been tested under neutron irradiation [88]. Obviously, no electronic equipment is free from threat due to SEE by terrestrial radiations, these days.

There are a number of fault/error/failure modes that reflect their root-cause mechanisms. Prediction and estimation techniques of faulty conditions and their rates of occurrence have a primary importance in designing devices, circuits and electronic systems. Detection techniques of faulty conditions must be advanced to know the nature of the faults/errors/failures based on their underlying physical mechanisms and to validate the prediction and estimation techniques. Cost-effective resilient techniques may be assigned according to each nature of the failure and application. The following sections introduce some examples of prediction/estimation, detection and classification techniques of fault/error/failures.

3.1.10 Conventional and Advanced Mitigation Techniques

As explained in Sects. 3.1.5 and 3.1.6, an SET takes places only in well/substrate region. Therefore, strategies to mitigate soft-errors in devices or failures in electronic systems boil down to simple strategies as summarized in Table 3.4 with some typical examples [1, 24, 89–98]:

- Restriction of production of faults in wells or acceleration of recombination of electron-hole pairs.

  Implantation of catalyst element like Au in wells is possible choice.

- *Restriction of production or collection of charges in the relevant volume. Triple-well structure is* among such techniques. Volume of the triple well and depth of STI (Shallow Trench Isolation) can be important factor to reduce charge production and collection. Layout of pMOS and nMOS is also one of key design points in order to reduce MCUs in memory cells (see Sect. 3.2).
- Recovery of errors in memory elements. ECC for memories and DICE, BISER (Built-In Soft Error Resilience), BCDMR (Bistable Cross-Coupled Dual Modular Redundancy) for FFs are among such techniques (see Sect. 3.3 for more details).

Table 3.4 Status-of-the-art mitigation techniques known or proposed In the various faulty stages

Hierarchy (Layer)	Key nature	Basic strategy	Examples	Biography
Fault	Faults are produced mainly in a single well-stripe	Apply (well-) structure and/or material which surpress falut production.	Triple well	E. Ibe (2015, review)
			Low resistance material to enhance recombination.	-
Error	Only when the fault-induced-charge corrected to a single node exceeds Q_{crit}, soft-error takes place.	Apply structure /material /circuit which surpresses collection of charge to the data hold/storage node.	SOI[1]	P. Oldiges (2002)
			SOTB[2]	N. Sugii (2010)
			FinFET (TriGate)	N. Serfeit
			UTBB[3]	P. Roche (2013)
		Apply structure /material /circuit which surpresses data flips even when a certain amount of charge collected to the data hold/storage node.	SRAM with additional capacitance to the node.	H. Sato (1999) K. Hirose (2002)
			SRAM with additional resistance between two physical nodes.	K. Hirose (2002)
			STT-MRAM[4]	T. Ohsawa (2013)
Failure	Failures take place only when errors propagate without masking to the final execution stage or outputs.	Apply structure /material /circuit which surpresses propagation of errors to the final execution stage or outputs.	Conventional space/time-redundancy techniques such as DCC[5], DMR[6], RCC[7], and TMR[8]	E. Ibe (2015, review)
		Recover the system before errors result in a failure by detecting errrors at early stage.		
		Recover the system before errors resulting in a failure by detecting faults at early stage.	LABIR[9]	E. Ibe (2011)
			SBRM[10]	N. Wang (2006)
			BICS[11] application	E.H. Nelo (2008)
			SAW[12] application	G. Upasani (2014)
		Apply additional circuits and/or modeles which can recover the system immediately after detecting the falure.	Rapid Recovery Technique in FPGA	K. Shimbo (2015)

1: Silicon on Insulator, 2: Silicon-on Thin Box, 3: Ultra-Thin Body & Box, 4: Spin-Transfer-Torque Magnetoresistive RAM, 5: Duplication-Comparison-Checkpointing, Redundancy

6: Dual Modular Redundanct, 7: Replication-Comparison-Checkpointing, 8: Triple Modular 9: inter-Layer Built-In Reliability,10: Sympton Based Redundant Multithreading

Failures take place when an error propagates to the final output of an electronic system. Therefore mitigation techniques for failures are

- Enhancing masking effect to prevent propagation of errors in the circuitry.
- Space redundancy techniques to cancel out errors. TMR (see Sects. 3.3 and 3.4) and DMR (see Sect. 3.3) are typical methods. DCC (Duplication + Comparison + Checkpointing) [98] is an extended version of DMR. Lock-step operation of dual processors is mainly applied to automobile MCUs (Micro-Control Units).

Power consumption is one of major metrics that determine the mitigation techniques to be applied in large-scale systems like data-centers and supercomputers [53, 58, 59, 79, 80]. "Dark silicon" refers such constraints on performance and reliability due to power consumption [52]. Space redundancy techniques such as TMR and DMR may not be applied to such large big data systems in order to avoid large power consumption.

MCU may cause deactivation of space redundancy technique by simultaneous errors in redundant nodes. Layout design of redundant node must be carefully conducted (see Sect. 3.3).

- Time-redundancy techniques to cancel out errors. RAZOR [99] is one of simple solutions for FFs. RCC (Replication + Comparison + Checkpointing) is a typical time redundancy technique for an extra-large electronic systems from the viewpoint of suppressing power consumption, but concerns are addressed on even such time-redundancy techniques because error rate may exceed checkpointing frequency [79].
- FPGA (Field Programmable Gate Array) s are being widely used in a variety of applications due to their versatility and adjustability in programming [100]. Programs for operation of electronic systems are initially written and fixed in CRAM (Configuration RAM). Errors in CRAM may cause fatal failure due to malfunction of operation. Prompt detection of errors in CRAM and reconfiguration of CRAM are key techniques for reliability in FPGA (refer to Sect. 3.4).

Shimbo et al. have recently developed non-stop recovery CRAM system by using an embedded controller into FPGA array [101]. This kind of approaches seems to be promising in future.

- Reliability for the entire computer system is far more difficult to achieve and challenging because of its complexity and dependence on applications (refer to Sect. 3.5).

3.1.11 Symptom-Driven System Resilient Techniques

Ibe et al. [63, 64] proposed the LABIR approach that is a recovery method driven by a hardware error symptom. Symptom-driven techniques originally meant that predetermined optimization process for isolation of faulty conditions in electronic systems were initiated upon capturing any pretabulated “symptoms” of faulty conditions in OS [102, 103]. This approach utilizes the so-called *fuzzy/intelligent expert systems*. Unlike this approach, Ibe’s proposal is specific only to SEEs which evolve in a well as a detectable symptom. In this scheme, the recovery process is triggered by detecting the symptom before it grows to error/failure and the system is recovered in CPU or application level by means of time-redundancy techniques such as checkpointing and rollback [104]. It can avoid large area, power overheads because it does not apply space redundancy techniques such as TMR. In general, since time-redundancy techniques always apply the same procedure twice and make comparison, speed penalty is inevitable. Since terrestrial neutron-induced soft-errors and resulting symptoms do not take place so often (one per hour even for the largest super computers [105]), this approach can be adopted with a very small speed penalty. Software symptom based approaches are also proposed on the basis that only errors that affect execution of instructions have to be taken care of, while other errors can be left “don’t care” In this section, possible examples for such approaches are introduced.

(i) Hardware symptom

LABIR proposes interactive or communicative mitigation techniques in which a recovery action such as rollback to the checkpoint is triggered when a layer finds any error symptom, not necessarily error or fault itself.

As illustrated in Fig. 3.7, immediately after capturing such a symptom, errors or failures can be removed by a rollback-and-replicate operation in CPU level of the chip. In the case of the example in Fig. 3.7, sense amplifiers are applied to detect slight potential differences between adjacent two p-wells, so that other source of noises like EMI and noise in power supply line [105] propagate in wider area than

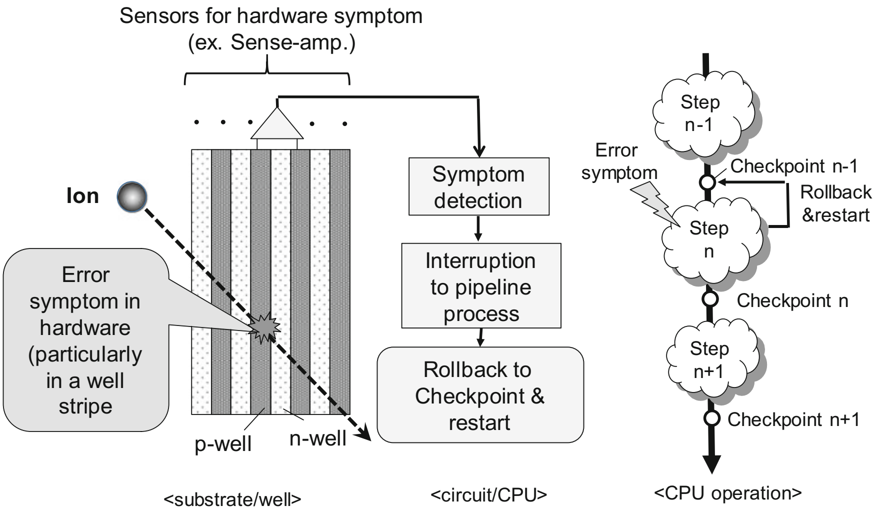


Fig. 3.7 An example of LABIR (inter-LAyer Built-In Reliability)

soft-error over many wells so that they can be eliminated as well by the differential method between adjacent wells. BIST (Built—In Self-Test) [106], Built-In Current (Pulse) Sensor (BICS [90, 107], BIPS)), SAW (Surface Acoustic Wave)-based symptom detector [81], on-chip monitor [108] can be used for such kind of technique. By using BIPS, a pulse propagated from a zone penetrated by a charged particle in p-well can be detected in I_{dd} line by using an embedded current or pulse sensor. In the SAW-based symptom detector, the surface acoustic wave generated by a hazardous event at any location in the semiconductor device is captured by micro-cantilever type detectors. The location of charged particle penetration is calculated by the capture time difference among the detectors. In the on-chip monitor approach, multiple micro-pulse monitors are embedded in the peripheral area of a chip to monitor noises in selected locations.

(ii) Software symptom

Li et al. has proposed a software–hardware co-designed resilient super-scalar system where failure symptom is detected mainly by software and recovery and diagnosis (software bug/permanent error/transient) are made during rollback from checkpoint [109]. Reconfiguration is made in fine grains based on the diagnosis. Fault injection is applied to Solaris-9 OS with the UltraSparc-III ISA. Application and OS crashes and hang-ups are monitored and classified by injected component. These authors have reported that a large fraction of the faults results in OS failures so that and that recovery methods for OSs must be developed.

Hari et al. proposed a symptom detector to detect fault including SDC in software behavior [110].

Wang et al. has proposed SBRM (Symptom Based Redundant Multithreading) where symptom of failure is monitored on software like deadlock, exception handling, miss-instruction in control flow, and error in the cache/translation look-aside buffer [97]. Instructions are executed simultaneously in two threads. Symptom monitoring is applied only to the redundant thread and results in two threads are compared. If the results do not match, an error signal is delivered and restore process is initiated. Checkpointing supported with input replication, symptom detector, and control logic for pipeline flush is used for restore process. Fault injection in the RTL model of Alpha microprocessor is made while SPEC2000 Integer benchmarks operated. By choosing deadlock and exception handling as symptoms, it has been demonstrated that 75% of errors can be recovered with a speed loss of only 2%.

3.1.12 Challenges in the Near Future

Table 3.5 shows future trends, conventional approaches against failures, challenges, and global standards being worked out relevant to the fault/error/failure modes actually encountered in various industry sectors.

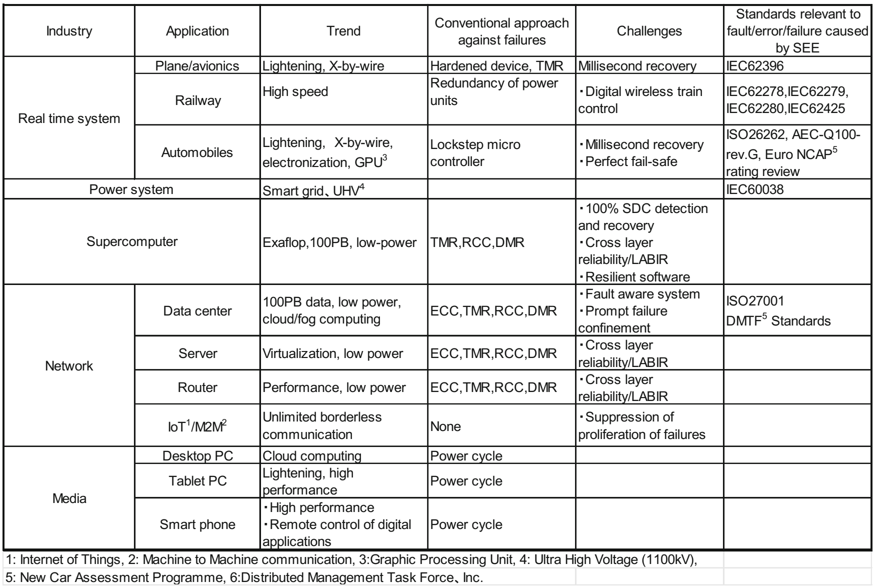
In safety critical system or real-time system like avionics and automobiles, weight saving in structural materials is one of major trends to reduce fuel and power consumption. Usage of GPUs will be extended to much wider areas [87]. *Millisecond recovery* is one of the most challenging themes in real-time systems. In railway systems, further computerization will proceed to realize cost effective, connected, and resilient railway systems [111]. In exa-scale supercomputer system, paradigm shifts in dependability techniques including HW and SW must be realized to avoid failures due to very frequent errors including SDC and DUE (Detected Unrecoverable Error) [112].

In network system as well as supercomputer system, large power consumption will be a serious bottleneck for selection of mitigation techniques.

PDA (Personal Digital Assistance) s or smartphones are being increasingly utilized to control in-house digital appliances remotely. Noise disturbances and malicious attacks must be considered as possible causes of serious accidents [113].

Best combination of mitigation techniques as in LABIR/Cross layer reliability should vary by industry and need to be extensively pursued as well as development of novel key technologies. A list of global standards with their objects and category types such as IEC61508, ISO26262, JESD89A, and so on are listed in Table 3.5.

Table 3.5 Future trends, challenges, and relevant global standards in various industries with respect to fault/error/failure



Industry	Application	Trend	Conventional approach against failures	Challenges	Standards relevant to fault/error/failure caused by SEE
Real time system	Plane/avionics	Lightening, X-by-wire	Hardened device, TMR	Millisecond recovery	IEC62396
	Railway	High speed	Redundancy of power units	・Digital wireless train control	IEC62278,IEC62279, IEC62280,IEC62425
	Automobiles	Lightening, X-by-wire, electronization, GPU[3]	Lockstep micro controller	・Millisecond recovery ・Perfect fail-safe	ISO26262, AEC-Q100-rev.G, Euro NCAP[5] rating review
Power system		Smart grid、UHV[4]			IEC60038
Supercomputer		Exaflop,100PB, low-power	TMR,RCC,DMR	・100% SDC detection and recovery ・Cross layer reliability/LABIR ・Resilient software	
Network	Data center	100PB data, low power, cloud/fog computing	ECC,TMR,RCC,DMR	・Fault aware system ・Prompt failure confinement	ISO27001 DMTF[5] Standards
	Server	Virtualization, low power	ECC,TMR,RCC,DMR	・Cross layer reliability/LABIR	
	Router	Performance, low power	ECC,TMR,RCC,DMR	・Cross layer reliability/LABIR	
	IoT[1]/M2M[2]	Unlimited borderless communication	None	・Suppression of proliferation of failures	
Media	Desktop PC	Cloud computing	Power cycle		
	Tablet PC	Lightening, high performance	Power cycle		
	Smart phone	・High performance ・Remote control of digital applications	Power cycle		

1: Internet of Things, 2: Machine to Machine communication, 3:Graphic Processing Unit, 4: Ultra High Voltage (1100kV),
5: New Car Assessment Programme, 6:Distributed Management Task Force、Inc.

In addition, it is predicted by SRAM soft-error simulation that further scaling may have significant impacts of processor/computer system design [112]. Namely,

- As scaling proceeds, Q_{crit} will decrease below 1 fC or even below 0.1 fC. This causes an extensive increase in area affected by an SEE: For 130 nm design rule, 100 bit × 100 bit SRAM memory matrix can be affected by an SEE, while 1000 bit × 1000 bit SRAM memory matrix would be affected by an SEE beyond 22 nm design rule. When the SRAM has six transistors, the area containing 6M transistors would be affected by an SEE for 22 nm design rule, resulting in unprecedented difficulty in reliability design of processor/computer systems. New breakthrough technologies are obviously required.

3.2 Soft-Error Tolerant SRAM Cell Layout

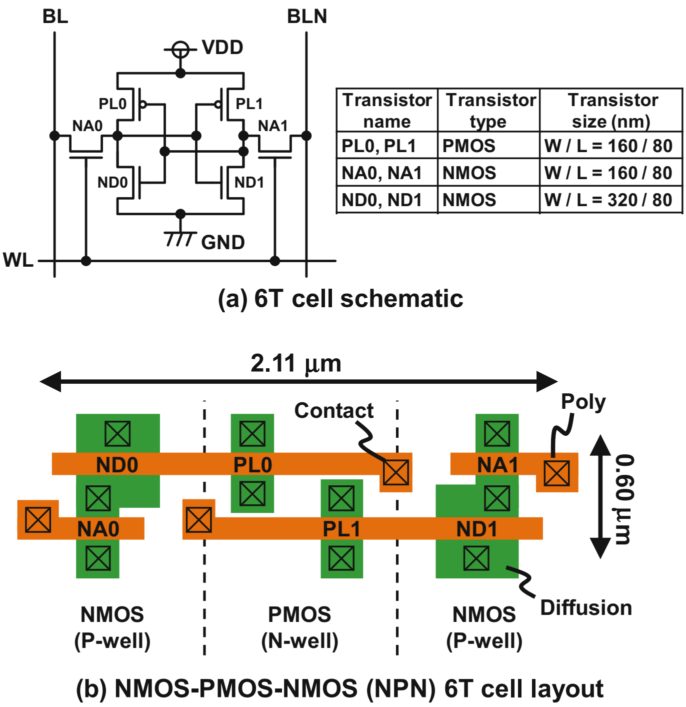
Shusuke Yoshimoto, Kobe University
Masahiko Yoshimoto, Kobe University
Hiroshi Kawaguchi, Kobe University

3.2.1 Introduction

Nano-scaled integrated circuits are susceptible to particle-induced single event effect (SEE) because of their low signal charge and noise margins [31, 65, 113, 114]. Particularly the effect of multi-cell upsets (MCUs), in which a single event results in simultaneous errors in more than one memory cells, have been closely investigated. MCUs are caused by collection of charges produced by secondary ions in neutron-induced nuclear reaction [1]. The ratio of MCUs to single event upsets (SEUs) is predicted to increase drastically in nano-scaled SRAMs [2, 33, 43, 114].

Figure 3.8 shows a schematic and a layout of a general 6T SRAM cell with a typical 65-nm CMOS logic design rule. In the design, the sizes of the transistors are relaxed to suppress threshold voltage variation so that the cell area is about twice as large as a commercial 65-nm 6T cell [115]. The 6T cell consists of PMOS load transistors (PL0, PL1), NMOS driver transistors (ND0, ND1) and access transistors (NA0, NA1). A wordline (WL) and two bitlines (BL, BLN) are horizontally and vertically connected among cells, respectively. In the layout of the general 6T cell, the PMOS transistors are centered in the memory cell; this structure is called an NMOS-PMOS-NMOS (NPN) layout hereafter.

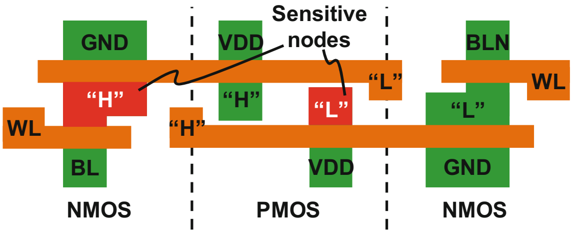
Figure 3.9 shows sensitive nodes in the general 6T cell layout: a low-state (“L”) PMOS diffusion and a high-state (“H”) NMOS diffusion. We have observed that the NMOS has a four-times larger SEU cross section than a PMOS for a wide range of



Transistor name	Transistor type	Transistor size (nm)
PL0, PL1	PMOS	W / L = 160 / 80
NA0, NA1	NMOS	W / L = 160 / 80
ND0, ND1	NMOS	W / L = 320 / 80

Fig. 3.8 **a** Schematic and **b** NMOS-PMOS-NMOS (NPN) layout of a general 6T SRAM cell

Fig. 3.9 Sensitive nodes in a general NPN 6T SRAM cell



supply voltages (see Fig. 3.10) [116]. The simulation results come from an iRoC TFIT soft-error simulator [117] with a database of a generic 65-nm bulk CMOS process [118].

In this subsection, we present a neutron-induced soft-error rate simulation tool and two types of soft-error tolerant SRAM cell layouts. Results show that the proposed memory cell layouts favorably affects their reliability; they enhance the effectiveness of single error correcting-double error detecting ECC (SEC-DED ECC).

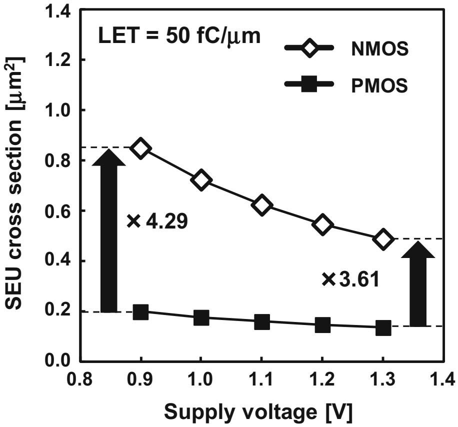


Fig. 3.10 SEU cross sections of NMOS and PMOS with a twin-well 65-nm process calculated using the iRoC TFIT simulator [116, 117]

3.2.2 *Neutron-Induced Soft-Error Rate Simulator*

Figure 3.11 illustrates a flow chart of our neutron-induced soft error simulator [116] using PHITS, the Particle and Heavy Ion Transport Code System [119]. The input data for PHITS are neutron spectrum data, device structure data, and nucleus reaction models. The cosmic-ray neutron spectrum is calculated using an Excel-based Program for calculating Atmospheric Cosmic-ray Spectrum (EXPACS) [120], as shown in Fig. 3.12. The device structure is constructed as presented in Fig. 3.13.

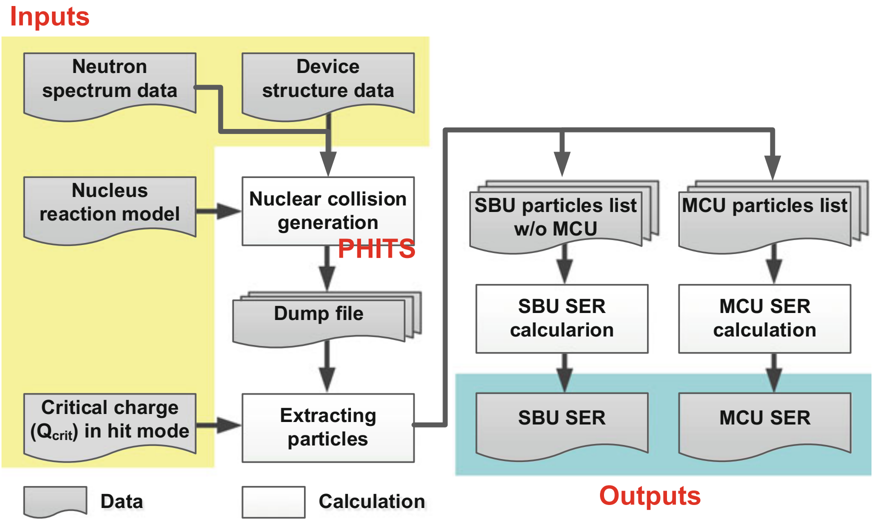


Fig. 3.11 Flow chart of the soft-error rate simulator [116] using PHITS [119]

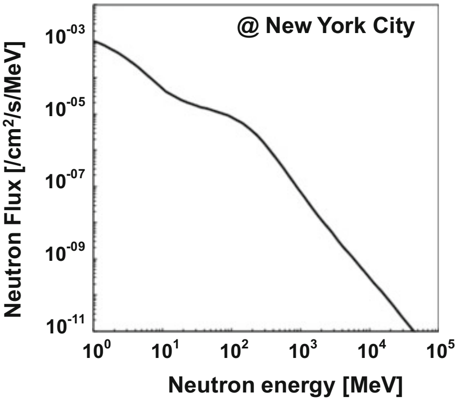


Fig. 3.12 Cosmic-ray neutron flux normalized to ground level in New York City. Flux is calculated with EXPACS [120]

The device structure includes the cell property (width, height, and position of sensitive nodes), a cell-to-cell pitch in a cell array, and data patterns. The cell height, width, and position of the sensitive nodes are modeled as presented in the figure. The diffusion area is derived from the transistor width and the cell height. The clearances between diffusion edges are all equal.

The PHITS can export secondary particle dump files presented in Fig. 3.14. In our simulation, the dump files are generated in respect to NMOS and PMOS sensitive volumes in an SRAM cell. The dump file includes nucleus reaction IDs (event numbers), atomic weight, geometry points (X, Y, Z), velocity vectors (dX, dY, dZ), and energy in the point (E). The deposit energy (E_{deposit}) is calculated with the dump files in the respective sensitive nodes. The deposit charge (Q_{deposit}) is calculated using the following equation, in which e is the elementary charge:

$$Q_{deposit}[\mathrm{C}] = \frac{e}{3.6} \times E_{deposit}[\mathrm{eV}] \tag{3.5}$$

When a secondary particle deposits more charge than the critical charge (Q_{crit}) to at least one memory cell, that particle is classified as a single event upset (SEU) particle. Finally, single-bit-upset and multi-cell-upset soft-error rates (SBU and MCU SERs) are calculated at every SEU particle event.

3.2.3 PMOS-NMOS-PMOS (PNP) 6T Cell Layout

The proposed 6T cell is designed as a PMOS-NMOS-PMOS (PNP) layout in Fig. 3.15. The NMOS-centered 6T layout has the same transistors as the general one. The WLs and the BLs are assigned in horizontal and vertical directions, respectively.

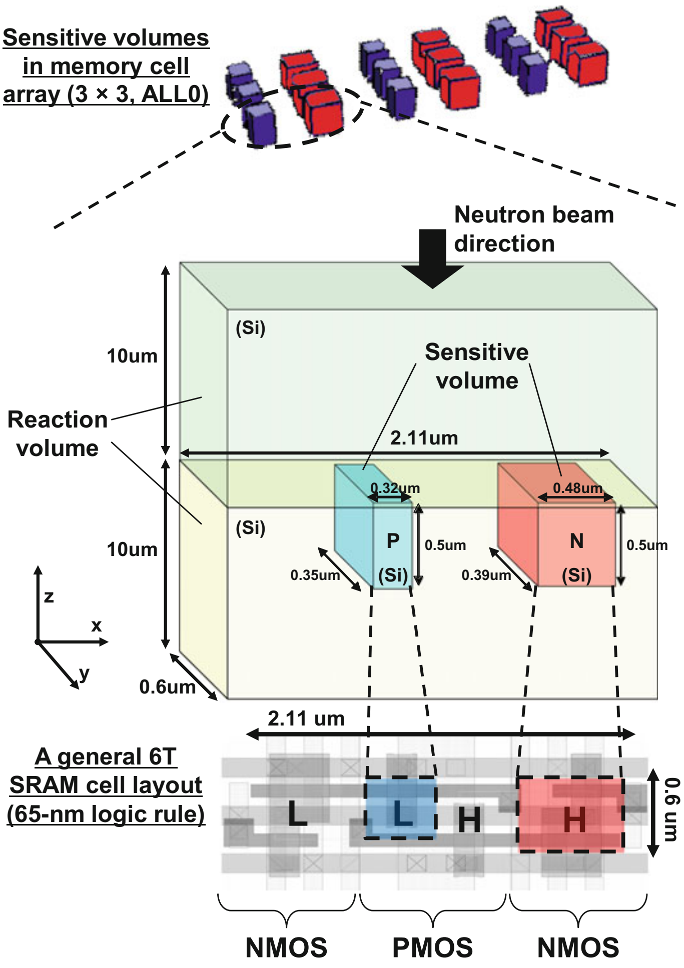


Fig. 3.13 Device structure based on a 65-nm general 6T SRAM cell layout (logic rule basis) [120]

Figure 3.16a shows an SRAM cell array using the general NPN 6T layout. In the conventional 6T SRAM, the sensitive NMOS nodes are in the same P-well in the horizontal direction; horizontal upsets can be easily incurred. In contrast, the proposed PNP 6T cell can lower a horizontal MCU rate because the NMOS-centered layout can separate the horizontally adjacent NMOS sensitive nodes with the N-well as shown in Fig. 3.16b.

The proposed layout has the same schematics and the cell area on the 65-nm logic rule basis, so that the proposed design can be implemented only by replacing its cell layout. Note that shared contacts, which are commonly used in an industrial SRAM rule, cannot be applied to the proposed 6T cell layout. This drawback incurs a certain area overhead in the SRAM rule basis design.

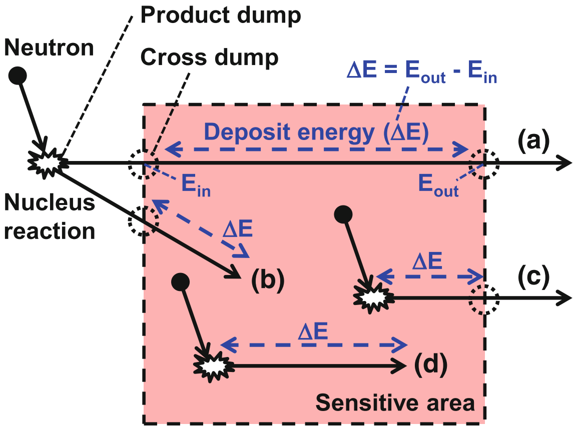


Fig. 3.14 Product-dump and cross-dump data related to secondary ions: **a** crossing the sensitive area, **b** entering the area, **c** leaving the area, and **d** remaining in the area

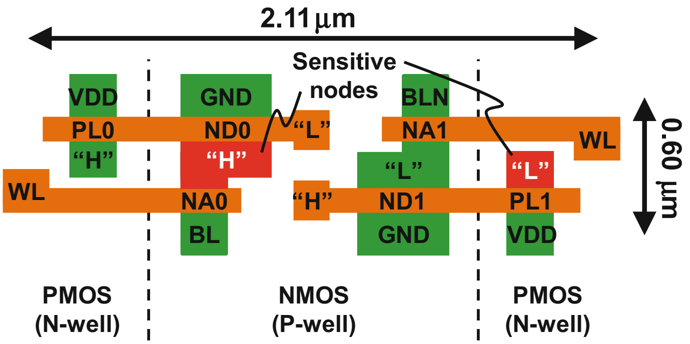


Fig. 3.15 Layout of a proposed PMOS-NMOS-PMOS (PNP) 6T cell

We designed and fabricated 1-Mb SRAM test chips consisting of 256-Kb macros of four types (NPN layout with twin well, PNP layout with twin well, NPN layout with triple well, and PNP layout with triple well). Figure 3.17 presents an experimental setup for a neutron-accelerated test. The neutron irradiation experiment was conducted at The Research Center for Nuclear Physics (RCNP), Osaka University. Spallation neutron beam generated by the 400-MeV proton beam irradiates a board under test (BUT) 7892-mm far from a tungsten target, on which three sample chips are placed in a BUT, for 30 h. The neutron flux is normalized to 13 cph/cm^2 above 10 MeV at ground level in New York City [7], which incorporates scattering effect [121], attenuation effect [44], and board screening effect [122].

As presented in Fig. 3.18, an MCU SER in the vertical direction is called MCU$_{BL=1}$ in this paper, and an MCU SER in the horizontal direction is called

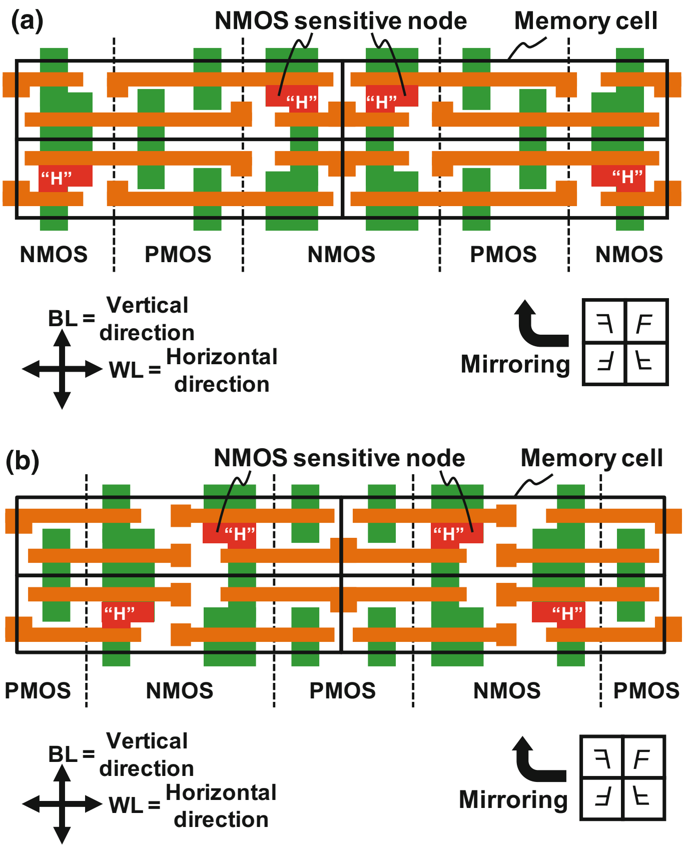


Fig. 3.16 SRAM cell arrays using **a** general NPN 6T cell layout and **b** proposed PNP cell layout

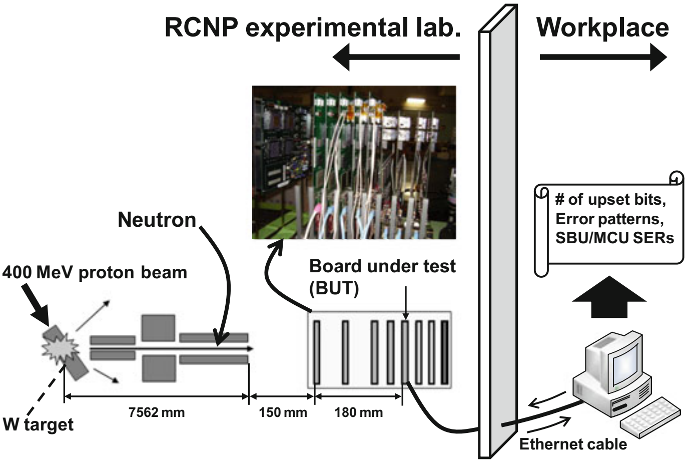


Fig. 3.17 Setup for neutron-accelerated test

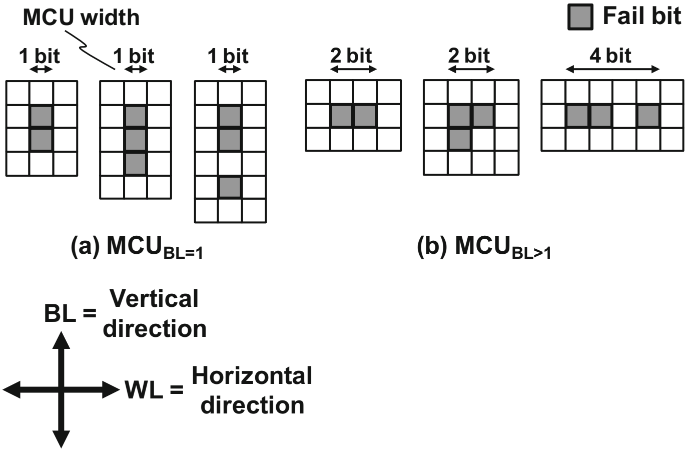


Fig. 3.18 Multiple-cell-upset patterns: **a** MCU$_{BL=1}$ and **b** MCU$_{BL>1}$ are defined respectively by vertical fail bits in a same column and by horizontal fail bits in two or more columns

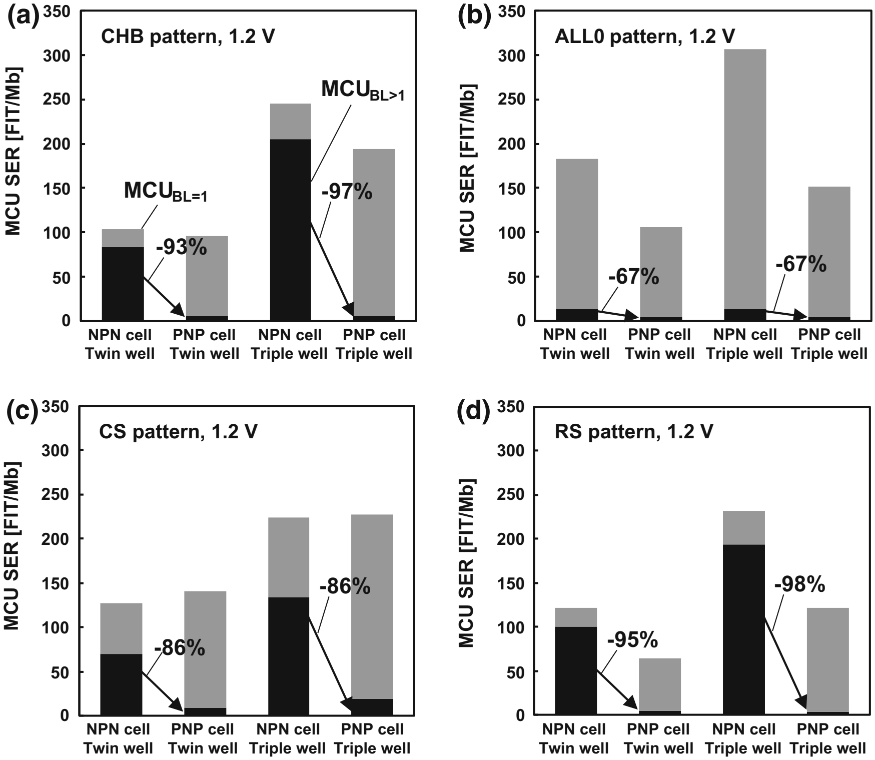


Fig. 3.19 Data patterns: **a** checkerboard (CHB), **b** all zero (ALL0), **c** column stripe (CS), and **d** row stripe (RS)

$MCU_{BL>1}$. The $MCU_{BL>1}$ is more important for designers to adopt the interleaving and/or ECC strategy.

Figure 3.19a–d illustrate measured MCU SER in the four data patterns at the supply voltage of 1.2 V. When using the CHB (checkerboard), CS (column stripe), and RS (raw stripe) patterns, the $MCU_{BL>1}$ in the PNP 6T SRAM can be suppressed by 86–98% compared to the general NPN layout. The proposed PNP layout separates NMOSs from adjacent ones in the horizontal direction, which reduces the $MCU_{BL>1}$ SER. In the ALL0 (all zero) pattern, the $MCU_{BL>1}$ even in the general NPN cells is low in nature because the sensitive nodes are not horizontally adjacent in a single bitline. As a result, only 67% improvement is observed in the MCU SER. The proposed PNP layout with the dual-well structure achieves $MCU_{BL>1}$ SERs of 5.78, 4.58, 9.48, and 4.70 FIT/Mb in the CHB, ALL0, CS and RS patterns and the PNP layout with the triple-well structure achieves $MCU_{BL>1}$ SERs of 5.78, 4.58, 18.96, and 3.13 FIT/Mb.

3.2.4 N-P Reversed 6T Cell Layout

To scale CMOS transistors down to a 45-nm process or less, it is important to use compressive and tensile strain engineering for PMOS and NMOS, respectively, thereby increasing the drain current. Particularly, for a PMOS, embedded SiGe (eSiGe) in a source and drain boosts its saturation current (I_{satp}). The strain engineering is thereby more effective for PMOS (I_{satp}) than for NMOS (I_{satn}). Current enhancement using eSiGe strain for the PMOS increases more effective with the process scaling: +30% and +45% in 45-nm and 22-nm processes [123, 124]. Figure 3.20 shows the trend of the saturation current ratio of an NMOS to a PMOS

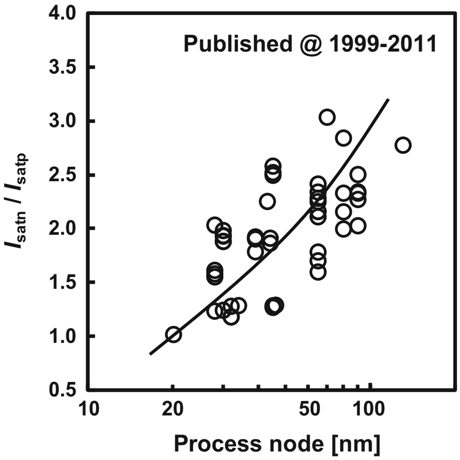


Fig. 3.20 Trend in the n-to-p saturation current ratio, I_{satn}/I_{satp}, in 1999–2011

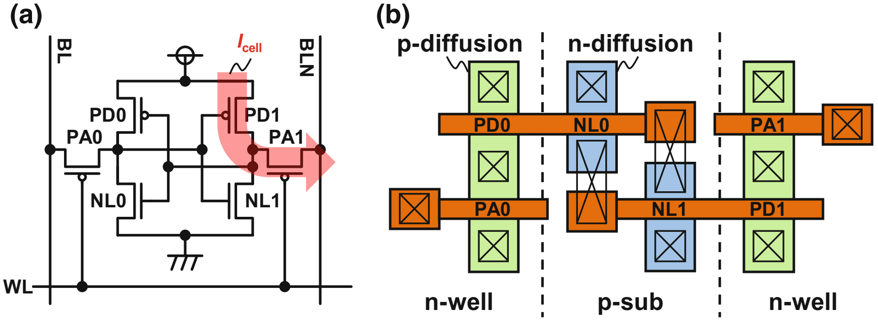


Fig. 3.21 **a** Schematic, and **b** layout of the proposed N-P reversed 6T SRAM cell. Cell current (I cell) flows through PMOS load and NMOS access transistors in read operation

(=$I_{\text{satn}}/I_{\text{satp}}$) along with a process node [125, 126]. The ratio approaches becomes unity when I_{satp} is comparable to I_{satn} at a 22-nm node. As previously described, the SEU cross section of the PMOS is 1/4 of that of the NMOS. Therefore, the conventional 6T cell suffers from the shortcomings of the soft-error vulnerability in the NMOS driver transistors. To cope with this NMOS problems and to leverage the PMOS benefit, we propose using PMOS access and driver transistors instead: an N-P (NMOS-PMOS) reversed structure. Soft-error tolerance is enhanced in the proposed N-P reversed 6T SRAM cell in future 22-nm node or advanced ones.

Figures 3.21a and 3.21b depict a schematic and a layout of the proposed NMOS-PMOS (N-P) reversed 6T SRAM cell, respectively. The 6T cell consists of NMOS load transistors (NL0 and NL1), PMOS driver transistors (PD0 and PD1), and PMOS access transistors (PA0 and PA1). The number of transistors and the poly-gate alignment are similar as the conventional one, although the N- and P-diffusions are swapped. The shared contacts are applicable to both 6T cells.

Therefore, the proposed cell has no area overhead over the conventional one. In a read operation, either bitline (BL or BLN in Fig. 3.21a) is pulled up by a cell current flowing through a PMOS access transistor. Generally, the read current of the proposed cell is degraded because I_{satp} is smaller than I_{satn}. However, as presented in Fig. 3.20, the saturation current ratio of I_{satn} to I_{satp} becomes smaller in the scaled process. Moreover, the random dopant fluctuation of the PMOS is less than that of the NMOS. Consequently, the cell current of the proposed cell will be larger than that of a conventional cell.

The device structure includes the cell property (width, height, and position of sensitive nodes), a cell-to-cell pitch in a cell array, and data patterns. The cell height, width, and position of the sensitive nodes are modeled as presented in Fig. 3.22. The ratio of the cell height to the cell width is set as 3.5. Each transistor width is doubled from the process node to suppress threshold voltage variation. The diffusion area is derived from the transistor width and the cell height. The clearances between diffusion edged are all equal. The parameters are presented in Table 3.6.

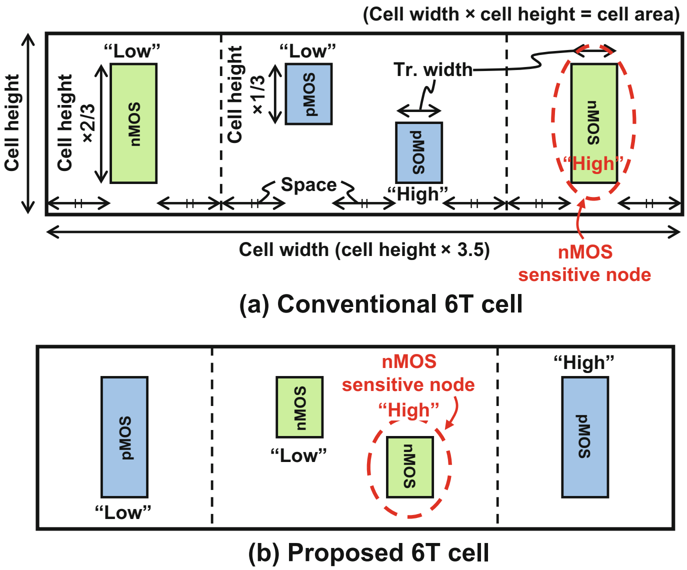


Fig. 3.22 Models of SRAM cell width, height, and positions of sensitive nodes in 22-nm to 130-nm processes using parameters in Table 3.6

Table 3.6 Size and position parameters for PHITS simulations in Fig. 3.22

	Process node [nm]					
	22	32	45	65	90	130
Cell area [μm^2]	0.081	0.156	0.283	0.537	0.947	1.796
Cell height [μm]	0.152	0.211	0.284	0.392	0.520	0.716
Cell width [μm]	0.533	0.739	0.995	1.371	1.820	2.507
Tr. width [μm]	0.044	0.064	0.090	0.130	0.180	0.260
Space [μm]	0.051	0.069	0.091	0.122	0.157	0.210

Figure 3.23a–d show neutron-induced soft-error simulation results obtained using CHB, ALL0, CS, and RS patterns. Although the critical charge is decreasing, the SBU SER is also decreasing with process scaling thanks to the smaller critical area. The MCU SER exhibits a similar tendency at the 65-nm and less nodes.

The proposed N-P reversed cell has 50% smaller NMOS diffusion area in our definition. Therefore, its SBU and MCU SERs are reduced by 11–51% and 34–70%, respectively, at the 22-nm node. Particularly for the column stripe pattern, the MCU SER is improved by 70% (but the SBU SER is decreased by only 11%) because NMOS diffusions in the conventional cells share the same p-substrate in the vertical direction and vertical MCUs occur easily. However, in the row stripe

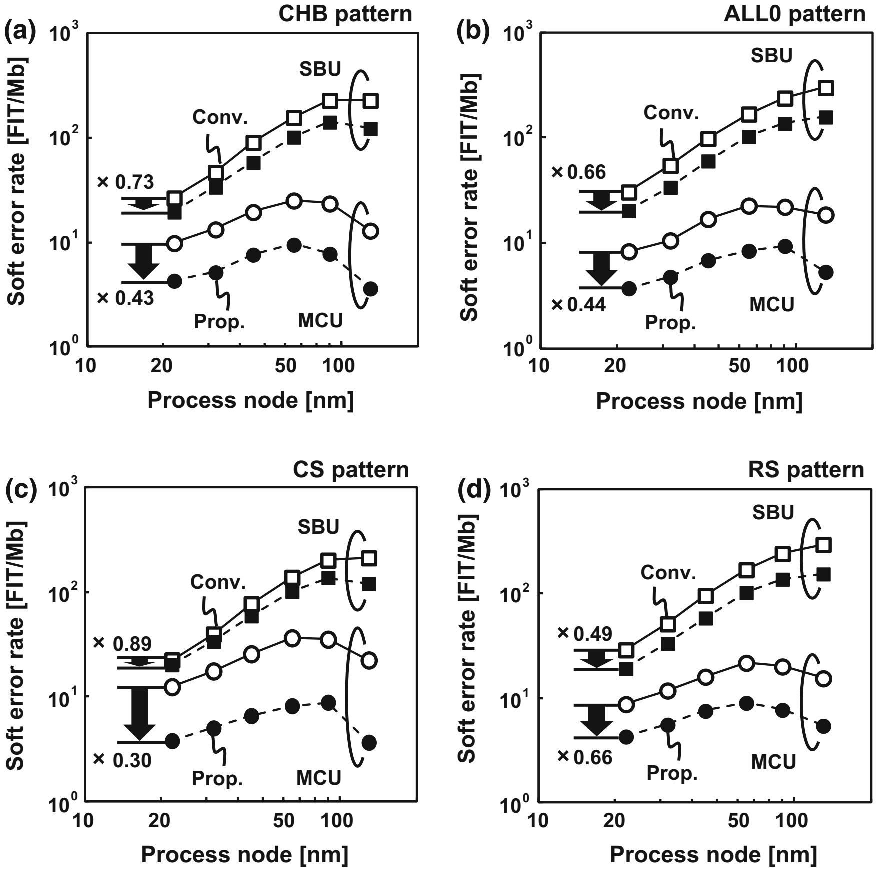


Fig. 3.23 SBU and MCU SERs of conventional and proposed cells in the **a** CHB, **b** ALL0, **c** CS, and **d** RS patterns

pattern, the MCU SER improvement is the smallest, 34% (but the SBU SER improvement is the largest, 51%), because the distance from a sensitive NMOS node to another in the conventional cells is the longest among the four patterns.

3.3 Radiation-Hardened Flip-Flops

Kazutoshi Kobayashi, Kyoto Institute of Technology
Jun Furuta, Kyoto Institute of Technology

Radiation-hardened flip-flops (FFs) are used to mitigate unwanted flips by radiation strikes. Here we first deal with several redundant FFs and then move to non-redundant ones. Finally, we discuss device/process/circuit-level mitigation techniques for nano-scaled CMOS.

3.3.1 Approaches for Radiation-Hardened Flip-Flops

It is mandatory to prevent soft errors in storage circuits such as SRAMs, latches and flip-flops. Aggressive process scaling relieves soft errors rates per bit. But semiconductor chips are utilized in the fields demanding high reliabilities such as automotive, aerospace and medical devices. It is mandatory to reduce soft error rates as small as possible.

Redundant flip-flops mitigate soft errors to prepare extra circuit elements. Usually, three storage cells are prepared. It is possible to correct an error in a storage cell by majority voting. Since redundant flip-flops have large area, delay and power overhead, non-redundant flip-flops are used to reduce soft error rates by adding extra circuit elements with smaller penalties.

Device and process approaches are also effective to reduce soft error rates. Silicon-On-Insulator (SOI) is one promising candidate. Compared with conventional bulk technologies, SOI is strong against soft errors since Buried-Oxide (BOX) layers prevent charge collections.

Those mitigation techniques are introduced in this section.

3.3.2 Redundant-Structured Flip-Flops

3.3.2.1 Triple Modular Redundancy Flip-Flop

Triple Modular Redundancy Flip-Flop (TMR-FF) mitigates soft errors by majority voting. Three storage elements are prepared. Even if one of them is flipped due to a radiation strike, it outputs the correct value by majority voting. Figure 3.24 depicts a typical TMR-FF which contains tripled latches and a majority voter. If one wishes to build a TMR-FF utilizing cells available out there, the majority voter can be constructed with combinations of conventional logic gates as shown in Fig. 3.25a, or using a PDK (Process Design Kit) that includes a special logic cell typically called MAJ as shown in Fig. 3.25b.

TMR-FF is immune from Single Bit Upsets (SBUs) but can fail against Multi-Cell Upsets (MCUs). If two storage elements are flipped, it outputs an incorrect value. Due to the aggressive process scaling, the probability of MCUs is getting higher and higher [127]. It is caused by the fact that *ranges of* radiation particles are not scaled, while *the sizes of* storage elements are scaled. If a particle strikes a storage node, generated charge is shared with neighbors. Parasitic bipolar effects [128] also elevate well potential, which turn on parasitic bipolar transistors. To mitigate MCUs, layout-level techniques are effective.

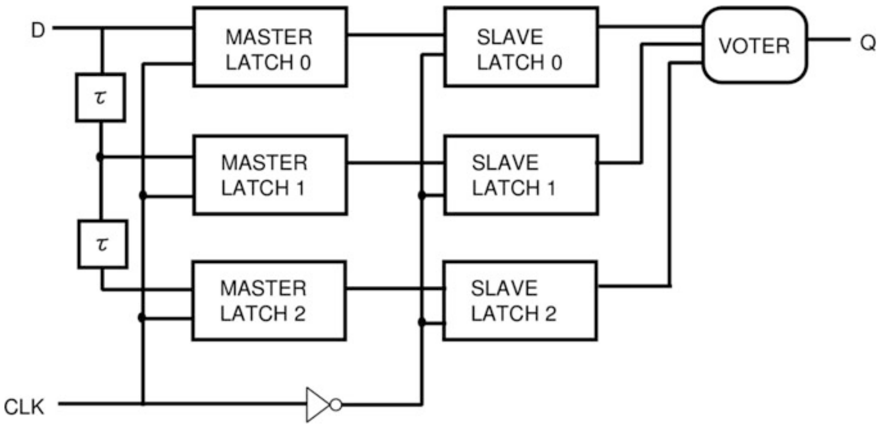


Fig. 3.24 Triple-modular-redundancy flip-flop. Delay elements (τ) prevents to store incorrect data in three redundant latches from input

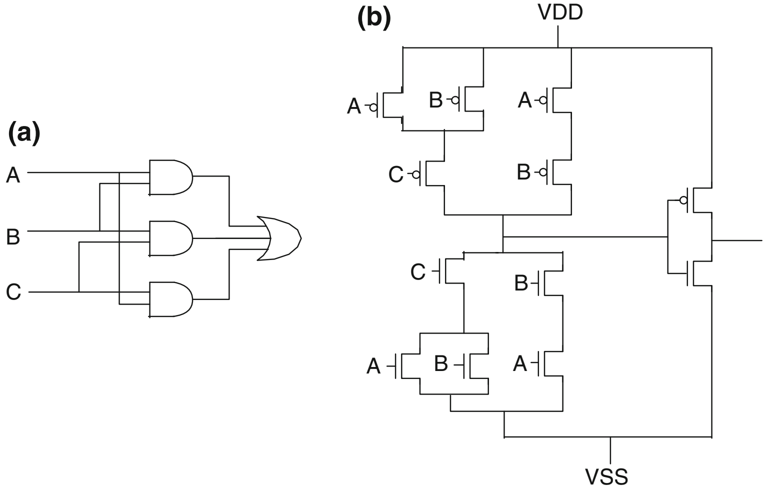
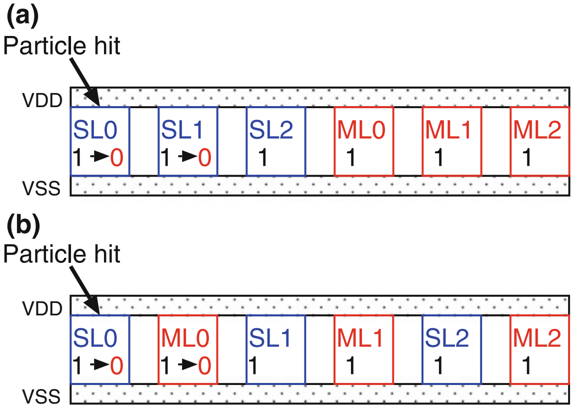


Fig. 3.25 Majority voters implemented by logic gates (**a**) and MAJ logic cell (**b**)

Figure 3.26 shows an example which interleaves the storage elements in the TMR-FF that must not be flipped at the same time [129]. If two storage elements are flipped, it outputs an incorrect value. Due to the aggressive process scaling, the probability of MCUs is getting higher and higher [127]. It is caused by the fact that ranges of radiation particles are not scaled, while the sizes of storage elements are scaled. If a particle strikes a storage node, generated charge is shared with neighbors. Parasitic bipolar effects [128] also elevate well potential, which turn on parasitic bipolar transistors. To mitigate MCUs, layout-level techniques are effective.

Fig. 3.26 Interleaving storage elements on the TMR-FF that must not be flipped at the same time. **a** w/o interleaving. **b** w/ interleaving. SL0 and ML0 denote Master Latch 0 and Slave Latch 0 in Fig. 3.24



3.3.2.2 Dual-Interlocked Storage Cell (DICE) Flip-Flop

DICE stands for Dual-Interlocked storage cell. It is utilized in SoCs for High-Performance Computers (HPCs) [46, 130, 131].

The DICE structure as shown in Fig. 3.27a mitigates soft errors by duplicating latches implemented by the half C-elements and the clocked half C-elements as shown in Fig. 3.27b. The input and output signals of these half C-elements have cross-coupled connections to be automatically recovered from a flip on a single node. On the other hand, redundant FFs such as TMR, BISER [132] and BCDMR [133] mitigates soft errors by majority voting among three storage cells, in which a flipped node is left until the next clock signal is injected to supply an unflipped new value.

Compared with these majority-voter-based structures, the DICE structure is area-efficient since latches are not triplicated but duplicated.

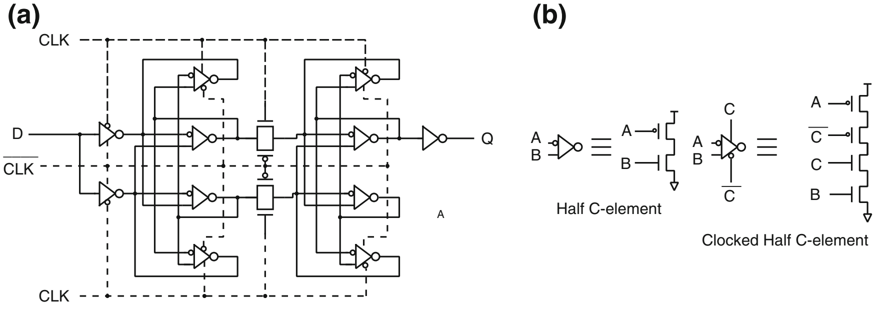
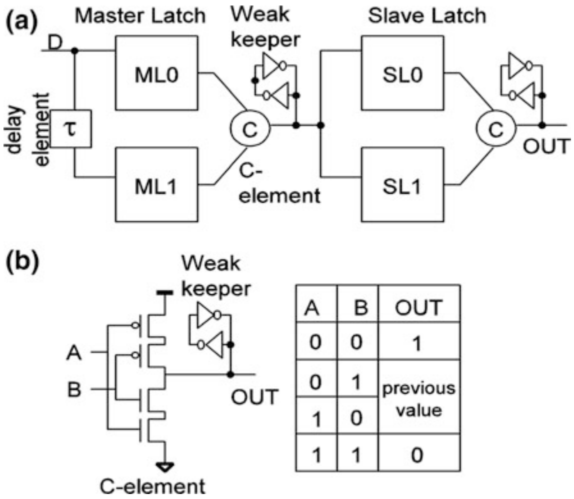


Fig. 3.27 DICE FF schematic. DICE has four cross-coupled half C-elements. If a C-element is flipped, other three restore the original stored value



A	B	OUT
0	0	1
0	1	previous value
1	0	
1	1	0

Fig. 3.28 BISER schematic

3.3.2.3 Dual-Modulared-Redundancy Flip-Flop

Several dual-modulared-Redundancy (DMR) FFs are developed to achieve equivalent SEU tolerance to the TMR-FF. The DMR FFs explained here have two latches, a cross-coupled inverter called a keeper and C-elements. Compared with the TMR-FF with triplicated latches and voters, the DMR FFs has less area/power/delay penalties. Built-In Soft Error Resilience (BISER) FF [132] is developed by Intel and Stanford Univ. It consists of dual-modulated latches, C-elements and weak keepers as shown in Fig. 3.28a. As shown in Fig. 3.28b, the C-element and the weak keeper keep the previous value even when one of duplicated latches is flipped. Therefore, BISER FF eliminates an unexpected flip caused by an SBU.

Bistable Cross-Coupled Dual Modular Redundancy (BCDMR) FF [133] is a modified version of the BISER FF with the functionality which was developed at Kyoto Univ. and Kyoto Inst. of Tech. It has duplicated C-elements with cross-coupled connection as shown in Fig. 3.29, which protects the slave latches from simultaneous flips caused by an SET in the C-element. In the BISER structure, duplicated slave latches are simultaneously flipped when a particle hits on the C-element and an SET pulse is transferred to the slave latches. The probability to capture the SET pulse is increased according to the clock frequencies. On the other hand, in the duplicated C-elements of the BCDMR structure, the SET pulse is only captured by one of the slave latches. Table 3.7 compares area, delay and power of BISER and BCDMR normalized by a conventional DFF. BCDMR FF has the same area with BISER. At 0.5 V, the delay of BISER FF becomes much slower than BCDMR.

In neutron-accelerated tests, BCDMR FF showed over 100× more error resilience than non-redundant FF at clock frequencies up to 100 MHz thanks to the

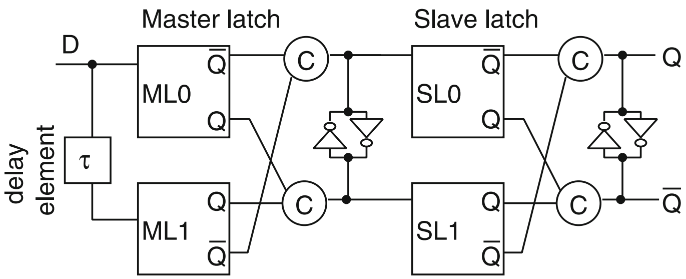


Fig. 3.29 BCDMR schematic

Table 3.7 Area, delay and power of BISER and BCDMR normalized by a conventional DFF

	BISER			BCDMR		
	Area	Delay	Power	Area	Delay	Power
1.2V	3.00	1.47	2.15	3.00	1.45	2.20
0.5V	3.00	1.96	2.39	3.00	1.57	2.23

stability given by the cross-coupled dual C-elements [129], while BISER FF became more susceptible to SET at higher clock frequencies [129].

3.3.3 Non-redundant-Structured Flip-Flops

In this subsection, several non-redundant-structured FFs which pay less area/power/delay penalties but with less robustness against SEUs compared with redundant ones will be introduced.

3.3.3.1 Reinforcing Charge Collection Flip-Flop

The Reinforcing Charge Collection (RCC) FF [134] was proposed by Intel with dummy transistors to increase critical charge. Figure 3.30 shows an RCC latch schematic. There are two pairs of dummy CMOS transistors between n1 and n2. They are laid out to minimize victim-to-reinforcing diffusion separation as depicted in Fig. 3.31. The OFF device's diffusion, referred as victim diffusion, collects charge that can flip the stored value. On the other hand, the ON devices diffusion, reffered as reinforcing diffusion, collects charge that can reinforce the stored value. In RCC, those diffusions are laid out besides the dummy gates DN1 and DN2.

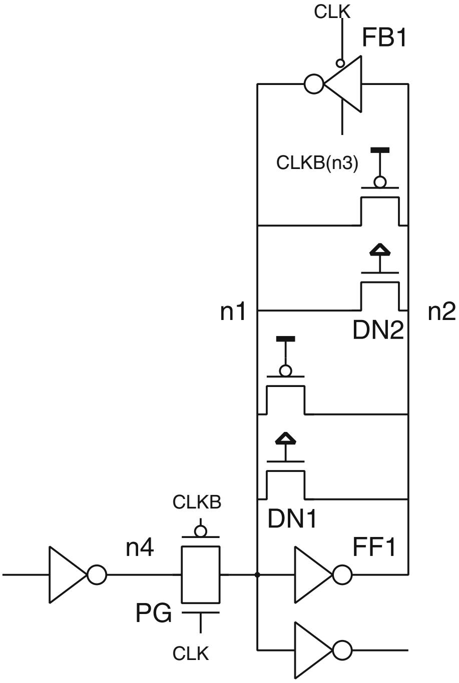


Fig. 3.30 RCC schematic

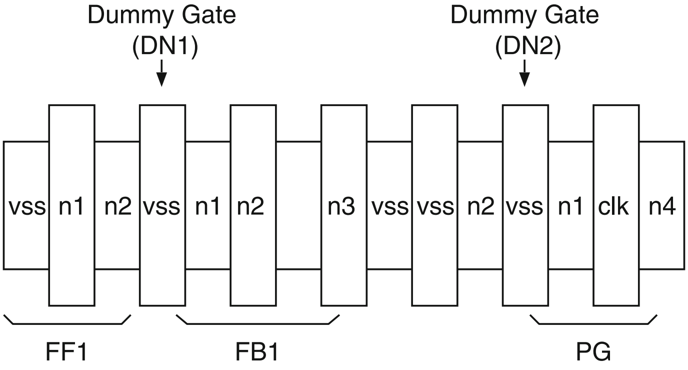


Fig. 3.31 RCC layout for N diffusions

3.3.3.2 Hysteresis Flip-Flop

Hysteresis Flip-Flop (HY-FF) was developed by Broadcom and Vanderbilt Univ. It is a non-redundant FF with additional weak keepers that restricts unwanted flips by radiation strikes [135]. Figure 3.32 shows a schematic diagram of HY-FF. It is

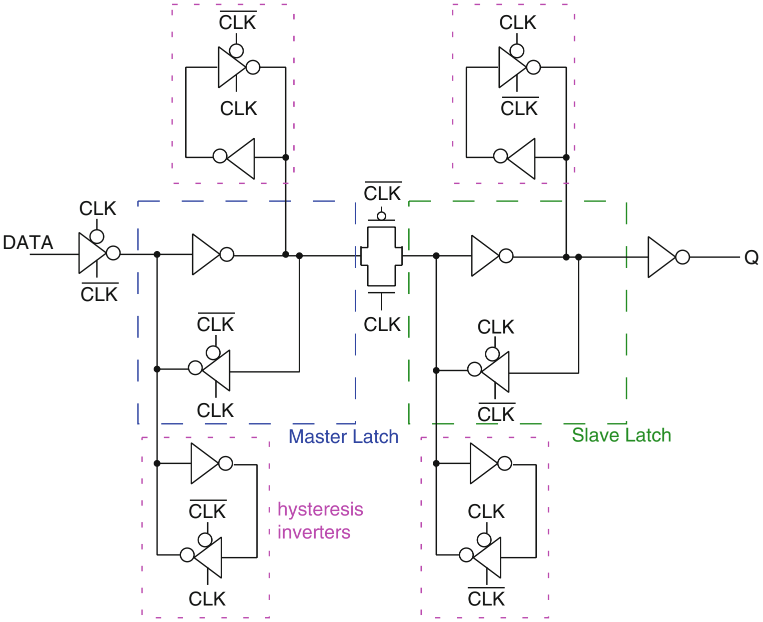


Fig. 3.32 Hysteresis Flip-Flop schematic

non-redundant but its area penalty is relatively large. It is reported in [136] that its radiation hardness is 5 × compared with a non-redundant FF and the area of the pulsed hysteresis latch is 108% of a non-redundant FF.

3.3.4 Device/Process/Circuit-Level Mitigation Techniques for Nano-Scaled CMOS

For nano-scaled CMOS technologies, MCUs, or multiple upsets of signal nodes in close vicinity caused by a single strike of energetic particles, have become more and more pronounced since ranges of radiation particles such as neutrons or alpha particles are not scaled while signal nodes are becoming closer to each other. MCUs may cancel out mitigation effect by redundancy; If two storage elements out of the two among the three in TMR are flipped, it becomes a fault. In nano-scaled CMOS down to 45 or 28 nm, device or process level mitigation techniques are therefore getting increasing attention. Fully Depleted Silicon-On-Insulator (FD-SOI) is one of promising candidates to supplant conventional bulk technologies to cope with. We introduce two FD-SOI processes which have thin BOX (Buried OXide) layers named 65-nm Silicon On Thin BOX (SOTB) and 28-nm Ultra-Thin Body and BOX

(UTBB). We also introduce a non-redundant mitigation technique adequate for an anti-soft-error process such as FD-SOI.

3.3.4.1 Thin BOX FD-SOI Technologies

FD-SOI suppresses the short-channel effect (SCE) and process variations. Two semiconductor companies in Japan and in France are developing similar FD-SOI technologies with thin BOX layers. Sugii et al. from LEAP (Low-Power Electronics Association & Project), an industry consortium in Japan, have developed a 65 nm Thin BOX FD-SOI technology called SOTB [137, 138].

Figure 3.33 shows a cross section of an SOTB transistor. The thickness of the BOX layer is only 10 nm thick so it is possible to control the threshold voltages through backgate biases. Kamohara et al. developed an SoC integrating a 32 bit microprocessor and SRAMs for Internet of Things (IoTs) [139]. ST Microelectronics is also developing another 28 nm Thin BOX FD-SOI technology named UTBB [140]. The thickness of the BOX layers is 25 nm, which is 2.5 × thicker than SOTB's, and has less controllability of threshold voltages than SOTB. Jaquet et al. have implemented a dual-core ARM A9 processor with 2.66 GHz enabled by forward body biases in the UTBB process [141].

FD-SOI technologies have a distinct advantage in soft error immunity, because the bulk Si substrate is separated from the active SOI (Silicon-On-Insulator) regions. Charges generated in the substrate do not penetrate the BOX oxide. SOI The results obtained by the author's group in spallation neutron irradiation experiment have shown that a conventional TGFF (Transmission Gate FF) on SOTB has the 16 × lower SER than a similar TGFF built-in bulk Si [142]. In addition to that, it has been found out that redundant FFs such as DICE, BCDMR and TMR built-in SOTB have no errors during the neutron irradiation [142].

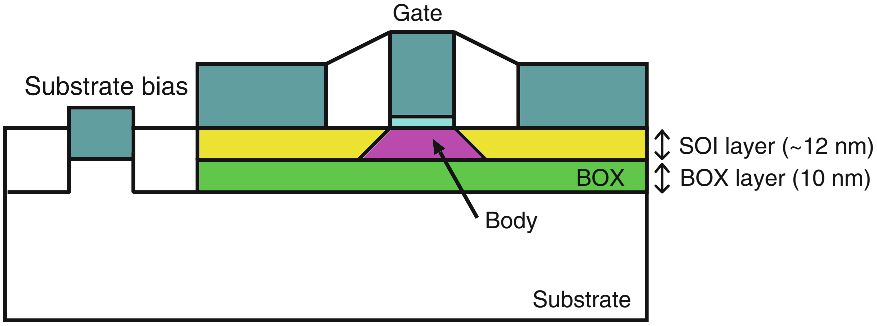


Fig. 3.33 Cross section of a Silicon on Thin BOX Transistor

Fig. 3.34 Relationship between particle energy and Critical charge

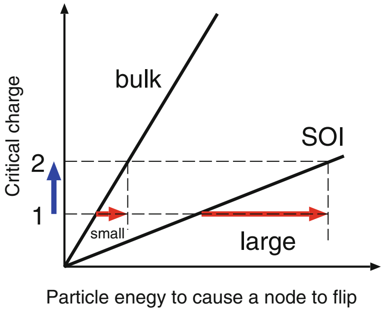
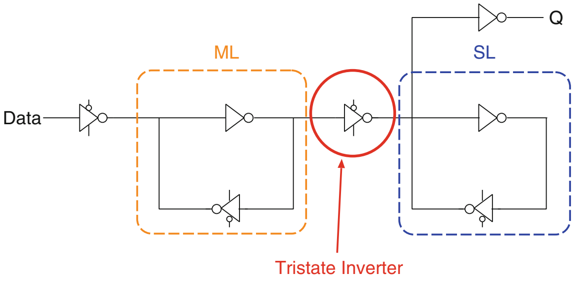


Fig. 3.35 Tristate-Inverter FF



3.3.4.2 Mitigation Technique Without Redundancy

In the low-SER technologies such as FD-SOIs, non-redundant circuits are enough to suppress SERs. Thus, redundant circuits may not be required. In such technologies, slight difference in critical charge (Q_{crit}) makes a lot of difference in threshold energy of particles as qualitatively shown in Fig. 3.34. Thus, layout or circuit-level techniques to increase Q_{crit} without redundancy are good candidates. Figure 3.35 is a non-redundant FF called Tristate-Inverter FF (TIFF) that replaces the transmission gate between master and slave latches on TGFF with a tristate inverter. The area of TIFF is only 5% larger than a Transfer-Gate FF (TGFF), but the critical charge of TIFF is larger than that of TGFF. TIFF has better SERs than TGFF. We fabricated a test chip by 65 nm bulk and FD-SOI processes. Table 3.8 shows the error probabilities by alpha irradiation of TIFF and TGFF. In bulk, the error probabilities are almost equivalent, while in FD-SOI the probability of TIFF is 0.6× of that of TGFF.

Table 3.8 Error probabilities by alpha irradiation normalized by bulk TGFF

Process	bulk		FD-SOI	
FF	TGFF	TIFF	TGFF	TIFF
Error Probability	1.0	1.0	0.049	0.030

3.4 Soft-Error-Tolerant Reconfigurable Architecture

Yukio Mitsuyama, Kochi University of Technology

Masanori Hashimoto, Osaka University

Takao Onoye, Osaka University

Hiroyuki Kanbara, Advanced Science, Technology & Management Research Institute of KYOTO

Hiroyuki Ochi, Ritsumeikan University

Kazutoshi Wakabayashi, NEC

Hidetoshi Onodera, Kyoto University

3.4.1 Soft Errors on Reconfigurable Architecture

Recently, the reliability of reconfigurable devices is drawing attentions, since implementing mission-critical applications with high reliability on reconfigurable devices is highly demanded for saving NRE (Non-Recurring Engineering) costs. Especially, soft errors are one of serious concerns threatening reliability of mission-critical applications. In reconfigurable devices, the reliability of the configuration memory is often considered to be more critical than that of the computed data in data/pipeline registers, since an SEU in the configuration memory damages the functionality until the configuration data is reloaded again; we will refer to this as a permanent error. In the majority of terrestrial applications, on the other hand, requirements for radiation hardness may not be as stringent as in space applications but can vary to such an extent that a single processor architecture would be hard to accommodate.

Coarse-grained reconfigurable architectures (CGRA) have been studied to fill the performance gap between FPGA and ASIC by reasonably limiting application domains and programmability. From reliability point of view, CGRA is inherently superior in soft error immunity to FPGA, since the amount of configuration bits is by orders of magnitude smaller than that of FPGA. Several groups have so far reported on CGRAs with reliability consideration [143–145].

Thus far, while CGRAs have been extensively discussed (e.g., [146–148]), their adoption for commercial use has been limited compared to FPGAs. FPGAs have dominated wide areas of applications that are rather popular despite of their large power dissipation and chip area for two major reasons. For one thing, CGRA is basically composed of an array of ALUs (Arithmetic Logical Units) handling multi-bit operands, and is therefore suitable for data-path implementation but not for efficiently implementing one-bit operations that are often used in flag computation, conditional branching and state machines. RTL (Register Transfer Level) designers and existing behavioral synthesis tools for ASIC and FPGA commonly synthesize data-path circuits that are controlled by state machines. The incompatibility with state machine implementation is, therefore, a significant problem that has prevented CGRA from being widely used. Another reason is that no CGRAs have been provided so far with the full benefit of IP reuse or the standard ANSI C/C ++ source codes available for designs. To overcome this issue, several CGRA architectures compatible with state machine implementation have been proposed [149–151]. To expand the application domains of CGRAs, an architecture having high compatibility with design automation tools and high flexibility that allows trade-offs between reliability, performance and cost has been highly demanded.

3.4.2 Proposed Reconfigurable Architecture

3.4.2.1 Design Concept

The concept of our reconfigurable architecture, which we call Flexible Reliability Reconfigurable Array (FRRA), is based on the above-mentioned recognition of the requirements for flexible reliability in architecture design and compatibility with behavioral synthesis.

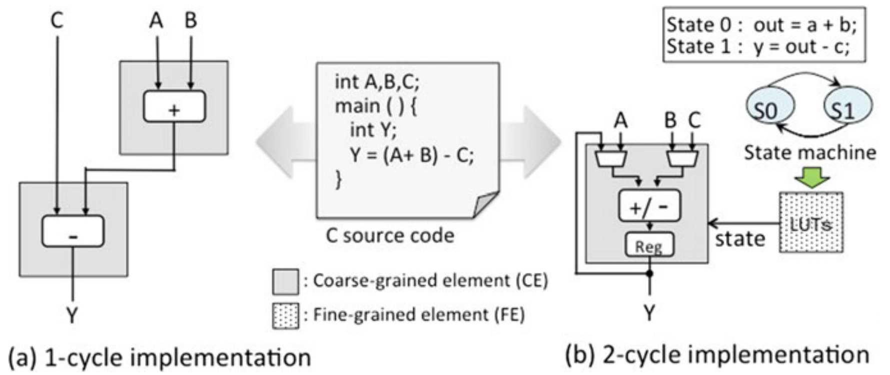
(1) Flexible reliability in architecture design

Reliability requirements depend on the application and operating environment, and hence, there is a growing demand for design scheme that would allow flexible choice of countermeasures to prevent reliability degradation. A reconfigurable device is suitable for a spatial redundancy based soft-error-tolerant design, which is applied in mission-critical applications with area costs. In order to achieve the desired level of reliability in a reconfigurable device, it is useful to be able to subject all its basic elements to trade-off between the sensitivity to soft errors and the chip area.

According to the reliability classifications against soft errors, each basic element of our reconfigurable architecture supports several operation modes. When an application is implemented on our reconfigurable device, the operation modes of each basic element are defined by our design tools, which can consider the trade-off between soft-error resilience and hardware cost.

(2) Compatibility with behavioral synthesis

Compatibility with behavioral synthesis requires architectural supports that help provide a trade-off between latency and resource usage (area). Figure 3.36 demonstrates how a C program can be implemented in one cycle and in two cycles. Our architecture supports not only one-cycle implementation of Fig. 3.36a but also multi-cycle implementation. In the two-cycle implementation of Fig. 3.36b, one coarse-grained processing element including two multiplexers and a register, and fine-grained elements for implementing a state machine are necessary. Dynamic



```
int A,B,C;
main ( ) {
  int Y;
  Y = (A+ B) - C;
}
```

C
A
B
+
-
Y
C source code
□ : Coarse-grained element (CE)
▨ : Fine-grained element (FE)
(a) 1-cycle implementation
State 0 : out = a + b;
State 1 : y = out - c;
S0
S1
State machine
A
B
C
+/ -
Reg
state
LUTs
Y
(b) 2-cycle implementation

Fig. 3.36 Examples of implementations with different latency

reconfiguration of the processing element is controlled by the state machine, which has two states, S0 and S1. In order to show a simple example of two types of implementations, Fig. 3.36 uses a small C program, and may not have been able to show an obvious trade-off between latency and area. In case of a practical C program, a large trade-off could be obtained. Such a trade-off between latency and area obtained by various implementations enables various types of desirable specifications.

In order to achieve this trade-off, the following elements are required: fine-grained elements to implement state machines, coarse-grained elements to perform various types of data processing with dynamic reconfiguration depending on the state signal, register files to save temporal data, and large memories to store large bulk data. Here, although an embedded CPU could be used to control the state of coarse-grained elements, we took the option of using the fine-grained elements built in the chip for pursuing low-latency state control. With these elements, behavioral synthesis allows designers to explore the solution space and select an implementation that satisfies the requirements of the design.

3.4.2.2 Architecture Design Overview

The proposed architecture is composed of coarse-grained elements as ALU clusters, fine-grained elements as LUT (Look-Up Table) clusters, register blocks called as REG clusters, and memory blocks called as MEM clusters, where the basic element is noted as cluster. Figure 3.37 shows an example of cluster array, in which an LUT block is composed of a number of LUT clusters. When an application is mapped on the proposed architecture, data-paths are assigned to ALU clusters. Meanwhile, state machines and one-bit operations are assigned to LUT clusters. The temporal intermediate data across the different states could be stored in REG clusters.

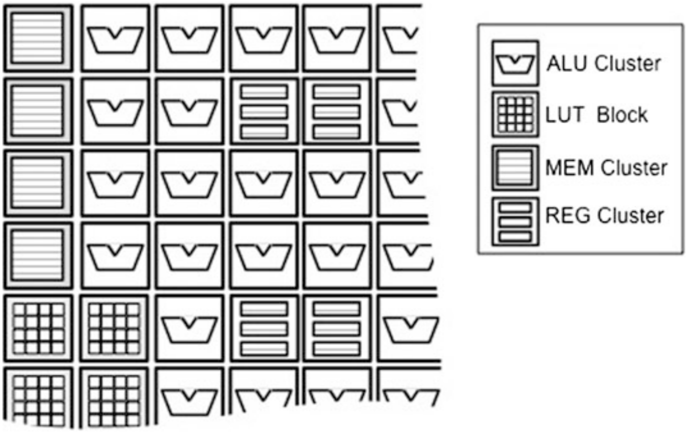


Fig. 3.37 Example of heterogeneous cluster array based on the proposed architecture

The proposed reconfigurable array architecture has two global signals: context signal and state signal. Both of these global signals are generated by designated LUT clusters. The inter-cluster connections are changed according to the context signal, which switches the mapped application or algorithm. An ALU cluster changes its functionality and data-path/flag operands according to the broadcast state signals, while the inter-cluster interconnection is unchanged. All the inter-cluster routings to provide data to clusters are fixed for all the states, and each ALU cluster selects a few data as operands, depending on the state, from all the data delivered to the ALU cluster. Also, a REG cluster selects input data and changes write address depending on the state signal, since the store of intermediate data depends on the state. On the other hand, the functionalities of LUT and MEM clusters are unchanged by the state signal.

ALU, LUT and REG clusters all have an inner structure with three cells as illustrated in Fig. 3.38, while the execution modules (EM) in the cells are specific to each of them. The EMs for ALU, LUT and REG clusters are ALU, LUT and register file, respectively. On the other hand, an MEM cluster includes a single SRAM macro, and hence the structure inside the cluster is different. Several LUT clusters are organized in a two-dimensional array forming a LUT block. ALU, REG, and MEM clusters and LUT blocks are placed in a two-dimensional array. The details of each cluster are explained in Sect. 3.4.2.3.

3.4.2.3 Details of Reconfigurable Architecture

As shown in Fig. 3.38, an ALU cluster consists of a reconfigurable cell unit for processing various types of operations, a redundancy control unit (RDU) for flexible reliability, a comparing and voting unit, switches and wires. An RCU is

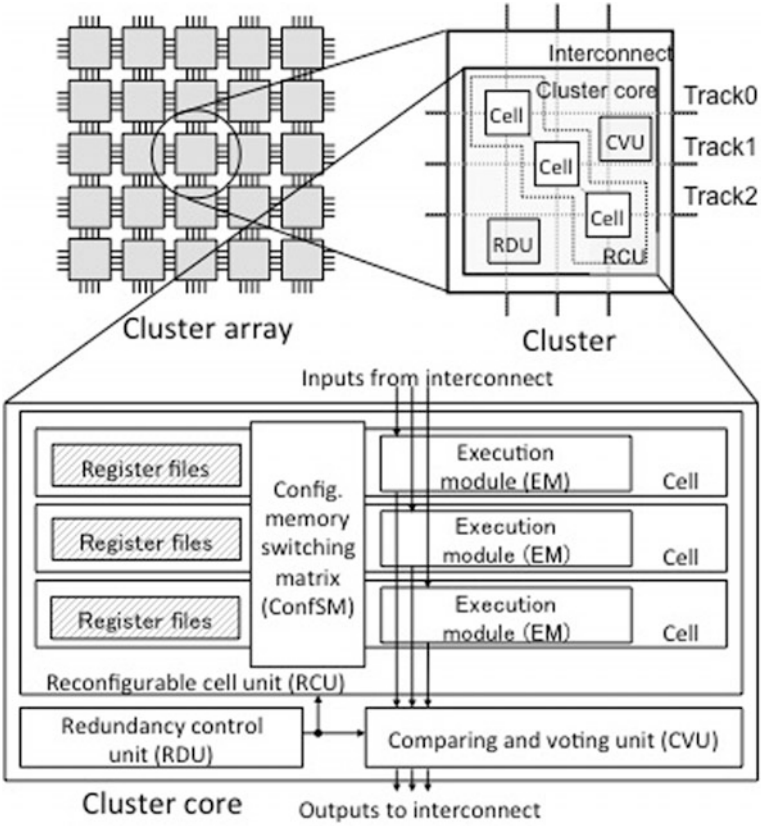


Fig. 3.38 The inner structure of ALU, LUT and REG clusters. Cluster-to-cluster interconnection is shown as well

composed of a configuration memory switching matrix (ConfSM) and three cells, each of which contains an execution module (EM), register files for storing configuration bits, and voters. In EM, arithmetic operations including multiplication, logic operation, and shift operation are performed.

The cluster interconnection has three tracks (Track 0–2), and each cell inside a cluster is placed on one of them. Thus, each cell in a cluster can be connected to the cells in adjacent clusters on the same track. The interconnection also has a diagonal track, connecting cells within one cluster. Switches to control these interconnections are implemented by multiplexers.

The cell architecture of ALU cluster is illustrated in Fig. 3.39. In order to implement dynamic reconfiguration with a small area overhead, configuration bits are divided and stored in three types of register files: instruction register file (InstRF), interconnection register file (InterRF), and constants register file (ConstRF). As mentioned earlier, instructions for ALU are locally stored in the

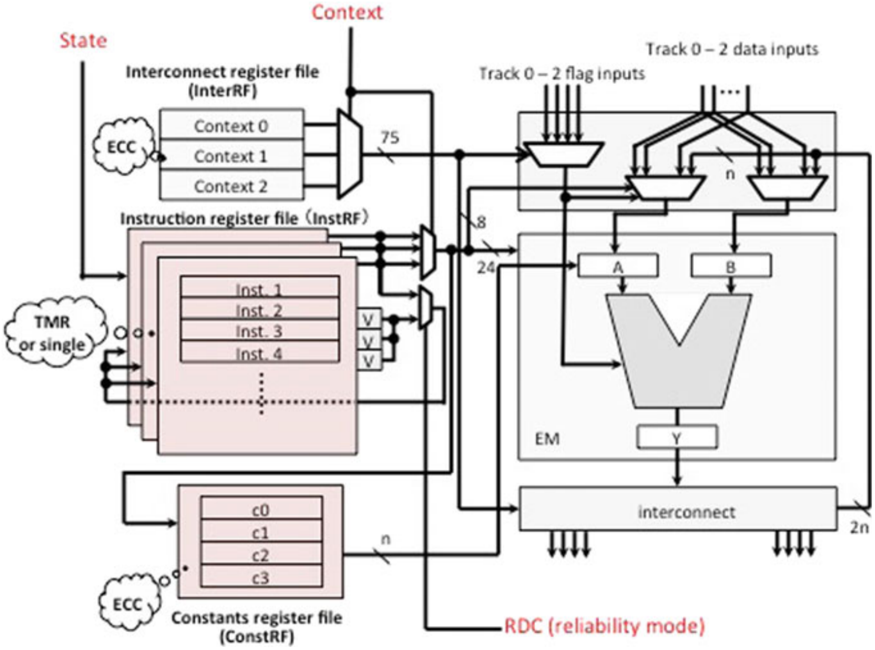


Fig. 3.39 Architecture of cell in ALU cluster

cluster, where an instruction for ALU represents a set of ALU configuration bits for a single state. On the other hand, the configuration bits for inter-cluster connection stored in InterRF are fixed for all the states in each context. In this paper, InterRF is implemented so that it can store three contexts. ConstRF is used to store up to four constants that are required in the application, and one of the four constants is selected by the 2-bit signal from InstRF. This implementation has been selected for area reduction because not all instructions need constants in most applications.

In this architecture, as pointed out earlier, an InstRF consisting of a larger number of words can accommodate a larger state machine, which enables trade-offs between the area and latency. However, as the number of ALU instructions stored in InstRF becomes larger, the silicon area of ALU cluster increases, and the area overhead originating from the unused words of InstRF tends to be significant. The detail of this trade-off is described in [152].

To attain soft error immunity, InterRF and ConstRF are protected with an error correction code (ECC). The selected code is single error correction/double error detection (SEC/DED) Hamming code. For every read of InterRF and ConstRF, the error corrected bits are regularly restored in InterRF and ConstRF to prevent error accumulation. In addition, three contexts of InterRF and four constants of ConstRF are restored by re-writing the data itself through another SEC/DED encoder/decoder in rotation. On the other hand, three InstRFs is implemented with bitwise triple

Table 3.9 Reliability levels in ALU cluster

Operation mode	Redundancy		SEU in InstRF	SEU in EM	SET in EM	Utilization		Throughput per cluster
	InstRF	EM				#contexts	#cells	
TMR	3	3	D&R	D&R	D&R	3	3	1
SMS	3	1	D&R	D	ND	1	1	3
SMM	1	1	ND	D	ND	3	1	3

D&R: Detection and Recovery, D: Detection, ND: Non-Detection

modular redundancy, since the path from the state signal to the register file output includes only a voter and its delay is small. This small delay is important, since this delay is necessarily included in the critical path. Three InstRFs can also be used as three contexts of configuration memory for dynamic reconfiguration without any soft error immunity. This is the reason why ECC, which would require an ECC decoder having large delays, was not selected for InstRF.

As summarized in Table 3.9, ALU cluster supports three operation modes: triple modular redundancy (TMR), single modular with single context (SMS), and single modular with multi-context (SMM). These operation modes also offer different capabilities of dynamic reconfigurability (number of contexts) and throughput per cluster.

TMR, in which both InstRF in a cell and data-paths in three cells are triplicated as shown in Figs. 3.38 and 3.39, provides the highest soft-error immunity. Meanwhile, in SMS, only InstRF is triplicated but the data-path is singular. In both TMR and SMS, an SEU occurring in the InstRF will be repaired when the next configuration clock is given, since the voted value is rewritten to the register file in every configuration clock cycle. Here, the configuration clock signal is given to the InstRF separately from the system clock. This configuration data is stored with bitwise TMR, and therefore, multiple SEUs in different bits will also be corrected when the next configuration clock is given. On the other hand, in SMM, the voters are disabled, and three contexts are stored independently using three InstRFs, each of which is included in individual cells. With this implementation, users can flexibly choose the operation modes, depending on the importance of SEUs in InstRF and SEU/SET in EM.

The detailed architecture of LUT, REG, and MEM clusters are described in [152]. REG, LUT, and MEM clusters support reliable and regular modes. In each operation mode, register files for storing configuration bits and EMs, which are LUT, register file, and SRAM macro in LUT, REG, and MEM cluster respectively, can be adopted individual reliability level. In order to achieve different levels of reliability to soft-errors, each operation modes of each cluster are defined by our design tools [153, 154], which can consider the trade-off between soft error resilience and hardware cost. The overview of our design tools is presented in Sect. 3.4.3.

3.4.3 Design Tools for Our Reconfigurable Architecture

3.4.3.1 Reliability Programming by Selective TMR

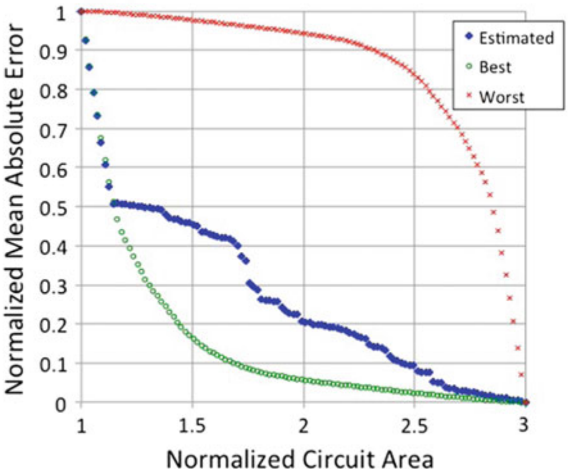
A study on SEU mitigation for FPGAs revealed that there are configuration bits that should be protected with higher priority and proposed to adopt costly TMR selectively [155]. Similarly, it is expected that selective TMR is also effective to CGRAs, and thus we developed an architecture that has capability of applying either TMR or non-TMR modes for each cluster as explained in Sect. 3.4.2.

In order to implement a given circuit to the proposed architecture with highest possible reliability under limited reconfigurable fabric, it is important to find vulnerable operations that should be triplicated with higher priority without time-consuming fault simulation. For this purpose, we developed a method to determine the priority to be triplicated [153, 154].

In the method, we assume that vulnerability, v, of an operation in a given DFG (Data Flow Graph) is modeled by a linear equation $v = \mathbf{w} \cdot \mathbf{a}$, where **a** is a vector of feature values of the operation (e.g., type of operation, distance to primary output), and **w** is a weight vector, in which each element corresponds to the element in the vector **a**. By analyzing some sample circuits in an application domain, we obtained examples of **a** vectors and corresponding v values, and from these **a**-v pairs, we found **w** that approximates model equation $v = \mathbf{w} \cdot \mathbf{a}$ using a generalized inverse matrix [153] or simulated annealing method [154]. Once **w** is found, we can obtain the priority for triplication of operations in a given DFG since we can estimate v of each operation.

Figure 3.40 shows the area-vulnerability trade-off of implementations of a 1024-point FFT [154]. The horizontal axis represents normalized circuit area, in other words, hardware cost. The entire TMR and non-TMR correspond to 3.0 and

Fig. 3.40 Area-vulnerability trade-off of application implementations



1.0 respectively, and a partial TMR in between. The vertical axis represents mean absolute error (MAE) at the output data-stream induced by soft-errors. The definition of MAE is given by

$$\mathrm{MAE} = \frac{1}{N}\sum_{i=1}^{N}|x_i - \tilde{x}_i|, \tag{3.6}$$

where N is the number of words in the output data, x_i and $\tilde{x}_i$ are the i-th word of actual output and error-free output, respectively. The “Best” and “Worst” plots show the entire design space obtained by exhaustive search and fault simulation, and the “Estimated” plots show the obtained implementation using our method. When the all clusters adopt TMR mode, the amount of mean absolute errors should be zero. According to the obtained priority, a small portion of triplication effectively reduces the vulnerability.

3.4.3.2 Reliability-Oriented C-Based Design Flow

Figure 3.41 shows the reliability-oriented C-based design flow for the dependable VLSI platform, which consists of the reliable processor [156] and the reliable reconfigurable array. An application can be written in ANSI-C language. After partitioning the whole operation to the processor and the reconfigurable array, the C source code for the reconfigurable array is translated to an RTL description. This behavioral synthesis is performed by Cyber Work Bench [157, 158] whose algorithm is optimized for our CGRA. The RTL description is then mapped and place-and-routed on the reconfigurable array.

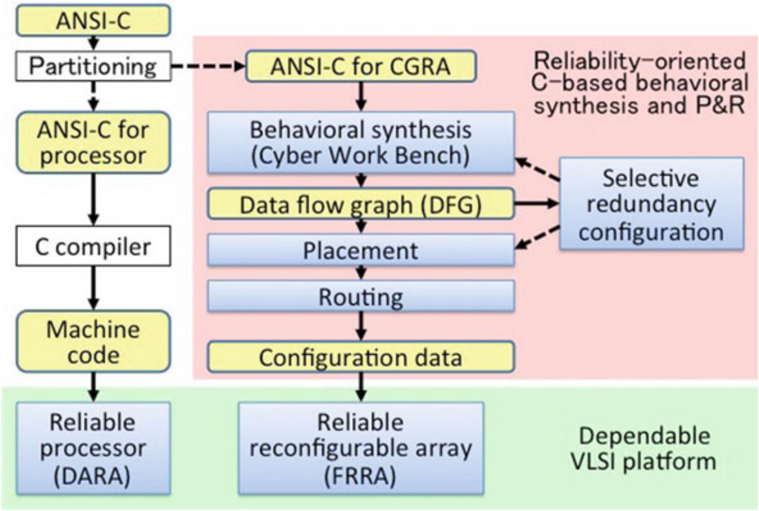

ANSI-C
Partitioning
ANSI-C for CGRA
Reliability−oriented C−based behavioral synthesis and P&R
ANSI-C for processor
Behavioral synthesis (Cyber Work Bench)
Selective redundancy configuration
Data flow graph (DFG)
C compiler
Placement
Routing
Machine code
Configuration data
Reliable processor (DARA)
Reliable reconfigurable array (FRRA)
Dependable VLSI platform

Fig. 3.41 Reliability-oriented C-based design flow

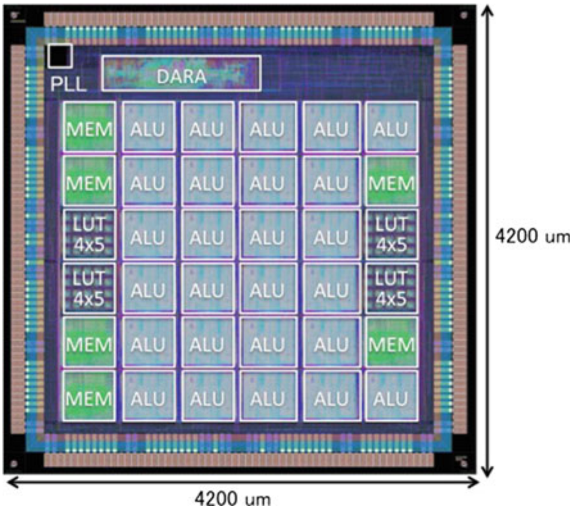
3.4.4 Test Chip Implementation

A proof-of-concept array based on the proposed reconfigurable architecture was fabricated in 65 nm 12ML CMOS process. The die size is 4.2 × 4.2 mm. Figure 3.42 shows a layout of the test chip, which has 26 ALU clusters, 6 MEM clusters and 4 LUT blocks. REG clusters have not been included in the test chip because of a constraint of chip area. ALU, LUT and MEM clusters include 120 k, 4 k, and 99 k gates, respectively. Here, REG clusters are not included in the test chip since our preliminary evaluation before the test chip implementation shows that small image processing applications that can be implemented on the test chip demand more ALU clusters instead of REG clusters.

Thanks to dynamic reconfiguration using states generated by an FSM, area-efficient mapping becomes possible. Here, in this implementation, the number of instructions for ALU was set to 16 due to the limited silicon area, while a work done by our colleagues suggested that the number of instructions of more than 24 is desirable [152]. Nevertheless, it has been shown that, for example, an edge detection filter can be implemented with 25 ALU clusters only, while 62 ALU clusters would be necessary if it were not for dynamic reconfiguration (i.e., in a single state). The number of clusters is reduced by 60% in this particular example. Thus, the proposed architecture implemented on the test chip has demonstrated the possibility of exploiting latency-area exploration using the behavioral synthesis.

Figure 3.43 illustrates the mapping of an application on our reconfigurable array. With the help of the C-based design flow taking into account reliability specifications, it has been demonstrated that the use of the proposed mixed-grained reconfigurable array enable to manage both the trade-off between soft-error resiliency and hardware cost, and the trade-off between latency and hardware resource usage.

Fig. 3.42 Chip layout of designed reconfigurable array



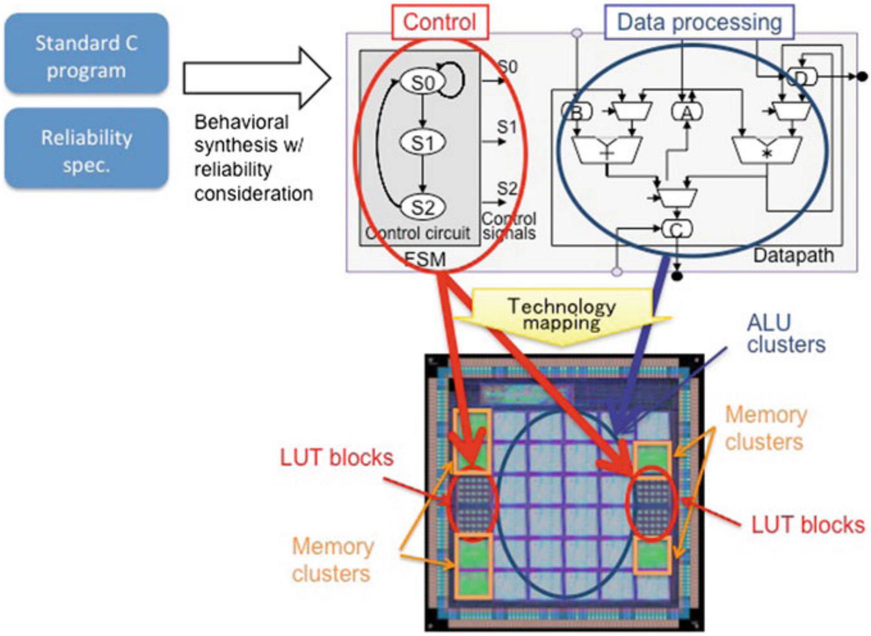


Fig. 3.43 Application implementation flow on the mixed-grained reconfigurable array

3.4.5 Demonstration of a Video Application

In order to validate the functionality and reliability of the architecture, a demonstration using two mappings of SMM and SMS was performed on the evaluation board shown in Fig. 3.44. The chip receives a live data stream from a video camera, and sends it to a monitor demonstrating the processed stream. The mapping of black and white reversal filter was generated from a C source code. Here, the black and white reversal filter is a filter that performs tone reversal, and a subtraction is performed for each pixel.

A snapshot of the results is shown in Fig. 3.45. After positioning an Am-241 alpha foil whose flux [7] is 9×10^9 cm^2 h^{-1} over the chip, it was observed that SMS mapping continued to output the processed video as expected. On the other hand, SMM mapping got destroyed in 2 s due to SEUs in configuration registers, and then video processing stopped within 10 s in all four trials. We also tested TMR mapping and confirmed the expected continuous functionality. The proposed architecture thus enables reliable operation, which includes application mapping, under harsh irradiation.

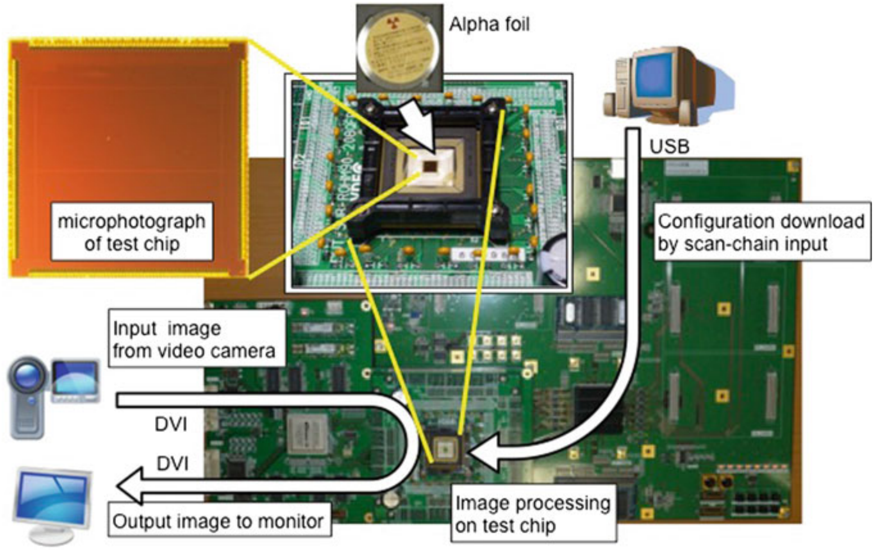

Alpha foil
USB
microphotograph of test chip
Configuration download by scan-chain input
Input image from video camera
DVI
DVI
Output image to monitor
Image processing on test chip

Fig. 3.44 Demonstration setup

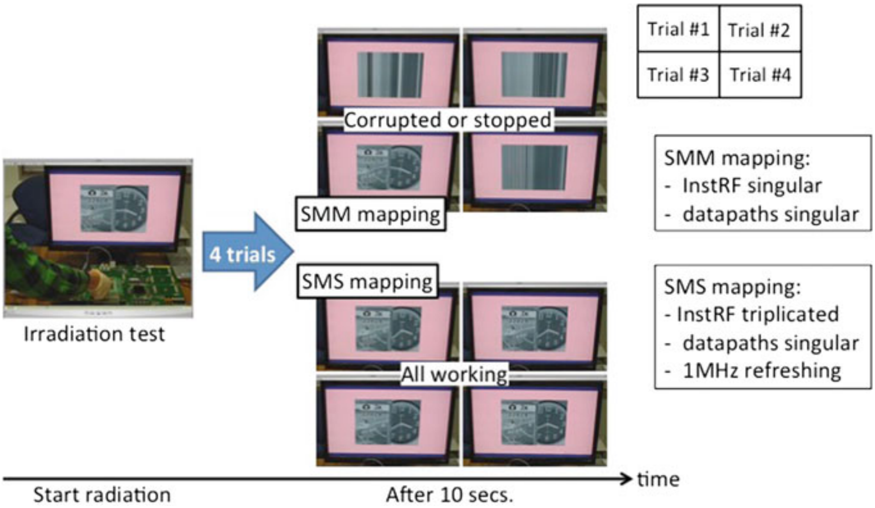


Fig. 3.45 Results of image processing under irradiation

3.4.6 Directions of Future Work

In the present work, we developed a mixed-grained reconfigurable architecture, which consists of fine-grained and coarse-grained fabrics, each of which can be configured for different levels of reliability depending on the reliability requirement of target applications, e.g., mission-critical applications to consumer products. Thanks to the fine-grained fabrics, the architecture can accommodate implementing a state machine, which is indispensable for exploiting C-based behavioral synthesis to trade latency with resource usage through multi-step processing using dynamic reconfiguration. The demonstration of a video application using a proof-of-concept VLSI chip, which is fabricated in 65 nm process, will answer a broad range of reliability requirements from terrestrial to space applications with varied resilience against radiation-induced soft errors.

Further extension of this work is under way in a few important directions. One is to further advance the basic concepts borne in the present work of reconfigurable architecture to better accommodate real-world trade-offs among performance, reliability, and cost. Another is to demonstrate the feasibility of this architecture at the levels of integration required for practical applications.

3.5 Simulation and Design Techniques for Computer Systems

Makoto Sugihara, Kyusyu University

3.5.1 Simulation Technique

A single event upset (SEU) is a change of state, which is caused by a high-energy particle strike to a sensitive node in semiconductor memory devices. An SEU in an integrated circuit (IC) component often causes a faulty behavior of a computer system. A soft error rate (SER) of a memory device is the rate at which the memory device encounters or is predicted to encounter SEUs during a unit time. The SER is often utilized as a metric for vulnerability of an IC component. The SER for a memory module is a vulnerability baseline rather than one reflecting its actual and accurate behavior. SERs of memory modules become over-pessimistic when the modules are embedded into computer systems and the system vulnerability is estimated as the simple sum of all memory SERs in the system. More specifically, every SEU occurring in memory modules is regarded as a critical error when memory modules are under field or accelerated tests. This implicitly assumes that every SEU on memory cells of a memory module *always* make a computer system faulty. Since memory modules are used spatially and temporarily in computer systems, only some of SEUs on the memory modules make the computer system faulty and others not. Therefore, the soft errors in an entire computer system should be estimated in a different way from the simple summation of memory SERs in the system.

Accurate vulnerability estimation of an entire computer system is essential for building reliable computer systems. This subsection summarizes a simulation-based vulnerability estimation approach for a computer system, which has several memory hierarchies in order that one can accurately estimate the reliability of the computer system within reasonable computation time [159, 160]. We define a critical SEU as one which may cause faulty behavior of a computer system. We also define an SEU vulnerability factor for a job running on a computer system as the expected number of critical SEUs which occur during the job, unlike a classical vulnerability factor. The architectural-level soft-error model identifies the part of memory modules that are utilized temporarily and spatially, and SEUs which are critical to the program execution at cycle-accurate ISS (instruction set simulation) level in the computer system. Our architectural-level soft-error model is capable of estimating the reliability of a computer system that has several memory hierarchies and finding which memory module is vulnerable in the computer system. Reliability estimation helps one apply reliable design techniques to vulnerable part of their design.

Unlike memory components, the rate at which a computer system encounters SEU-induced errors varies every moment because the computer system uses memory modules spatially and temporarily. Since only active part of the memory modules affects reliability of the computer system, it is essential to identify the active part of memory modules for accurately estimating the number of soft errors occurring in the computer system. A universal soft error metric other than an SER is necessary to estimate reliability of computer systems because an SER is a reliability metric suitable for components of regular and monotonous structure like memory modules but not for computer systems. In this subsection, the number of soft errors which occur during execution of a program is utilized as a soft error metric for computer systems. In computer systems, a word is a basic element for computation in CPUs. A word is an instruction in an instruction memory while that is a data in a data memory. A collection of words is required to be processed in order to run a program. We consider the reliability to process all words as the reliability of a computer system. The total number of SEUs which are expected to occur on all the words is regarded as the number of SEUs of the computer system. This subsection discusses an estimation model for the number of soft errors on a word. A CPU-centric computer system typically has the hierarchical structure of memory modules, which includes a register file, cache memory modules, and main memory modules. The computer system at which we target has levels of memory modules, in order of accessibility from/to the CPU. In the hierarchical memory system, instructions are generally processed as follows.

- Instructions are generated by a compiler and loaded into a main memory.

The birth time of an instruction is the time for the instruction to be loaded into the main memory, from the viewpoint of program execution.

- When the CPU requires an instruction, it fetches the instruction from the memory module closest to it. The instruction is duplicated into all levels of memory modules which reside between the CPU and the source memory module.

Note that instructions are basically read-only. Duplication of instructions is uni-directionally made from a low level to a high level of a memory module.

Data items in data memory are processed as follows.

- Some data are given as initial values of a program when the program is generated with a compiler. The birth time of such a data is the time for the program to be loaded into a main memory. The other data are generated during execution of the program by the CPU. The birth time of the data which is made online is the time for the data item to be made and saved to the register file.
- When a data is requested by a CPU, the CPU fetches it from the memory module closest to the CPU. If the write allocate policy is adopted, the data is duplicated at all levels of memory modules which reside between the CPU and the master memory module, and otherwise it is not duplicated at the inter-adjacent memory modules.

Note that data are writable as well as readable. This means that data can be copied from a high level to a low level of a memory module, and vice versa.

In CPU-centric computer systems, data are utilized as constituent elements. The data vary in lifetime and the numbers of soft errors on the data vary from data to data.

Let us consider critical SEUs in a computer system whose memory hierarchy is shown in Fig. 3.46. The memory hierarchy of the computer system consists of a register file, an L1 cache, an L2 cache, and a main memory.

Figure 3.47 shows an example of critical SEUs in instruction memory.

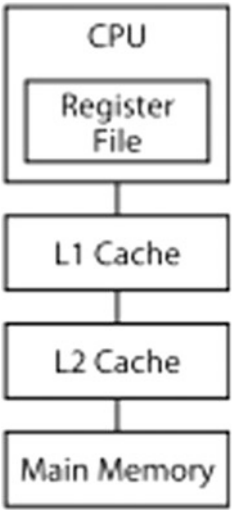


Fig. 3.46 Memory hierarchy example

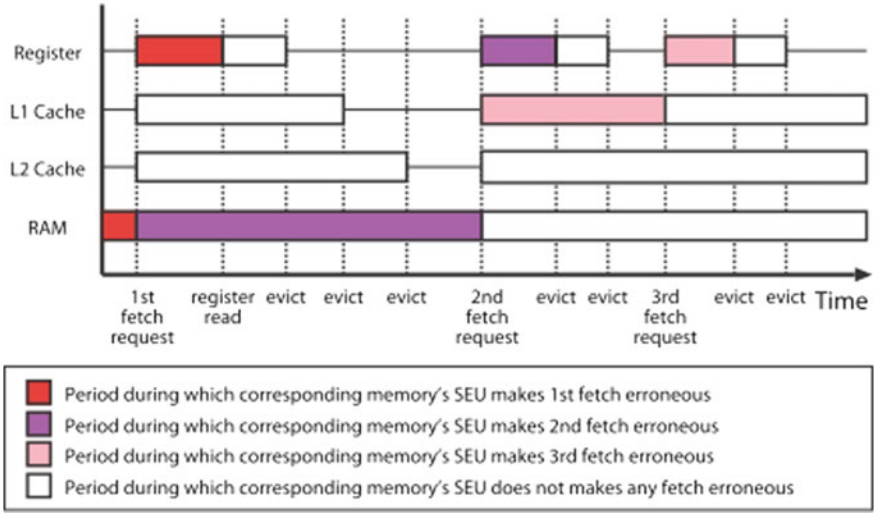

Register
L1 Cache
L2 Cache
RAM
1st fetch request
register read
evict
evict
evict
2nd fetch request
evict
evict
3rd fetch request
evict
evict
Time
🟥 Period during which corresponding memory's SEU makes 1st fetch erroneous
🟪 Period during which corresponding memory's SEU makes 2nd fetch erroneous
▨ Period during which corresponding memory's SEU makes 3rd fetch erroneous
□ Period during which corresponding memory's SEU does not makes any fetch erroneous

Fig. 3.47 Periods for critical SEUs in instruction memory

In this example, we ideally assume that an instruction is instantaneously transmitted between memory hierarchy levels. A rectangle indicates a period during which its corresponding memory hierarchy level stores a copy of the word. In the example, there are three fetch requests for the instruction which resides at a certain address. On the first instruction fetch, the target word item resides only in the main memory. It is assumed that a word is directly brought from the main memory to the register file while copies are made in the register file, L1 and L2 caches. SEUs which occur during the periods indicated by the red rectangles are regarded as critical with regard to the first instruction fetch. The same for the second instruction fetch. SEUs which occur during the periods indicated by the purple rectangles are regarded as critical. On the third instruction fetch, the target word resides at the L1 cache. SEUs which occur during the periods indicated by the pink rectangles are regarded as critical. The periods indicated by the white rectangles are finally found to be non-critical.

Figure 3.48 shows an example of critical SEUs in data memory on the assumption of the write-through policy. In this example, we ideally assume that a data is instantaneously transmitted between memory hierarchy levels. A rectangle indicates a period during which its corresponding memory hierarchy level stores the data. Initially, a word is stored in the register file. Then the first store writes the word through. A load instruction follows. On the load instruction, the highest memory hierarchy which has a copy of the target word is the L1 cache and a copy is made from the L1 cache to the register file. Then the CPU uses the copy of the word. The register read makes SEUs which occur during the periods indicated the red rectangles critical. Then another register write, the second store, an L1 overwrite, a load instruction and register read follow. On the second load instruction, the

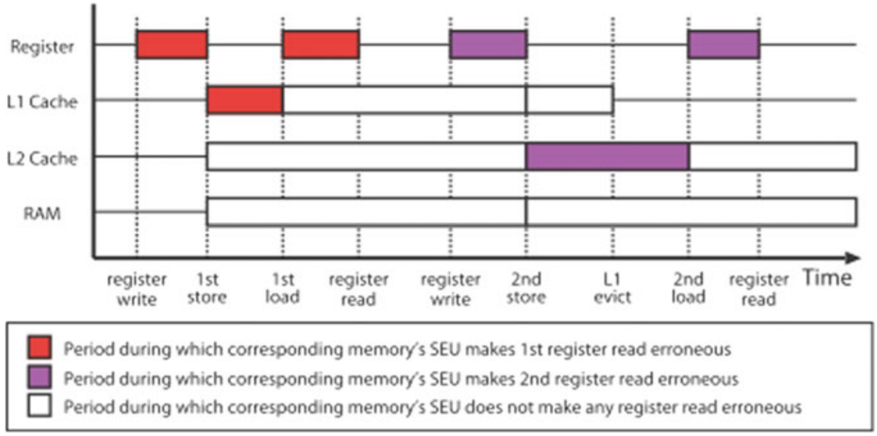

Register
L1 Cache
L2 Cache
RAM
register write
1st store
1st load
register read
register write
2nd store
L1 evict
2nd load
register read
Time
🟥 Period during which corresponding memory's SEU makes 1st register read erroneous
🟪 Period during which corresponding memory's SEU makes 2nd register read erroneous
□ Period during which corresponding memory's SEU does not make any register read erroneous

Fig. 3.48 Periods for critical SEUs in write-through data memory

highest memory hierarchy which has a copy of the target word is the L2 cache and a copy is made from the L2 cache to the register file. Then the CPU uses the copy of the word. The second register read makes SEUs which occur during the periods indicated the purple rectangles critical. The periods indicated by the white rectangle are finally found to be non-critical.

Counting the periods for critical SEUs in instruction set simulation calculates the number of fault bits which are inputted to the CPU, that is an SEU vulnerability factor.

3.5.2 Design Techniques

Design for reliability (DFR) is one of the themes of urgent concern. Based on the simulation-based vulnerability estimation technique [142, 143], several DFR techniques were proposed.

In [144, 145], a reliable cache architecture was presented which offered performance and reliability modes. More cache memory is used in the performance mode while less cache memory is used in the reliability mode to avoid SEUs. Task scheduling approach was also presented in [161, 162]. All tasks are statistically scheduled under real-time and reliability constraints. The demerit of the approach is that switching operation modes causes performance and area overheads and might be unacceptable to high-performance or general-purpose microprocessors.

In [163, 164], a task scheduling approach was presented which minimized SEU vulnerability of a heterogeneous multiprocessor under real-time constraints. Architectural heterogeneity among CPU cores offers a variety of reliability for a task. A task scheduling problem was presented which minimized SEU vulnerability of an entire system under a real-time constraint. The demerit of the approach is that the fixed heterogeneous architecture loses general-purpose programmability.

In [165, 166], a heterogeneous multiprocessor synthesis approach was presented which minimizes chip area under SEU vulnerability and execution time constraints.

To the best of our knowledge, this is the first study to synthesize a heterogeneous multiprocessor system with a soft error issue taken into account. In this section we use the SEU vulnerability factor as a vulnerability factor. The other vulnerability factors, however, are applicable to our system synthesis methodology as far as they are capable to estimating task-wise vulnerability on a processor. If a single event transient (SET) is a dominant factor to fail a system, a vulnerability factor which can treat SETs should be used in our heterogeneous multiprocessor synthesis methodology. Our methodology assumes that a set of tasks are given and that several variants of processors are given as building blocks. It also assumes that real-time and vulnerability constraints are given by system designers. Simulation with every combination of a processor model and a task characterizes performance and reliability. Our system synthesis methodology uses the values of the chip area of every building block, the characterized runtime and vulnerability, and the given real-time and vulnerability constraints in order to synthesize a heterogeneous multiprocessor system whose chip area is minimal under the constraints.

References

1. E. Ibe, *Terrestrial Radiation Effects in ULSI Devices and Electronic Systems* (IEEE Press and Wiley, 2015)
2. E. Ibe, H. Taniguchi, Y. Yahagi, K. Shimbo, T. Toba, Impact of scaling on neutron-induced soft error in SRAMs from a 250 nm to a 22 nm design rule. Trans. Electron Devices **57**(7), 1527–1538 (2010)
3. N. Kanekawa, E. Ibe, T. Suga, Y. Uematsu, *Dependability in Electronic Systems-Mitigation of Hardware Failures, Soft Errors, and Electro-Magnetic Disturbances* (Springer, New York, 2010)
4. S. Kuboyama, K. Sugimoto, S. Shugyo, S. Matsuda, T. Hirao, Single-event burnout of epitaxial bipolar transistors. Trans. Nucl. Sci. **45**(6), 2527–2533 (1998)
5. http://helios.izmiran.rssi.ru/cosray/main.htm#top. Accessed 14 Feb 2013
6. T. Nakamura, M. Baba, E. Ibe, Y. Yahagi, H. Kameyama, *Terrestrial Neutron-Induced Soft-Errors in Advanced Memory Devices* (World Scientific, New Jersey, 2008)
7. JEDEC, Measurement and reporting of alpha particle and terrestrial COSMIC ray induced soft errors in semiconductor devices. in *JEDEC Standard JESD89A*, pp. 1–93 (2006)
8. T. Inoue, H. Henmi, Y. Yoshikawa, H. Ichihara, High-level synthesis for multi-cycle transient fault tolerant data paths. in *17th IEEE International On-line Testing Symposium*, vol. 1.3, Athens, Greece, 13–15 July 2011, pp. 13–18
9. https://repository.exst.jaxa.jp/dspace/bitstream/a-is/19254/1/61889032.pdf
10. C.S. Walker, *Capacitance, Inductance and Crosstalk Analysis* (Artech House Antennas and Propagation Library, Altech House Publisher)
11. http://www.bostonscientific.com/lifebeat-online/electromagnetic-interference.html
12. K. Ishibashi, K. Osada (eds.), *Low Power and Reliable SRAM Memory Cell and Array Design* (Springer, 2011)

13. http://www.opsalacarte.com/pdfs/Tech_Papers/Soft_Error_Trends_and_Mitigation_Techniques_in_Memory_Devices_Presentation_by_Charlie_Slayman,Opsalacarte.pdf
14. G. Cellere, A. Paccagnella, A. Visconti, M. Bonanomi, S. Beltrami, Single event effects in NAND flash memory arrays. IEEE Trans. Nucl. Sci. **53**(4), 1813–1818 (2006)
15. M. Nicolaidis (ed.), *Soft Errors in Modern Electronic Systems* (Springer, 2011) pp. 1–239
16. S. Sayil, N.B. Patel, Soft error and soft delay mitigation using dynamic threshold technique. IEEE Trans. Nucl. Sci. **57**(6), 3553–3559 (2010)
17. D.M. Fleetwood, R.D. Schrimpf (eds.), Radiation effects and soft errors in integrated circuits and electronic devices World Sci. 1–324 (2004)
18. C. Slayman, M. Ma, S. Lindley, Impact of error correction code and dynamic memory reconfiguration on high-reliability/low-cost server memory. in *IEEE International Integrated Reliability Workshop* Final Report, pp. 190–193 (2006)
19. P. Andrei, S. Manoj (eds.), *CMOS SRAM Circuit Design and Parametric Test in Nano-Scaled Technologies* (Springer, 2008) pp. 1–192
20. http://www.csl.cornell.edu/courses/ece5745/handouts/ece5745-T02-cmos-devices.pdf
21. http://www.eesemi.com/soi.htm
22. B. Nikolić1, M. Blagojević, O. Thomas, P. Flatresse, A. Vladimirescu, Circuit design in nanoscale FDSOI technologies. in *Proceedings of 29th International Conference on Microelectronics* (*MIEL 2014*), Belgrade, Servia 12–14 May 2014, pp. 3–6
23. O. Kononchuk, B.-Y. Nguyen (eds.), *Silicon-On-Insulator (SOI) Technology: Manufacture and Applications* (Elsevier, 2014)
24. N. Sugii, R. Tsuchiya, T. Ishigaki, Y. Morita, H. Yoshimoto, K. Torii, S. Kimura, Comprehensive study on Vth variability in silicon on thin BOX (SOTB) CMOS with small random-dopant fluctuation: finding a way to further reduce variation, in *IEEE International Devices Meeting,* San Francisco, 15–17 Dec 2008, pp. 249–253
25. T.C. May, M.H. Woods, Alpha-Particle-induced soft errors in dynamic memories. IEEE Trans. Elect. Device **ED-26**(1), 2–9
26. C. Hu, Alpha-particle-induced field and enhanced collection of carriers. IEEE Elect. Device Lett. **EDL-3**(2), 31–34 (1982)
27. https://www.jedec.org/standards-documents/dictionary/terms/single-event-functional-interrupt-sefi
28. J. Barak, E. Adler, B. Fischer, M. Schlogl, S. Metzger, Micro-beam mapping of single event Latchups and single event upsets in CMOS SRAMs. IEEE Trans. Nucl. Sci. Seattle **45**(3), 1595–1602 (1998)
29. H. Asai, K. Sugimoto, I. Nashiyama, Y. Iide, K. Shiba, M. Matsuda, Y. Miyazaki, Terrestrial neutron-induced single-event burnout in SiC power diodes, in *The Conference on Radiation Effects on Components and Systems*, vol. (PC-3), Sevilla, Spain, 19–23 Sept. 2011
30. T. Shoji, S. Nishida, T. Ohnishi, T. Fujikawa, N. Nose, M. Ishiko, K. Hamada, Neutron induced single-event burnout of IGBT, in *The 2010 International Power Electronics Conference*, Sapporo, Hokkaido, 21–24 June 2010, pp. 142–148
31. S. Nishida, T. Shoji, T. Ohnishi, T. Fujikawa, N. Nose, M. Ishiko, K. Hamada, Cosmic ray ruggedness of IGBTs for hybrid vehicles, in *The 22nd International Symposium on Power Semiconductor Devices & ICs*, Hiroshima, 6–10 June 2010, pp. 129–132
32. ITRS Report 2010. http://www.itrs.net/
33. N. Seifert, B. Gill, M. Zhang, V. Zia, V. Ambrose, On the scalability of redundancy based SER mitigation schemes, in *International Conference on IC Design and Technology*, Austin, Texas 18–20 May, vol. G2, pp. 197–205
34. E. Ibe, S. Chung, S. Wen, H. Yamaguchi, Y. Yahagi, H. Kameyama, S. Yamamoto, T. Akioka, Spreading diversity in multi-cell neutron-induced upsets with device scaling, in *The 2006 IEEE Custom Integrated Circuits Conference*, San Jose, CA, 10–13 Sept 2006, pp. 437–444
35. J.F. Ziegler, W.A. Lanford, Effect of cosmic rays on computer memories. Science **206**, 776–788 (1979)

36. M. Gutsche, et al., Capacitance enhancement techniques for sub-100 nm trench DRAMs, in *International Electron Device Meeting*, Washington, DC, 3–6 Dec 2001, pp. 18.6.1–18.6.4
37. K. Takeuchi, K. Shimohigashi, E. Takeda, E. Yamasaki, Experimental characterization of α-induced charge collection mechanism for megabit DRAM cells, in *IEEE International Solid-State Circuits Conference*, N.Y., 10 Feb 1987, pp. 99–100
38. G.A. Sai-Halasz, M.R. Wordeman, R.H. Dennard, Alpha-particle-induced soft error rate in VLSI circuits. IEEE Trans. Elect. Devices **ED-29**(4), 725–731 (1982)
39. C.E. Thompson, J.M. Meese, Reduction of α-particle sensitivity in dynamic semiconductor memories (16 k d-RAMs) by neutron irradiation. IEEE Trans. Nucl. Sci. **NS-28**(6), 3987–3993 (1981)
40. E. Ibe, Current and future trend on cosmic-ray-neutron induced single event upset at the ground down to 0.1-micron-device, in *The Svedberg Laboratory Workshop on Applied Physics*, Uppsala, 3 May (1)
41. JEDEC, Measurement and reporting of alpha particle and terrestrial cosmic ray induced soft errors in semiconductor devices. *JEDEC Standard JESD89*, pp. 1–63 (2001)
42. E. Ibe, H. Kameyama, Y. Yahagi, K. Nishimoto, Y. Takahashi, Distinctive asymmetry in neutron-induced multiple error patterns of 0.13 umocess SRAM, in *The 6th International Workshop on Radiation Effects on Semiconductor Devices for Space Application,* Tsukuba, 6–8 Oct 2004, pp. 19–23 (2004)
43. N. Seifert, V. Zia, Assessing the impact of scaling on the efficacy of spatial redundancy based mitigation schemes for terrestrial applications, in *2007 IEEE Workshop on Silicon Errors in Logic—System Effects*, Austin, Texas, April 3, 4 (2007)
44. P. Shivakumar, M. Kistler, S.W. Keckler, D. Burger, L. Alvisi, Modeling the effect of technology trends on the soft error rate of combinational logic, in *International Conference on Dependable Systems and Networks*, pp. 389–398 (2002)
45. H. Quinn, K. Morgan, P. Graham, J. Krone, M. Caffrey, K. Lundgren, Static proton and heavy ion testing of the Xilinx Virtex-5 device, in *Radiation Effects Data Workshop*, No. W-31, Honolulu, Hawaii, 23–27 July, pp. 177–184 (2007)
46. T. Calin, M. Nicolaidis, R. Velazco, Upset hardened memory design for submicron CMOS technology. IEEE Trans. Nucl. Sci. **43**(6), 2874–2878 (1996)
47. H. Quinn, J. Tripp, T. Fairbanks, A. Manuzzato, Improving microprocessor reliability through software mitigation, in *2011 IEEE Workshop on Silicon Errors in Logic—System Effects,* Urbana-Champaign, Illinoi, 29–30 Mar 2011, pp. 16–21
48. T. Uemura, Y. Tosaka, H. Matsuyama, K. Shono, SEILA: soft error immune latch for mitigating multi-node-SEU and local-clock-SET, in *IEEE International Reliability Physics Symposium 2010,* Anaheim, CA, USA, 2–6 May 2010, pp. 218–223
49. H.-H. Lee, K. Lilja, S. Mitra, Design of a sequential logic cell using LEAP: layout design through error aware placement, in *2010 IEEE Workshop on Silicon Errors in Logic—System Effects*, Stanford University, 23–24 Mar 2010
50. R.C. Baumann, E.B. Smith, Neutron-induced boron fission as a major source of soft errors in deep submicron SRAM devices, in *2000 IEEE International Reliability Physics* (2000)
51. IEC (2008) Part 38: soft error test method for semiconductor devices with memory. Semiconductor devices. Mechanical and climatic test methods, in *Symposium Proceedings IEC60749-38*, San Jose, CA, 10–13 Apr 2008 pp. 152–157
52. B. Falsafi, Reliability in the dark silicon era, in *International On-Line Testing Symposium 2011*, Athens, Greece, 13–15 July 2011, p. xvi
53. J. Loncaric, DOE's exascale initiative and resilience, in 2011 *IEEE Workshop on Silicon Errors in Logic—System Effects*, Urbana-Champaign, Illinois, 29–30 Mar 2011
54. J.F. Abella, J. Cazorlal, D. Gizopoulos, E. Quinones, A. Grasset, S. Yehia, P. Bonnot, R. Mariani, G. Bernat, Towards improved survivability in safety-critical systems, in *17th IEEE International On-Line Testing Symposium*, Athens, Greece, 13–15 July 2011 (S3), pp. 242–247

55. D. Baumeister, S.G.H. Anderson, Evaluation of chip-level irradiation effects in a 32-bit safety microcontroller for automotive braking applications, in *2012 IEEE Workshop on Silicon Errors in Logic—System Effects*, vol. 2.2, Urbana-Champaign, Illinois, 27–28 Mar 2012
56. Automotive Electronics Council, Failure mechanism based stress test quantification for integrated circuits, in *AEC-Q100 Revolution G*, pp. 1–35 (2007)
57. ISO, International Standard ISO26262 Road vehicles-Functional safety (2011)
58. H. Quinn, Study on cross-layer reliability, in *2011 IEEE Workshop on Silicon Errors in Logic—System Effects*, Urbana-Champaign, Illinois, March 29–30
59. N. Carter, Cross-layer reliability, in *2010 IEEE Workshop on Silicon Errors in Logic—System Effects,* Stanford University, March 23, 24 (2010)
60. C. Slayman, Eliminating the threat of soft errors—a system vendor perspective, in *IRPS SER Panel Discussion, Eliminating the Threat of Soft Error*, vol. 6 Dallas, Texas, April 2, 2003
61. E. Ibe, H. Kameyama, Y. Yahagi, H. Yamaguchi, Single event effects as a reliability issue of IT infrastructure, in *3rd International Conference on Information Technology and Applications*, July 3–7, 2005, Sydney, vol. I, pp. 555–560
62. E. Ibe, K. Shimbo, T. Toba, H. Taniguchi, Y. Taniguchi, LABIR: Inter-LAyer built-in reliability for electronic components and systems, in *Silicon Errors in Logic—System Effects*, Urbana-Champaign, Illinois, USA, March 27–28 2011
63. E. Ibe, K. Shimbo, T. Toba, H. Taniguchi, Y. Taniguchi, Quantification and mitigation strategies of neutron induced soft-errors in CMOS devices and components-the past and future, in *2011 IEEE International Reliability Physics Symposium, Monterey, California*, April 12–14 (3C2)
64. A. Evans, M. Nicolaidis, S.-J. Wen, D. Alexandrescu, E. Costenaro, RIIF—Reliability Information Interchange Format, in *IEEE International On-Line Testing Symposium, Sitges, Spain*, June 27–29, 2012 (6.2)
65. E. Ibe, T. Toba, K. Shimbo, H. Taniguchi, Fault-Based reliable design on-upper-bound of electronic systems for terrestrial radiation including muons, electrons, protons and low energy neutrons, in *IEEE International On-Line Testing Symposium, Sitges, Spain*, June 27–29, 2012 (3.2)
66. H. Kobayashi, N. Kawamoto, J. Kase, K. Shiraishi, Alpha particle and neutron-induced soft error rates and sling trends in SRAM, in *IEEE International Reliability Physics Symposium 2009, Montreal, Quebec, Canada,* April 28–30 (2H4), pp. 206–211
67. B.D. Sierawski, M.H. Mendenhall, R.A. Reed, M.A. Clemens, R.A. Welle, R.D. Schrimp, E. W. Blackmore, M. Trinczek, B. Hitti, J.A. Pellish, R.C. Baumann, S.-J. Wen, R. Wong, N. Tam, Muon-Induced single event upsets in deep-submicron technology. Trans. Nucl. Sci. **57** (6), 3273–3278 (2010)
68. S. Wen, R. Wong, M. Romain, N. Tam, Thermal neutron soft error rate for SRAMs in the 90 nm–45 nm technology range, in *2010 IEEE International Reliability Physics Symposium*, Anaheim, CA, 2–6 May 2010 (SE5.1), pp. 1036–1039
69. S. Wen, S.Y. Pai, R. Wong, M. Romain, M., N. Tam, B10 Findings and correlation to thermal neutron soft error rate sensitivity for SRAMs, in the sub-micron technology, in *IEEE International Integrated Reliability Workshop*, Stanford Sierra, CA, Oct. 17–21 2010, pp. 31–33
70. R.C. Baumann, Determining the impact of alpha-particle-emitting contamination from the Fukushima Daiichi disaster on Japanese manufacturing sites, in *The 12th European Conference on Radiation and Its Effects on Component and Systems*, Sevilla, Spain, Sept. 19–23 2010, pp. 784–787
71. http://semicon.jeita.or.jp/hp/srg/docs/JEITA-SERPG-View_en.pdf
72. D.C. Matthews, M.J. Dion, NSE impact on commercial avionics, in *2009 IEEE International Reliability Physics Symposium*, Montreal, QC, April 26–30 2009, pp. 181–193

73. E. Normand, J. Wert, D. Oberg, P. Majewski, P. Voss, S.A. Wender, Neutron-induced single event burnout in high voltage electronics. Trans. Nucl. Sci. **44**, 2358–2368 (1997)
74. C. Slayman, Cache and memory error detection, correction, and reduction techniques for terrestrial servers and workstations. IEEE Trans. Device Mater. Reliab. **5**(3), 397–404 (2005)
75. G. Schindlbeck, C. Slayman, Neutron-induced logic soft errors in dram technology and their impact on reliable server memory, in *IEEE Workshop on Silicon Errors in Logic—System Effects,* Austin Texas, April 3–4 2007, p. 3
76. K. Shimbo, T. Toba, K. Nishii, E. Ibe, Y. Taniguchi, Y. Yahagi, Quantification & mitigation techniques of soft-error rates in routers validated in accelerated neutron irradiation test and field test, in *2011 IEEE Workshop on Silicon Errors in Logic—System Effects,* Urbana-Champaign, Illinois, 29–30 Mar 2011, pp. 11–15
77. C. Rivetta, B. Allongue, G. Berger, F. Faccio, W. Hajdas, Single event burnout in DC-DC converters for the LHC experiments, in *The 6th European Conference on Radiation and Its Effects on Components and Systems*, Grenoble, France, 10–14 Sept 2001, pp. 315–322
78. P. Rech, L. Carro, Experimental evaluation of neutron-induced effects in graphic processing units, in *The 9th Workshop on Silicon Errors in Logic—System Effects*, Palo Alto, California, USA, 26–27 Mar, vol. 5.3
79. A. Geist, Exascale monster in the closest, in *2012 IEEE Workshop on Silicon Errors in Logic —System Effects, Urbana-Champaign*, Illinois, 27–28 Mar, vol 5.1 (2012)
80. J.T. Daly, Emerging challenges in high performance computing: resilience and the science of embracing failure, in *The 9th Workshop on Silicon Errors in Logic—System Effects*, Palo Alto, California, USA, 26–27 Mar (Keynote III) (2013)
81. G. Upasani, X. Vera, A. Gonzalez, Achieving zero DUE for L1 data caches by adapting acoustic wave detectors for error detection, in *19th IEEE International On-Line Testing Symposium*, Chania, Crete, 8–10 July, vol. 5.2 (2013)
82. D. Skarin, J. Sanfridson, Impact of soft errors in a brake-by-wire system, in *IEEE Workshop on Silicon Errors in Logic—System Effects 3*, Austin, Texas, 3–4 Apr (2007)
83. B. Nemeth, P. Gaspar, Z. Szabo, J. Bokor, O. Sename, L. Dugard, Design of fault-tolerant control for trajectory tracking, in *13th Mini Conference on Vehicle System Dynamics, Identification and Anomalies*, Budapest, Hungary, 5–7 Nov 2012 (2012)
84. Y. Nakata, Y. Ito, Y. Sugure, S. Oho, Y. Takeuchi, S. Okumura, H. Kawaguchi, M. Yoshimoto, Model-based fault injection for failure effect analysis—evaluation of dependable SRAM for vehicle control units, in *The 5th Workshop on Dependable and Secure Nanocomputing*, Hong Kong, China, 27 July 2011
85. C. Lopez-Ongil, M. Portela-Garcia, M. Garcia-Valderas, A. Vaskova, J. Rivas-Abalo, L. Entrena, A. Martinortega, J. Martinez-Oter, S. Rodriguez-Bustabad, I. Arruego, SEU sensitivity of robust communication protocols, in *IEEE International On-Line Testing Symposium*, Sitges, Spain, 27–29 June 2012, vol. 9.4 (2012), pp. 188–193
86. A. Vaskova, M. Portela-Garcia, M. Garcia-Valderas, M. SonzaReorda, C. Lopez-Ongil, Hardening of serial communication protocols for potentially critical systems in automotive applications: LIN Bus, in *19th IEEE International On-Line Testing Symposium*, Chania, Crete, 8–10 July, vol. 1.3 (2013), pp. 13–18
87. P. Rech, C. Aguiar, R. Ferreira, C. Frost, L. Carro, Neutrons radiation test of graphic processing units, in *IEEE International On-Line Testing Symposium*, Sitges, Spain, 27–29 June 2012, vol. 3.3 (2012)
88. Y. Chen, Cosmic ray effects on cellphone and laptop applications, in *The 9th Workshop on Silicon Errors in Logic—System Effects*, Palo Alto, California, USA, 26–27 Mar, vol. 5.4 (2013)
89. G. Upasani, X. Vera, A. González, Avoiding core's DUE & SDC via acoustic wave detectors and tailored error containment and recovery, in *2014 ACM/IEEE 41st International Symposium on Computer Architecture (ISCA) 14–18* June 2014, Minneapolis, Minnesota, pp. 37–48

90. E.H. Neto, F.L. Kastensmidt, G.I. Wirth, A Built-In current sensor for high speed soft errors detection robust to process and temperature variations, in *Proceedings of the 20th Annual Symposium on Integrated Circuits and System Design, Rio de Janeiro,* Brazil, September 2007, pp. 190–195
91. P. Oldiges, K. Bernstein, D. Heidel, B. Klaasen, E. Cannon, R. Dennard, H. Tang, M. Ieong, H.-S.P. Wong, Soft error rate scaling for emerging SOI technology options, in *VLSI Technology, 2002. Digest of Technical Papers. 2002 Symposium on 11–13 June 2002* Honolulu, Hawaii, USA, pp. 46–47
92. N. Seifert, B. Gill, S. Jahinuzzaman, J. Basile, V. Ambrose, Q. Shi, R. Allmon, A. Bramnik, Soft error susceptibilities of 22 nm tri-gate devices, in *IEEE Transactions on Nucear. Science*, vol. 59, No. 6, pp. 2666–2673
93. P. Roche, Technology downscaling worsening radiation effects in bulk: SOI to the rescue, in *2013 IEEE International Electron Devices Meeting,* 9–11 Dec. 2013, pp. 31.1.1–31.1.4
94. H. Sato, T. Wada, S. Ohbayashi, K. Kozaru, Y. Okamoto, Y. Higashide, T. Shimizu, Y. Maki, R. Morimot, H. Otoi, T. Koga, H. Honda, M. Taniguchi, Y. Arita, T. Shiomi, A 500-MHz pipelined burst SRAM with improved SER immunity. IEEE J. Solid State Circ. **34** (11), 1571–1579 (1999)
95. L.W. Massengill, SEU-hardened resistive-load static RAMs. IEEE Trans. Nucl. Sci. **38**(6), 1478–1485 (1991)
96. T. Ohsawa, S. Ikeda, T. Hanyu, H. Ohno, T. Endoh, A 1-Mb STT-MRAM with zero-array standby power and 1.5-ns quick wake-up by 8-b fine-grained power gating, in *2013 5th IEEE International Memory Workshop, Monterey, California*, 26–29 May 2013, pp. 80–83
97. N. Wang, S.J. Patel, Symptom based redundant multithreading, in *The Second Workshop on System Effects of Logic Soft Errors, Urbana-Champaign*, Illinois, 11–12 Apr 2006
98. K. Shimbo, T. Toba, T. Uezono, E. Ibe, Rapid recovery technique from soft error of FPGAs in information and communication apparatus. The Institute of Electronics, Information Technical Report **115**(58), 37–42 (2015)
99. D. Ernst, S. Das, S. Lee, D. Blaauw, T. Austin, T. Mudge, N. Kim, K. Flautner, Razor: circuit-level correction of timing errors for low-power operation. Micro **24**(6), 10–20 (2004)
100. http://www.nextplatform.com/2016/03/14/intel-marrying-fpga-beefy-broadwell-open-compute-future/
101. http://www.mst.or.jp/Portals/0/prize/english/index_en.html
102. J.J. Chen, R. Tsai, H. Tzeng, A symptom-driven fuzzy system for isolating faults, in *IEEE International Conference on Systems, Man and Cybernetics*, Chicago, Illinois, vol. 2, pp. 1589–1592 (1992)
103. T. Marques, A symptom-driven expert system for isolating and correcting network faults. IEEE Commun. Mag. **26**(3), 6–13 (1988)
104. M. Lee, A. Krishnakumar, P. Krishnan, N. Singh, S. Yajnik, Hypervisor-assisted application checkpointing in virtualized environments, in *DSN2011*, 28–30 June 2011, Hong Kong, China
105. Y. Sazeides, A. Geist, S. Adve, R. Iyer, T. Wenisch, Panel discussion: reliability requirements of large scale data centers, in *2012 IEEE Workshop on Silicon Errors in Logic —System Effects*, *Urbana-Champaign,* Illinois, 27–28 Mar 2012, vol. 4.1 (2012)
106. A. Sanyal, S. Alam, S. Kundu, A built-in self-test scheme for soft error rate characterization, in *International On-Line Testing Symposium 2008*, 6–9 July 2008, Greece, vol. 3.3, p. 65
107. S. Siskos, A new built-in current sensor for low supply voltage analog and mixed-signal circuits testing, in *International On-Line Testing Symposium*, 5–7 July 2010, Corfu Island, Greece
108. K. Yoshikawa, T. Hashida, M. Nagata, An on-chip waveform capturer for diagnosing off-chip power delivery, in *International Conference on IC Design and Technology*, 2–4 May 2011 Kaohsiung, Taiwan

109. M.-L. Li, P. Ramachandran, Towards a software-hardware co-designed resilient system, in *IEEE Workshop on Silicon Errors in Logic—System Effects*, 3–4 Apr 2007, vol. 3, Austin Texas
110. S.K.S. Hari, H. Naeimi, P. Ramachandran, S.V. Adve, Relyzer: application resiliency analyzer for transient faults, in *2011 IEEE Workshop on Silicon Errors in Logic—System Effects,* Urbana-Champaign, Illinois, March 29–30, pp. 22–26
111. http://www.hitachi.com/rev/archive/2001/_icsFiles/afieldfile/2004/06/08/r2001_04_101.pdf. Accessed 22 Nov 2013
112. http://hes-standards.org/sc25_wg1_introduction.pdf. Accessed 22 Nov 2013
113. A. Dixit, A. Wood, The impact of new technology on soft error rates, in *IEEE International Reliability Physics Symposium (IRPS)*, Monterey, California, pp. 486–492 (2011)
114. J. Maiz, S. Hareland, K. Zhang, P. Armstrong, Characterization of multi-bit soft error events in advanced SRAMs, in *IEEE International Electron Devices Meeting (IEDM)*, (Washington, DC, 2003) pp. 519–522
115. S. Ohbayashi, M. Yabuuchi, K. Nii, Y. Tsukamoto, S. Imaoka, Y. Oda, T. Yoshihara, M. Igarashi, M. Takeuchi, H. Kawashima, Y. Yamaguchi, K. Tsukamoto, M. Inuishi, H. Makino., K. Ishibashi, H. Shinohara, A 65-nm SoC embedded 6T-SRAM designed for manufacturability with read and write operation stabilizing circuits, in *IEEE Symposium on VLSl Circuits Digest of Technical Pap*ers, Kyoto, Japan, pp. 820–829 (2007)
116. S. Yoshimoto, T. Amashita, D. Kozuwa, T. Takata, M. Yoshimura, Y. Matsunaga, H. Yasuura, H. Kawaguchi, M. Yoshimoto, Multiple-bit-upset and single-bit-upset resilient 8T SRAM bitcell layout with divided wordline structure, in *IEEE International On-Line Testing Symposium (IOLTS)*, (Athens, Greece, 2011) pp. 151–156
117. iRoC TFIT Simulator, Transistor Level Soft Error Analysis. http://www.iroctech.com
118. G. Gasiot, D. Giot, P. Roche, Multiple cell upsets as the key contribution to the total ser of 65 nm cmos srams and its dependence on well engineering. IEEE Trans. Nucl. Sci. **54**(6), 2468–2473 (2007)
119. H. Iwase, K. Nitta, T. Nakamura, Development of general-purpose particle and heavy ion transport Monte Carlo code, in *IEEE Transactions on Nuclear Science*, vol. 39, pp. 1142–1151 (2002). http://phits.jaea.go.jp/
120. T. Sato, H. Yasuda, K. Niita, A. Endo, L. Sihverd, Development of PARMA: PHITS-based analytical radiation model in the atmosphere, in Rad. Res. 170, 244–259, 2008; EXPACS ver. 2.21, 2011, http://phits.jaea.go.jp/expacs/index.html
121. P. Hazucha, C. Svensson, Impact of CMOS technology scaling on the atmospheric neutron soft error rate. IEEE Trans. Nucl. Sci. **47**(6), 2586–2594 (2000)
122. C. Robert, Radiation-induced soft errors in advanced semiconductor technologies. IEEE Trans. Nucl. Sci. **5**(3), 305–316 (2005)
123. C. Auth, A. Cappellani, J.S. Chun, A. Dalis, A. Davis, T. Ghani, G. Glass, T. Glassman, M. Harper, M. Hattendorf, P. Hentges, S. Jaloviar, S. Joshi, J. Klaus, K. Kuhn, D. Lavric, M. Lu, H. Mariappan, K. Mistry, B. No.rris, N. Rahhal-orabi, P. Ranade, J. Sandford, L. Shifren, V. Souw, K. Tone, F. Tambwe, A. Thompson, D. Towner, T. Troeger, P. Vandervoorn, C. Wallace, J. Wiedemer, C. Wiegand, 45 nm High-k + Metal Gate Strain-Enhanced Transistors, in *IEEE Symposium on VLSI Technology*, Honolulu, Hawaii, pp. 128–129 (2008)
124. H.J. Cho, K.I. Seo, W.C. Jeong, Y.H. Kim, Y.D. Lim, W.W. Jang, J.G. Hong, S.D. Suk, M. Li, C. Ryou, H.S. Rhee, J.G. Lee, H.S. Kang, Y.S. Son, C.L. Cheng, S.H. Hong, W.S. Yang, S.W. Nam, J.H. Ahn, D.H. Lee, S. Park, M. Sadaaki, D.H. Cha, D.W. Kim, S.P. Sim, S. Hyun, C.G. Koh, B.C. Lee, S.G. Lee, M.C. Kim, Y.K. Bae, B. Yoon, S.B. Kang, J.S. Hong, S. Choi, D.K. Sohn, J.S. Yoon, C. Chung, Bulk planar 20 nm high-K/metal gate CMOS technology platform for low power and high performance applications, in *IEEE International Electron Devices Meeting (IEDM)* (Washington, DC, 2011), pp. 350–353

125. C.C. Wu, Y.K. Leung, C.S. Chang, M.H. Tsai, H.T. Huang, D.W. Lin, Y. M. Sheu, C.H. Hsieh, W.J. Liang, L.K. Han, W.M. Chen, S.Z. Chang, S.Y. Wu, S.S. Lin, H. C. Lin, C. H. Wang, P.W. Wang, T.L. Lee, C.Y. Fu, C. W. Chang, S.C. Chen, S.M. Jang, S.L. Shue, H. T. Lin, Y.C. See, Y.J. Mii, C. H. Diaz, B. J. Lin, M. S. Liang, Y.C. Sun, A 90-nm CMOS device technology with high-speed, general-purpose, and low-leakage transistors for system on chip applications, in *IEEE International Electron Devices Meeting (IEDM),* San Francisco, California, pp. 65–68 (2002)
126. C. Shin, N. Damrongplasit, X. Sun, Y. Tsukamoto, B. Nikoli, T.J.K. Liu, Performance and yield benefits of Quasi-Planar bulk CMOS technology for 6-T SRAM at the 22-nm node. IEEE Trans. Elect. Devices **58**(7), 1846–1854 (2011)
127. J. Furuta, K. Kobayashi, H. Onodera, Impact of cell distance and well-contact density on neutron-induced multiple cell upsets, in *Proceedings of International Reliability Physical Symposium*, *Monterey*, California, Apr 2013, pp. 6C.3.1–6C.3.4
128. K. Zhang, K. Kobayashi, Contributions of charge sharing and bipolar effects to cause or suppress MCUs on redundant latches, in *Proceedings of International Reliability Physical Symposium,* Monterey, Calirofonia, Apr 2013, pp. SE.5.1–SE.5.4
129. R. Yamamoto, C. Hamanaka, J. Furuta, K. Kobayashi, H. Onodera, An area-efficient 65 nm radiation-hard dual-modular flip-flop to avoid multiple cell upsets. IEEE Trans. Nucl. Sci. **58** (6), 3053–3059 (2011)
130. D. Krueger, E. Francom, J. Langsdorf, Circuit design for voltage scaling and SER immunity on a quad-core itanium processor, in *ISSCC*, Feb 2008, San Francisco, California, pp. 94–95
131. R. Kan, T. Tanaka, G. Sugizaki, K. Ishizaka, R. Nishiyama, S. Sakabayashi, Y. Koyanagi, R. Iwatsuki, K. Hayasaka, T. Uemura, G. Ito, Y. Ozeki, H. Adachi, K. Furuya, T. Motokurumada, The 10th generation 16-core SPARC64$^{\mathrm{TM}}$; processor for mission critical UNIX server. IEEE J. Solid State Circ. **49**(1), 32–40 (2014)
132. M. Zhang, S. Mitra, T.M. Mak, N. Seifert, N.J. Wang, Q. Shi, K.S. Kim, N.R. Shanbhag, S. J. Patel, Sequential element design with built-in soft error resilience. IEEE Trans. VLSI Syst. **14**(12), 1368–1378 (2006)
133. J. Furuta, C. Hamanaka, K. Kobayashi, H. Onodera, A 65 nm bistable cross-coupled dual modular redundancy flip-flop capable of protecting soft errors on the C-element, in *VLSI Circuit Symposium*, June 2010, Honolulu, Hawaii, pp. 123–124
134. N. Seifert, V. Ambrose, B. Gill, Q. Shi, R. Allmon, C. Recchia, S. Mukherjee, N. Nassif, J. Krause, J. Pickholtz, A. Balasubramanian, On the radiation-induced soft error performance of hardened sequential elements in advanced bulk CMOS technologies, in *Proceedings of International Relational Physics Symposium*, May 2010, Anaheim, California, pp. 188–197
135. B. Narasimham, K. Chandrasekharan, Z. Liu, J. Wang, G. Djaja, N. Gaspard, J. Kauppila, B. Bhuva, A hysteresis-based d-flip-flop design in 28 nm CMOS for improved SER hardness at low performance overhead. IEEE Trans. Nucl. Sci. **59**(6), 2847–2851 (2012)
136. N. Gaspard, S. Jagannathan, Z. Diggins, N. Mahatme, T. Loveless, B. Bhuva, L. Massengill, W. Holman, B. Narasimham, A. Oates, P. Marcoux, N. Tam, M. Vilchis, S.-J. Wen, R. Wong, Y. Xu, Soft error rate comparison of various hardened and non-hardened flip-flops at 28-nm node, in *Proceedings of International Reliability Physical Symposium Waikoloa,* Hawaii, June 2014, pp. SE.5.1–SE.5.5
137. R. Tsuchiya, M. Horiuchi, S. Kimura, M. Yamaoka, T. Kawahara, S. Maegawa, T. Ipposhi, Y. Ohji, H. Matsuoka, Silicon on thin BOX: a new paradigm of the CMOSFET for low-power high-performance application featuring wide-range back-bias control, in *IEDM,* San Francisco, California, Dec 2004, pp. 631–634
138. N. Sugii, R. Tsuchiya, T. Ishigaki, Y. Morita, H. Yoshimoto, S. Kimura, Local Vth variability and scalability in Silicon on-Thin-BOX (SOTB) CMOS with small random-dopant fluctuation. IEEE Trans. Elect. Dev. **57**(4), 835–845 (2010)
139. S. Kamohara, N. Sugii, Y. Yoshiki, H. Makiyama, T. Yamashita, T. Hasegawa, S. Okanishi, H. Yanagita, M. Kadoshima, K. Maekawa, M. Hiroshi, Y. Yamagata, H. Oda, Y.

Yamaguchi, K. Ishibashi, A. Hideharu, K. Usami, K. Kobayashi, T. Mizutani, T. Hiramoto, Ultra low-voltage design and technology of silicon on-thin-buried-oxide (SOTB) CMOS for highly energy efficient electronics in iot era, in *VLSI Technology Symposium* (Honolulu, Hawaii, 2014)

140. P. Roche, J.-L. Autran, G. Gasiot, D. Munteanu, Technology downscaling worsening radiation effects in bulk: SOI to the rescue, in *IEDM*, Washington, DC, Dec 2013, pp. 31.1.1–31.1.4
141. D. Jacquet, G. Cesana, P. Flatresse, F. Arnaud, P. Menut, F. Hasbani, T. Di Gilio, C. Lecocq, T. Roy, A. Chhabra, C. Grover, O. Minez, J. Uginet, G. Durieu, F. Nyer, C. Adobati, R. Wilson, D. Casalotto, 2.6 GHz ultra-wide voltage range energy efficient dual A9 in 28 nm UTBB FD-SOI, in *VLSI Technical Symposium*, Kyoto, Japan, 2013, pp. C44–C45.8
142. K. Kobayashi, K. Kubota, M. Masuda, Y. Manzawa, J. Furuta, S. Kanda, H. Onodera, A low-power and area-efficient radiation-hard redundant flip-flop, DICE ACFF in a 65 nm thin-box FD-SOI, in *IEEE Tranactions on Nuclear Science* vol. 61, no. 4, June 2014
143. S.M.A.H. Jafri, et al., Design of a fault-tolerant coarse-grained reconfigurable architecture: a case study, in *Proceedings of International Symposium on Quality Electronic Design (ISQED)*, Mar 2010, San Jose, California, pp. 845–852
144. M.M. Azeem, et al., Error recovery technique for coarse-grained reconfigurable architectures, in *Proceedings of IEEE Symposium on Design and Diagnostics of Electronic Circuits and Systems (DDECS)*, Apr 2011, Cottbus, Germany, pp. 441–446
145. T. Schweizer, et al., Low-cost TMR for fault-tolerance on coarse-grained reconfigurable architectures, in *Proceedings of International Conference on Reconfigurable Computing and FPGAs (ReConFig)*, Dec 2011, Cancun, Mexico, pp. 135–140
146. S.C. Goldstein et al., PipeRench: a reconfigurable architecture and compiler. IEEE Trans. Comput. **33**(4), 70–77 (2000)
147. C. Ebeling, et al., RaPiD—reconfigurable pipelined data-path, in *Proceedings of International Conference on Field Programmable Logic and Applications (FPL)*, Sept 1996, Darmstadt, Germany, pp. 126–135
148. Y. Mitsuyama, et al., Area-efficient reconfigurable architecture for media processing, *IEICE Transactions in Fundamentals of Electronics, Communications and Computer Sciences*, Dec 2008, vol. E91-A, no. 12, pp. 3651–3662
149. T. Toi, et al., High-level synthesis challenges and solutions for a dynamically reconfigurable processor, in *Proceedings of International Conference on Computer-Aided Design (ICCAD)*, Nov. 2006, San Jose, California, pp. 702–708
150. T. Sugawara et al., Dynamically reconfigurable processor implementation with IPFlex's DAPDNA technology. IEICE Trans. Informat. Syst. **E87-D**(8), 1997–2003 (2004)
151. V. Baumgarte et al., PACT XPP—a self-reconfigurable data processing architecture. J. Supercomput. **26**(2), 167–184 (2003)
152. H. Konoura, et al., Reliability-configurable mixed-grained reconfigurable array supporting C-based design and its irradiation testing, in *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, to appear, Dec. 2014
153. T. Imagawa, et al., A cost-effective selective TMR for heterogeneous coarse-grained Reconfigurable architectures based on DFG-level vulnerability analysis, in *Proceedings of Design, Automation & Test in Europe (DATE)*, Mar 2013, Grenoble, France, pp. 701–706
154. T. Imagawa, H. Tsutsui, H. Ochi, T. Sato, A cost-effective selective TMR for coarse-grained reconfigurable architectures based on DFG-level vulnerability analysis, in *IEICE Transactions on Electronics*, vol. E96-C, no. 4, Apr. 2013
155. B. Pratt, M. Caffrey, P. Graham, K. Morgan, M. Wirthlin, Improving FPGA design robustness with partial TMR, in *Proceedings of International Reliability Physics Symposium (IRPS)*, San Jose, California, Mar. 2006, pp. 226–232,
156. J. Yao et al., DARA: a low-cost reliable architecture based on unhardened devices and its case study of radiation stress test. IEEE Trans. Nucl. Sci. **59**(6), 2852–2858 (2012)

157. K. Wakabayashi, T. Okamoto, C-based SoC design flow and EDA tools: an ASIC and system vendor perspective, in *IEEE Transactions Computer-Aided Design of Integrated Circuits and Systems*, vol. 19, no. 12, Dec 2000, pp. 1507–1522
158. CyberWorkbench, http://www.nec.com/en/global/prod/cwb/
159. M. Sugihara, T. Ishihara, M. Muroyama, K. Hashimoto, A simulation-based soft error estimation methodology for computer system, in *Proceedings of International Symposium on Quality Electronic Design (ISQED)*, Mar 2006, San Jose, California, pp. 196–203
160. M. Sugihara, T. Ishihara, and K. Murakami, Architectural-level soft-error modelling for estimating reliability of computer systems, IEICE Trans. Electron. **E90-C**(10), 1983–1991 (2007)
161. M. Sugihara, T. Ishihara, K. Murakami, Task scheduling for reliable cache architectures of multiprocessor systems, in *Proceedings of Design, Automation and Test in Europe (DATE), Nice Acropolis, France*, Apr 2007, pp. 1490–1495
162. M. Sugihara, T. Ishihara, K. Murakami, Reliable cache architectures and task scheduling for multiprocessor systems. IEICE Trans. Electron. **E91-C**(4), 410–417 (2008)
163. M. Sugihara, SEU vulnerability of multiprocessor systems and task scheduling of heterogeneous multiprocessor systems, in *Proceedings of EUROMICRO Conference on Digital System Design (DSD)*, Patras, Greece, Aug 2009 pp. 333–340
164. M. Sugihara, Reliability inherent in heterogeneous multiprocessor systems and task scheduling for ameliorating their reliability. IEICE Trans. Fundament. Electron. Commun. Comput. Sci. **E92-A**(4), 1121–1128 (2009)
165. M. Sugihara, Heterogeneous multiprocessor synthesis under performance and reliability constraints, in *Proceedings of EUROMICRO Conference on Digital System Design (DSD)*, Patras, Greece, Sept 2009, pp. 232–239
166. M. Sugihara, On synthesizing a reliable multiprocessor for embedded systems. IEICE Trans. Fundament. Electron. Commun. Comput. Sci. **E93-A**(12), 2560–2569 (2010)

Chapter 4
Electromagnetic Noises

Makoto Nagata, Nobuyuki Yamasaki, Yusuke Kumura, Shuma Hagiwara and Masayuki Inaba

Abstract VLSI chips in a practical system always experience interactions with surrounding electromagnetic (EM) environment. EM noise emitted from circuits can interfere with other circuits on the same chip or in another chip. Circuits and systems performance may be unpredictably and dynamically degraded by EM noise through its impacts on power and signal integrity.This chapter discusses the state-of-the-art knowledge and countermeasures associated with such unseen noise problems, covering noise emission, noise immunity, noise mitigation, tolerance, and integrity, all for the noise awareness in the design of dependable VLSI systems. An overview of EM compatibility (EMC) in CMOS digital integrated circuits (ICs) is given in Sect. 4.1, along with simulation and measurements of EM noise in a semiconductor IC chip. EM noise emission is explained as the interaction of dynamic power currents in ICs and parasitic impedance in a chip-package-board combined power delivery network (PDN).Electromagnetic susceptibility (EMS) of IC chips against incoming radio frequency high-power disturbance is discussed in Sect. 4.2. Static random access memory (SRAM) cores are chosen for demonstrating EMS evaluation based on direct power injection (IEC 62132-4). On-chip

M. Nagata (✉)
Kobe University, Kobe, Japan
e-mail: nagata@cs.kobe-u.ac.jp

N. Yamasaki · Y. Kumura · S. Hagiwara
Keio University, Yokohama, Japan
e-mail: yamasaki@ny.ics.keio.ac.jp

Y. Kumura
e-mail: yusuke@ny.ics.keio.ac.jp

S. Hagiwara
e-mail: hagiwara@ny.ics.keio.ac.jp

M. Inaba
The University of Tokyo, Tokyo, Japan
e-mail: inaba@i.u-tokyo.ac.jp

S. Asai (ed.), *VLSI Design and Test for Systems Dependability*,
https://doi.org/10.1007/978-4-431-56594-9_4

waveform monitoring provides useful means to analyze the mechanisms in which incoming RF power causes SRAM bit failures.On-chip power supply filtering adaptively suppresses EM noise due to PDN resonance, as a proactive measure for reducing electromagnetic interference (EMI) of IC chips, discussed in Sect. 4.3.The 4b/10b is a dependable line code with error correction ability. Responsive Link, which is a real-time communication link, can control the trade-off among the error correction strength, throughput, and latency, based on the communication environment such as inside a high-power robot operated by extremely high voltage (80 V) and huge current (200 A), by selecting a line code including the 4b/10b, a bit-level error correction code, and a block-level error correction code, as demonstrated in Sect. 4.4.

Keywords Electromagnetic compatibility · Power noise awareness
Power and signal integrity · *Responsive Link* · 4b/10b line code with ECC

4.1 Electromagnetic Compatibility of CMOS ICs

Makoto Nagata, Kobe University

4.1.1 IC Chip Viewpoints

An electronic system experiences the irradiation of electromagnetic (EM) waves from environments, mostly unintentionally. Vehicles and aircrafts may approach EM sources such as radar stations on their road without knowing their exact entity on a map and be exposed to high-power and high-frequency EM waves. Mobile terminals transmit and receive radio frequency (RF) waves for their communications, while being interfered with other EM waves from other radio sources, each compliant to certain standards that may not be fully compatible with each other. Natural sparkles from phenomena such as lightning, ignition, electrostatic shocks, and others emit broadband EM waves spherically in any directions and interact in some degrees with operations of nearby electronic equipment. For an electronic system to properly and safely operate in the presence of those EM waves, it has to comply with electromagnetic compatibility (EMC) regulations. There are a variety of international standards and regulations in the field of EMC to be followed in a product development for worldwide markets. Designers have concerned EMC standards set by IEC, ISO, IEEE, FCC, and CISPR. The regulation series of no. 10 (R10) by United Nations Economic Commission for Europe (UNECE) is well known in automotive segment. Those standards influence every building component of an electronic system, from materials, IC chips, packaging and assembly, to software and systems. The reader may be interested in the whole area of EMC and also even in the phenomenon of electrostatic discharge (ESD) somewhat relevant to the IC chip level EMC as well. Those topics are to be covered in general EMC/ESD text books. We focus on EMC problems of integrated circuit (IC) chip in this chapter, to stay in the viewpoints of the dependability of VLSI systems. The following few sections will discuss the emission and interaction of EM waves on power delivery networks (PDNs) of an IC chip, in close relations with power integrity problems in a chip-package-board unified system. The general knowledge of EMC at the IC level can cover signal integrity problems as well, where signal routing and associated logic elements in a chip directly interact with EM waves. While the chapters are unfortunately limited in contents and spaces, the readers can expand their interests and insights to wider topics of IC chip EMC from modeling and analysis to measurements in state-of-the-art research publications. One of the well-known workshops in the field of IC chip EMC is IEEE EMC Compo [1].

Design for EMC is highly demanded for integrated circuit (IC) chips. An IC chip emits electromagnetic (EM) noise into space and/or receives EM noise from space, through its power supply lanes as illustrated in Fig. 4.1. An IC chip needs to guarantee the sufficiently low level of noise emission during its operation, not to disturb proper operation of surrounding equipment by electromagnetic interference (EMI). It is also requested to carry sufficient immunity against incoming noises from other equipment, not to degrade operating performance or even not to lose its functionality by electromagnetic susceptibility (EMS). The EMC requires the pair of such two-way characteristics to be simultaneously met.

An electronic system consists of many IC chips and therefore the remedies against EM noise coupling are necessary at the IC chip level, in order to make system operations robust and dependable against electromagnetic environment. Electronic control unit (ECU) as an automotive subsystem has stringent requirements of electromagnetic (EM) noise emission in a vehicle as being below the regulatory limits. Computing facilities like a cluster of servers also need to suppress EM noise from their high-frequency operation as well as large power current consumption. The EM noise of radio frequency (RF) chips may cause fatal interference with wireless communication. EM noise emission is closely related with power supply current of an IC chip, and that is time varying according to the

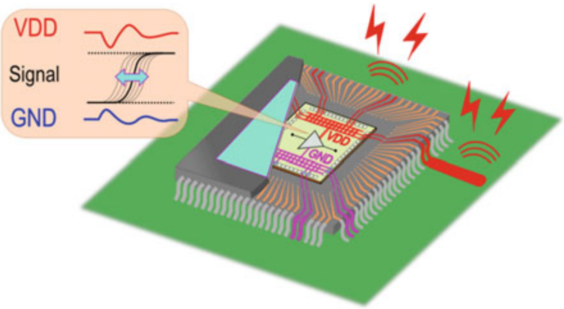


Fig. 4.1 Electromagnetic noise emission and susceptibility of integrated circuit

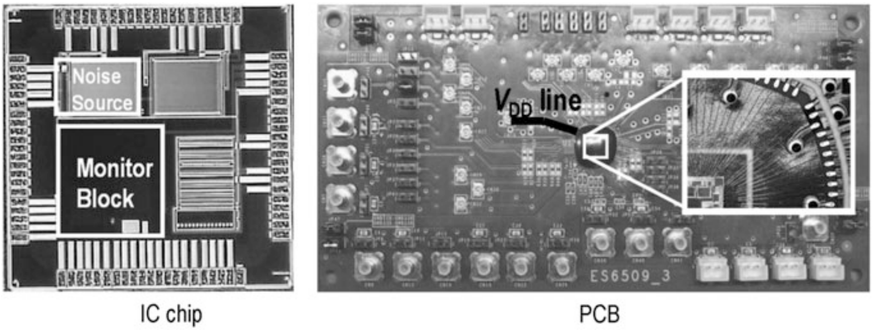
operation of internal circuits and interacts with power line impedance that is frequency dependent.

The techniques to evaluate EMC include measurements and simulation. Regarding EMI, a near-field magnetic probe (equivalently a tiny coil) scans magnetic fields in a whole plane of printed circuit board (PCB), assembled with IC chips and other electronic components. This shows a map of EM radiation (emission) in strengths and also in frequencies as well. A capacitive sensor also complementarily evaluates local electric fields. While for EMS, an RF power can be intentionally applied to any pins of ICs or components on a PCB and then the tolerance (susceptibility) of system operations is evaluated. While those measurements can reveal EMC performance of a product, the simulation techniques are fundamental for the design of IC chips and electronic systems in assembly to comply with EMC standards and regulations.

A simulation technique of dynamic (AC) power supply current at an IC chip level is explained in the following subsections, where silicon examples of the measurements and analysis of EMI will be also given. It should be noted that the topics of EMS will be covered in the next chapter (Sect. 4.2). In addition, EMC suppressions (Sect. 4.3) and EMC solutions (Sect. 4.4) will also follow.

4.1.2 EMC Evaluation Using a Package-Board-Level Simulation

An IC chip of typically less than 5 mm in each side is assembled in a system board with the scale of a few centimeters, as in an example photo of Fig. 4.2 [2]. The AC components of power supply current are generated by circuits in operation, within a small area of silicon die. In contrast, a closed loop of entire power delivery includes the chip, system board, and power source, and forms a macroscopic antenna. The flow of AC power current essentially creates EM noise emission.



IC chip PCB

Fig. 4.2 IC chip and PC board [1] (copyright 2011 IEEE)

Co-simulation of the power current of an IC chip and the frequency domain response of on-chip and on-board integrated power delivery network (PDN), namely IC chip-package-board co-simulation, is a key element of system-level power noise analysis [2–4]. An equivalent circuit of Fig. 4.3 captures the AC power current consumption in a capacitor charging model [5, 6] and the AC impedance characteristics of the PDN in an S-parameter model. The capacitor charging and S-parameter models represent the active and passive portion of power noise analysis, respectively, and the entire equivalent circuit is simulated with a conventional SPICE simulator.

The equivalent circuit of Fig. 4.3 involves parasitic impedances of on- and off-chip parts of the PDN. The on-chip part includes full-chip power planes of power supply (V_{DD}) and ground (V_{SS}). The planes are modeled as resistive mesh networks with the resistance extracted from detailed layout data of the whole of the chip. The parasitic capacitance of an entire chip, C_{die}, couples the V_{DD} and V_{SS} planes. The power pins for connecting to off-chip parts of the PDN are also explicitly included. In addition, a silicon substrate can be involved in the computation of the V_{SS} resistive network, since substrate currents flow from V_{SS} lines of a digital circuit to multiple V_{SS} pins of peripheral I/O rings via p^+ substrate contacts. These substrate connections in parallel effectively reduce V_{SS} impedance and also impact on power noise seen on the V_{SS} network.

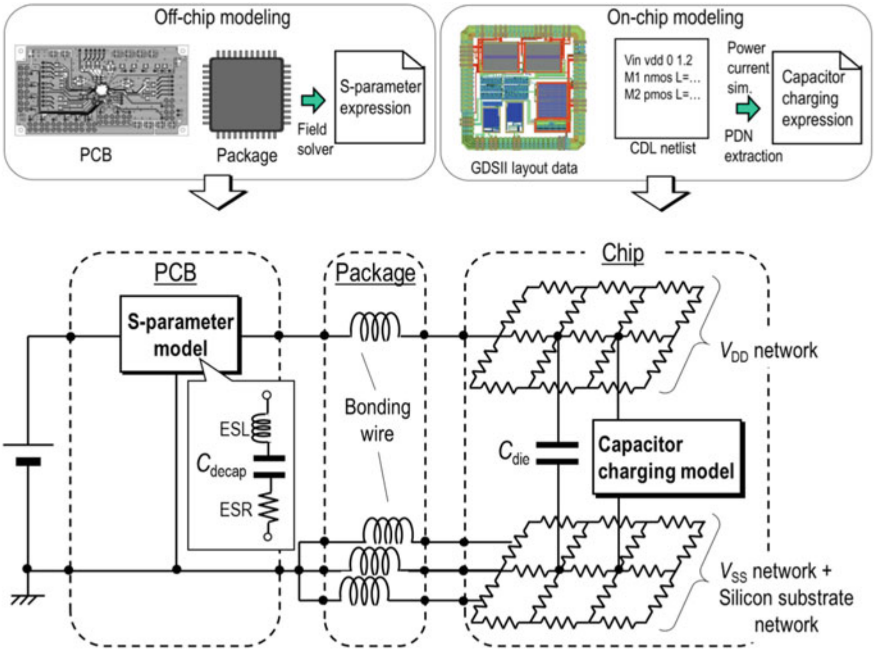


Fig. 4.3 On-chip and on-board integrated power noise co-simulation model

The off-chip part attributes to a chip in assembly and a printed circuit board (PCB). A bonding wire is replaced by a series inductance for each connection of V_{DD} or V_{SS} pin on the chip and the corresponding metallic land on the PCB. Decoupling capacitors (decap) are also inserted between V_{DD} trace and V_{SS} plane on the PCB, along with equivalent series inductance (ESL) as well as resistance (ESR). The transfer characteristics of PDN traces on a PCB are simulated by a conventional full-wave three-dimensional (3D) solver.

In the capacitor charging model of Fig. 4.4, the group of logic switching operation in a digital circuit that is considered approximately simultaneous, or happens within a narrow time slice, is substituted by a single capacitor charging process. The size of a capacitor is equivalent to the amount of charges to be drawn from an external power source during the corresponding time slice. The time-domain progress of power current is represented by the successive charging of such equivalent capacitors. The distribution of gate toggles is derived from gate-level simulation of the target circuit, including gate and wire delays extracted from the final physical layout. The equivalent capacitor is then calculated by slicing the distribution in every time interval. The time intervals of $\{t_1, t_2, \ldots, t_n\}$ can be empirically chosen like the 1/10 of a clock period. The amount of charges needs to be pre-characterized for each gate element of a given standard logic cell library.

The results of simulations will be presented and compared with experiments in Sect. 4.1.4.

4.1.3 Test Structure for Power Noise Investigation

A generally applicable method to evaluate power noise emission of a VLSI chip is discussed in this section. The test structure of Fig. 4.5 features on-board AC power current measurements using a near-field magnetic probe, in accordance with

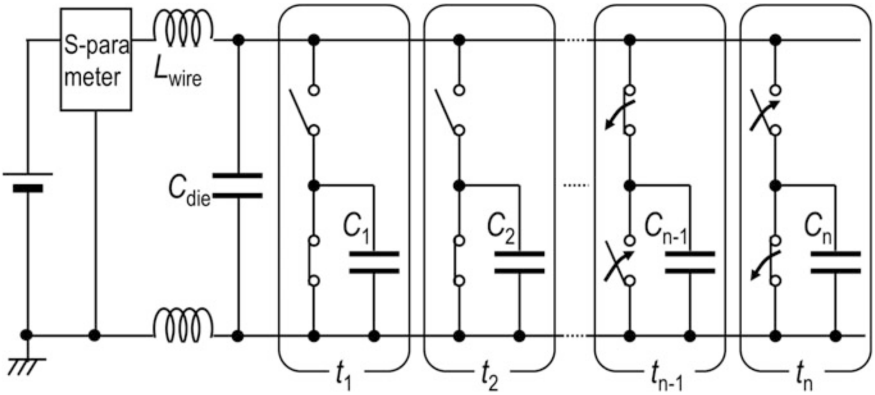


Fig. 4.4 Capacitor charging (TSDPC) model [1] (copyright 2011 IEEE)

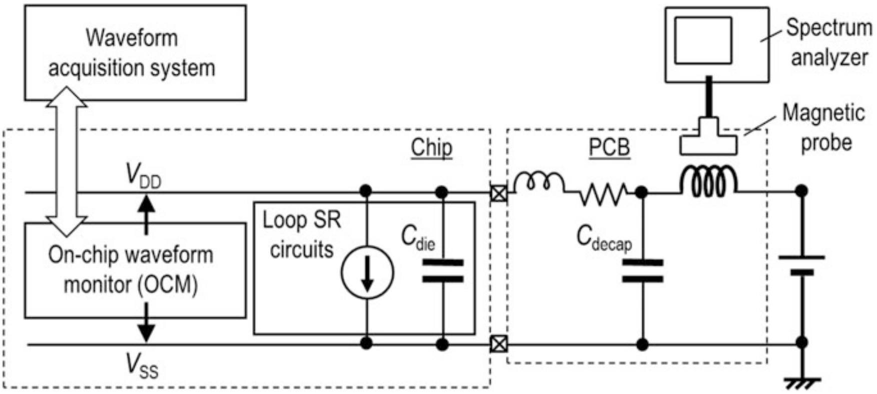


Fig. 4.5 Test structure for on-chip and on-board AC power noise measurements

IEC61967-1 [7] and IEC69197-6 [8], along with on-chip voltage monitoring on power nodes. A silicon chip fabricated in a 65 nm CMOS process embeds an array of loop shift registers (SR) of Fig. 4.6 as the source of power noise. This circuit primarily consists of a cascade of D-type flip flop (DFF) cells where a series of preregistered bits is sequentially rotated in the loop. It is regarded as a synchronous digital circuit having the shallowest logical depth and operating in a broad range of clock frequencies, F_{clk}. The power supply voltage is 1.2 V.

The test chip additionally includes an on-chip waveform monitor (OCM) of Fig. 4.7 to evaluate dynamic voltage variation on power lines in a circuit [9]. The capturer consists of a probing front end circuit (PFE) to sense the voltage variation at the point of probing, and the output voltage of PFE is in-place digitized with the help of on-chip reference voltage and sample timing generators. Power noise waveforms on V_{DD} and V_{SS} traces of the SR are acquired by the on-chip measurement. The voltage and timing resolutions can be adaptive and typically of the orders of 100 uV and 100 ps, respectively.

4.1.4 Power Noise Frequency Response

On-chip power noise waveforms are compared between simulations using the method described in Sect. 4.1.1 and measurements in Sect. 4.1.3. The results are exemplified in Fig. 4.8 for a single clock cycle of F_{clk} in SR operation at 10 MHz, comparing simulation and measurements. Power line traces on the PCB have options whether to include or exclude an on-board decap of $C_{decap} = 1$ μF between the chip and an external power source, as also shown in the figure. The co-simulation with the unified PDN and capacitor charging models adequately captures the frequency domain power noise response.

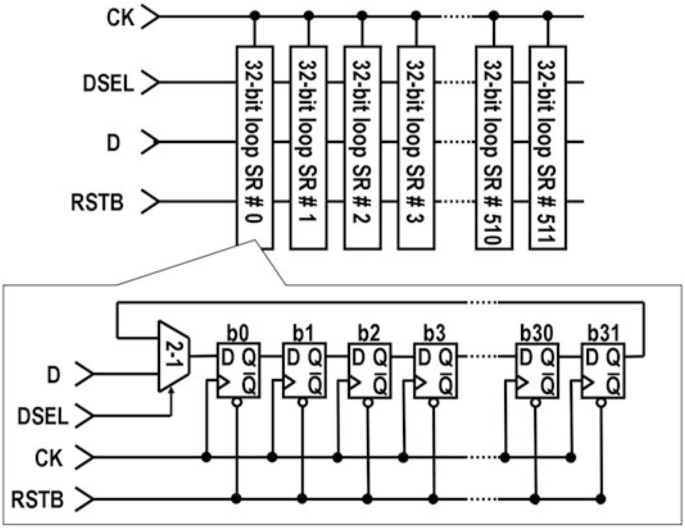


Fig. 4.6 Loop shift register (SR) circuit [1] (copyright 2011 IEEE)

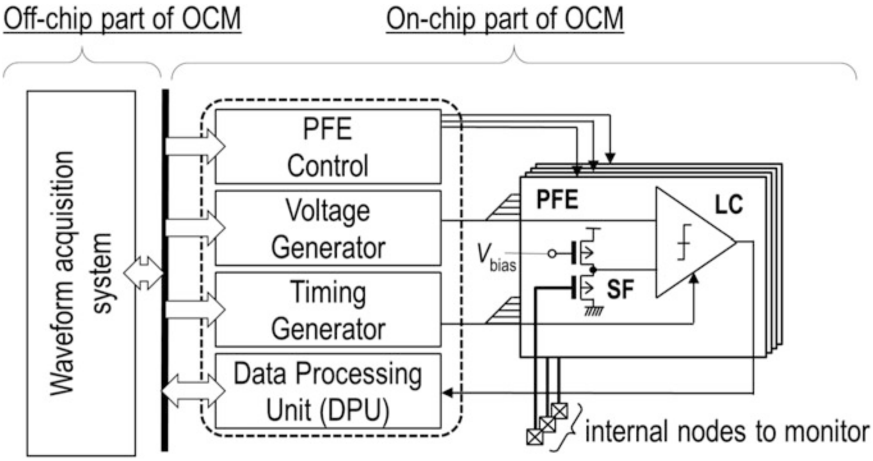


Fig. 4.7 On-chip waveform monitor (OCM) system

The frequency response is mainly governed by the power line impedance. The V_{DD} impedance seen from the power source terminal of the PCB is shown in Figs. 4.9a and 4.10a, for with and without the decap, respectively. The V_{DD} impedance exhibits a series LCR resonance since the end of the trace is openly terminated with C_{die}. On the other hand, the V_{DD} impedance seen from on-chip circuits, or from the point of AC power current consumption, is shown in Figs. 4.9b and 4.10b. The V_{DD} trace is considered virtually AC grounded at the power source

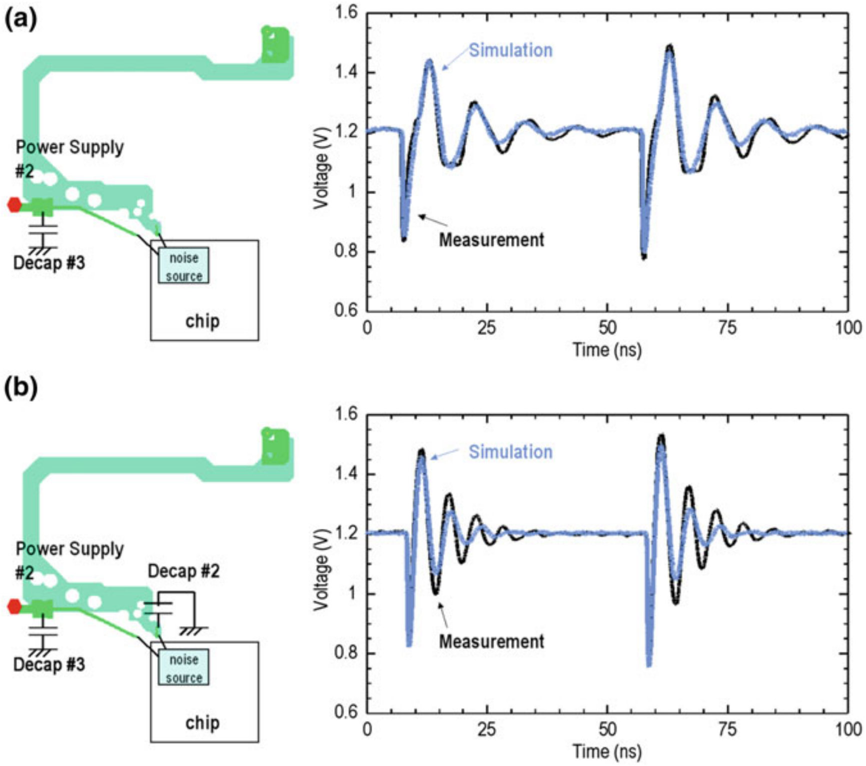


Fig. 4.8 On-chip power noise waveform in V_{DD} of SR, **a** without on-board decap and **b** with on-board decap. Power trace on PCB is also shown [6] (copyright 2012 IEICE)

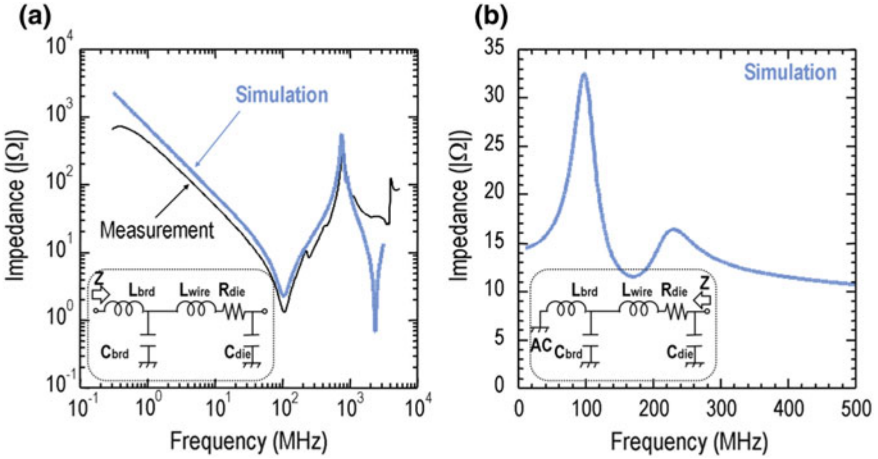


Fig. 4.9 Frequency response of **a** PDN series impedance seen from power supply terminals and **b** PDN parallel impedance seen from circuits inside chip, without on-board decap [1] (copyright 2011 IEEE)

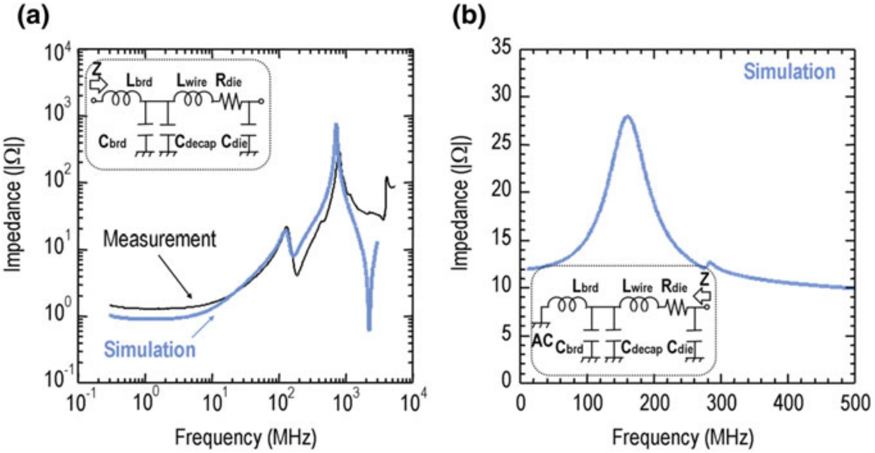


Fig. 4.10 Frequency response of **a** PDN series impedance seen from power supply terminals and **b** PDN parallel impedance seen from circuits inside chip, with on-board decap [1] (copyright 2011 IEEE)

for AC power current, and hence its response seen from on-chip circuits experiences parallel resonance [10]. While the V_{DD} impedance is measurable with the case of series resonance, the parallel resonance is of prime interest in terms of power noise analysis.

The frequency components of power noise waveforms are compared in Fig. 4.11 both in simulation and measurements. It is obviously shown that the distribution of frequency components is strongly characterized by the parallel resonance. The frequency components with the significant magnitudes, as well as the width of frequency distribution, are in accordance with the resonance frequency F_{res}. The

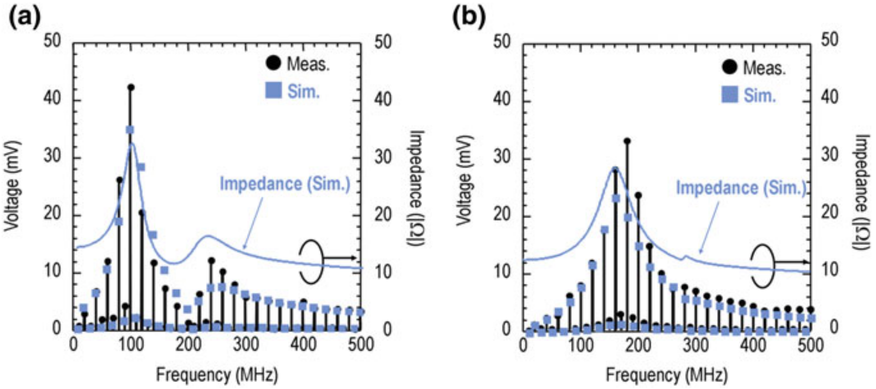


Fig. 4.11 Frequency components of on-chip power noise with F_{clk} = 10 MHz, **a** without on-board decap and **b** with on-board decap [1] (copyright 2011 IEEE)

first resonance frequency approximately at 120 MHz comes mainly from C_{die} = 175 pF derived from layout parameters and L_{wire} of 10 nH from the typical length of bonding wires. The board capacitance, C_{brd}, is smaller than 5 pF and negligible. The inclusion of 1-μF decap significantly reduces the first resonance, while making the second one at approximately 200 MHz to be noticeable. The demonstrated chip-package-board combined PDN analysis will actualize intentional tuning of F_{res} for suppressing EM interference at the frequencies of interest.

The co-simulation also predicts power current flowing on the PCB V_{DD} traces, which is associated with the measurement results with a near-field magnetic probing. The most significant frequency component of the AC power current is derived as the function of F_{clk}, as shown in Fig. 4.12. The largest AC power noise is found when the operation frequency is equal to the half F_{res}. This comes naturally from the fact that a clock distribution network of the SR consumes large portion of power current at every signal transition either in rise or fall direction. The EM noise emission from a digital IC chip can be computed with the combination of power current generation of circuits and antenna propagation through power supply traces.

4.1.5 EMC Awareness in IC Chip Design

Power noise simulation provides the ways to evaluate dynamic power currents consumed by IC chips in time-domain operation and to estimate EM emissions in a frequency domain. This facilitates the design of an electronic system in compliance with EMC regulations. The accuracy of power noise simulation is governed by the underlined techniques to draw active and passive parts of a PDN in completing the

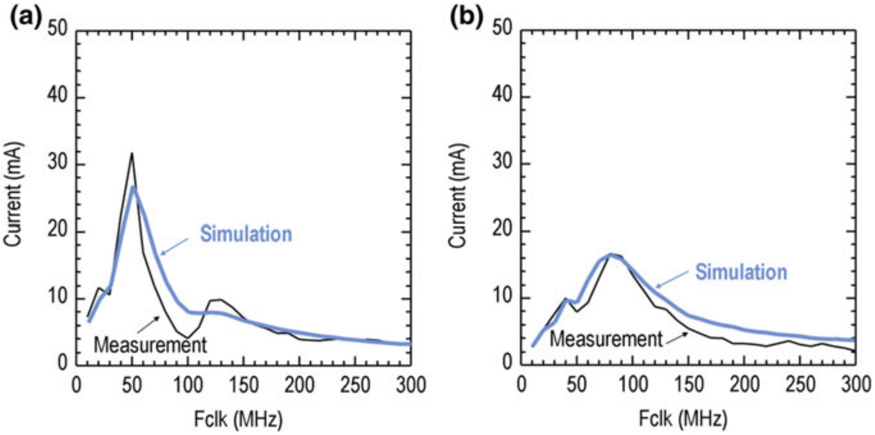


Fig. 4.12 Most significant frequency component of power noise current flowing on-board V_{DD} trace by near-field magnetic probing, **a** without on-board decap and **b** with on-board decap [1] (copyright 2011 IEEE)

design of a whole system, including chip-package-board interaction. There are generally conceived standard modeling technologies like chip power model (CPM) and associated broadband PDN models for this objective, created by and handled in commercially available electronic design automation (EDA) software. The on-chip waveform monitoring technique quantitatively evaluates the correlation between simulation and measurements of power currents and EM interferences in existing designs. This helps to set up a certified analysis flow against EMC problems for future developments.

This section studies mostly on EM noises around resonating frequencies inherent to a PDN with chip-package-board interaction, as the most fundamental cause of EMC problems. On the other hand, the high-frequency EM wave emissions due to clocking and associated synchronous signal transitions can also exist and potentially interfere with radio frequency circuits [11]. This is actively discussed in the research areas of signal and power integrity (not given in this section).

4.2 Electromagnetic Noise Immunity in Memory Circuits

Makoto Nagata, Kobe University

4.2.1 Susceptibility of IC Chip to EM Noise

An IC chip is potentially susceptible to EM noise, either internally through direct coupling of EM waves with on-chip circuits or externally by the interactions of EM waves with parasitic antennas on cables. In order to simplify and evaluate such the various origins of susceptibility problems in a consistent way, the world standardized methodology of measuring the susceptibility of an IC chip has been established [12]. The probability of erroneous operations of an IC chip is evaluated in response to incoming conductive radio frequency (RF) power, under the direct power injection (DPI) method. Figure 4.13 depicts the measurement setup. An RF signal at the frequency of F_{rf} from a signal generator (SG) is amplified (AMP) and then forwarded to a specified pin of an IC chip in a package. The net power, P_{net}, injected into the die is calculated from forward (P_{fwd}) and reflect (P_{ref}) power measured by power meters after a directional coupler, according to (4.2.1). A bias-T network is introduced at the point of injection of RF signal to properly supply DC voltage (e.g., V_{DD}) to the pin of interest.

$$P_{\mathrm{net}} = P_{\mathrm{fwd}} - P_{\mathrm{ref}} \tag{4.2.1}$$

The IC chip under DPI can assert a special flag bit of “reset” or record the number of erroneous bits in data, by using watch dog or built-in self test (BIST)

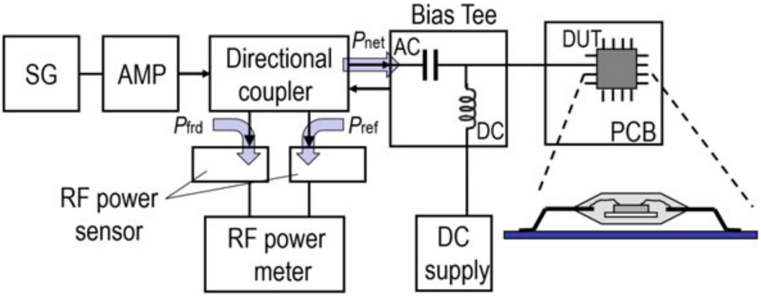


Fig. 4.13 Direct RF power injection method [16] (copyright 2011 IEEE)

capability, respectively. The susceptibility of an IC chip is evaluated by the minimum net power in DPI to cause a certain probability of erroneous operations, P_{min}, as the frequency of F_{RF}.

In some reports, the larger P_{min} is measured for the higher F_{rf} in the medium range of RF frequencies (e.g., up to 500 MHz), suggesting the smaller susceptibility of integrated circuits to the higher frequency incoming noise [13]. The high-power RF with F_{rf} of 1 GHz or higher can create more complex responses and sometimes lead to catastrophic events, due mostly to transistor-level parasitic capacitive couplings between circuits.

It has been observed that a microprocessor in an electronic control unit (ECU) exhibits frequent unexpected transitions to the “reset” mode under DPI, with increasing P_{min} for higher F_{rf}. The variation of the delay time of a logic gate and signal chains also shows the similar response under DPI [14, 15]. On the other hand, this section focuses on the EM susceptibility (EMS) of static random access memory (SRAM) [16–18]. Since a binary digital value is carried by analog waveforms and processed in memory circuit operation, the voltage variations due to DPI will impact on digital results through analog response. The measurement-based approach using on-chip waveform monitoring (OCM) in this section will greatly help to probe the EMS of general digital ICs.

4.2.2 DPI on SRAM Core

The SRAM core is of prime interest in EMC of digitally controlled systems with high reliability, for such as automotive and industrial applications. This is because of its usage as critical data and program storage, and the substantial occupation of silicon areas in a system-on-chip (SoC) die for supporting high-computation capabilities. The design for EMC of SRAMs becomes more prerequisite for SoCs in many-core architectures and using more advanced low-voltage CMOS technologies.

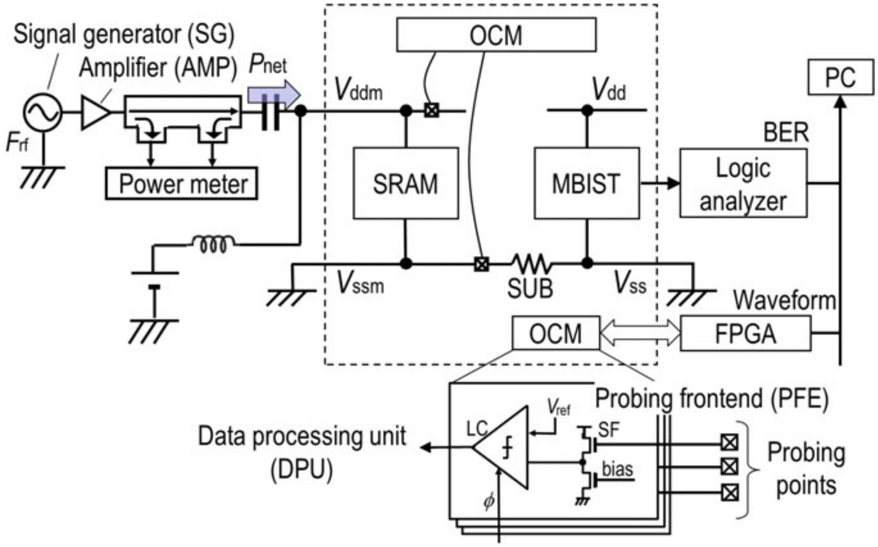


Fig. 4.14 System diagram of susceptibility evaluation of SRAM core [18] (copyright 2015 IEEE)

The system diagram of Fig. 4.14 shows how DPI is used for evaluating the susceptibility of an SRAM core against EM noise, in combination with the memory BIST (MBIST) and on-chip waveform monitoring (OCM). The MBIST realizes the on-chip diagnosis of bitwise SRAM write/read operation. The MBIST generates word data with bit patterns like a checker board or alternate lines and writes the data in the SRAM core under test (CUT). Then, the MBIST reads all data out from the CUT and check the correctness of data in a bitwise manner. The write-in and read-out sequences are iterated (with bit patterns reversed in each sequence) and all the erroneous bits are cumulatively stored in the MBIST. Finally, the MBIST calculates the bit error rate (BER) as the average number of erroneous bits divided by the total number of bits. The location of erroneous bits in the memory cell array can also be drawn in an erroneous bit map. The MBIST can be programmed and its data can be accessed by external logic structures in field programmable gate array (FPGA) device.

When a single error is found in average among the BIST iterations, the BER is calculated to be 7.6e-6 for a 16 k byte SRAM core. The BER is evaluated under the DPI as a function of RF power, RF frequency, SRAM power supply voltage (V_{ddm}), and SRAM operation frequency (F_{clk}). Figure 4.15a demonstrates that the BER increases for increasing P_{net} of RF disturbance. It is also seen that a SRAM is more susceptible for smaller DC supply voltage of V_{ddm}. In addition to the conventional DPI, the OCM measures the sinusoidal voltage variations induced by the RF signal,

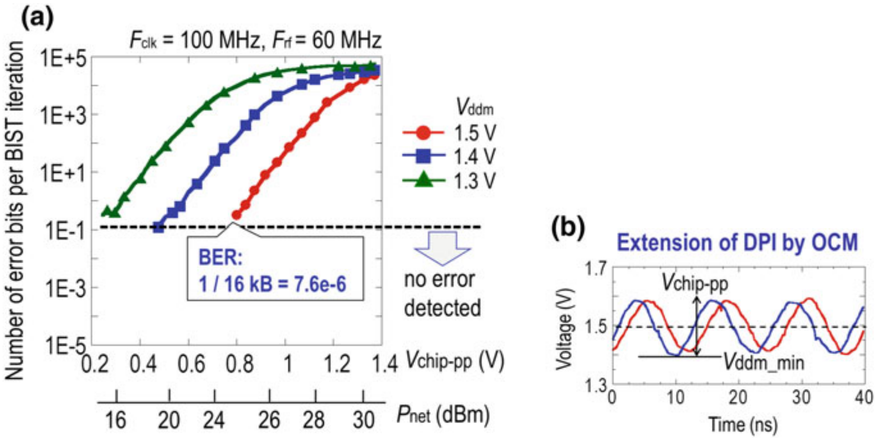


Fig. 4.15 Measured BER versus P_{net}. On-chip voltage variation is also given

at the power supply node of the SRAM core, as exhibited in Fig. 4.15b. The magnitude of voltage variation is derived as $V_{chip\text{-}pp}$ from the on-chip waveform captured for each DPI condition. The minimum instantaneous voltage due to the variation is also measured as V_{ddm_min}. Since transistors in SRAM cells operate under source–drain voltage, it is better to interpret the relationship between the susceptibility of an SRAM core in the DPI with the voltage variables that are only measurable by the OCM. This is the extension of the DPI method toward the understanding of circuit-level interactions with the conductive RF power due to EM coupling. Again in Fig. 4.15a with dual x-axes, the BER monotonically increases for the larger $V_{chip\text{-}pp}$ that is induced by the larger P_{net}. It is interesting to note that there is a certain threshold of $V_{chip\text{-}pp}$ under which no single-bit failure is found during BIST iterations. This threshold voltage depends intrinsically on the design of an SRAM core and also the technology of transistors used.

4.2.3 *Frequency Response in DPI*

The minimum RF power in DPI to cause a single-bit failure during BIST iterations is defined as P_{net_min}. It is measured as the function of F_{rf} for the 16 k byte SRAM core under operations with different F_{clk} as given in Fig. 4.16a. The larger P_{net_min} is measured for the higher F_{rf}. This is consistent with the general trend found in the reported DPI of integrated circuits [13–15] as addressed in Sect. 4.2.1. In response to the larger P_{net_min}, the supply voltage of SRAM cells experiences the higher drop of $V_{ddm\_min,}$ as measured in Fig. 4.16b by the OCM. The standard supply voltage of

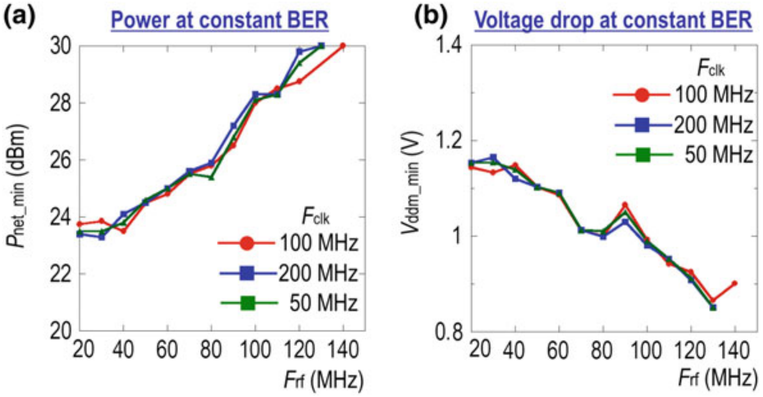


Fig. 4.16 Frequency dependency of DPI; **a** BER versus $P_{\mathrm{net\_min}}$ and **b** BER versus $V_{\mathrm{ddm\_min}}$ [17] (copyright 2015 JSAP)

1.5 V was given. The relation of $P_{\mathrm{net\_min}}$ or $V_{\mathrm{ddm\_min}}$ on F_{rf} is almost independent on the F_{clk}, showing that the EM susceptibility in the SRAM core is irrelevant to the relative phase difference between the RF sinusoids and the SRAM clock signal, or the relative timing difference between the voltage drop and SRAM operations.

The V_{ddm} of SRAM cells is often internally isolated in an SRAM core from the other power domain of V_{dd} for the peripheral circuits of digital access control (e.g., address decoding) and analog signal processing (e.g., bit line voltage sensing and amplification), as depicted in the simplified power supply network of Fig. 4.17. This is mainly for the enhancement of static operation margins of an SRAM core, by intentionally introducing a slight DC voltage difference between V_{ddm} and V_{dd} or even by controlling back-gate voltage of transistors only in SRAM cells. On the other hand, the DPI may introduce the undesirable voltage difference between the supply voltages of SRAM core and SRAM periphery, and bring about the collapse of binary data. Since the power domains involve highly capacitive couplings due naturally to their very dense transistor placements as in Fig. 4.17, the higher frequency of DPI on V_{ddm} induces sinusoidal voltage variations even similarly on V_{dd} by the capacitive coupling and results in the reduced relative voltage difference between them. This is one of possible qualitative explanations for the insensitiveness of an SRAM core against the high-frequency DPI. Many other physical mechanisms can be simultaneously present regarding EM noise interactions, and advanced analysis methodologies are needed for thorough and quantitative understandings of EMS. The mitigation techniques will be also derived in conjunction with the design of power delivery network (PDN) in the next section.

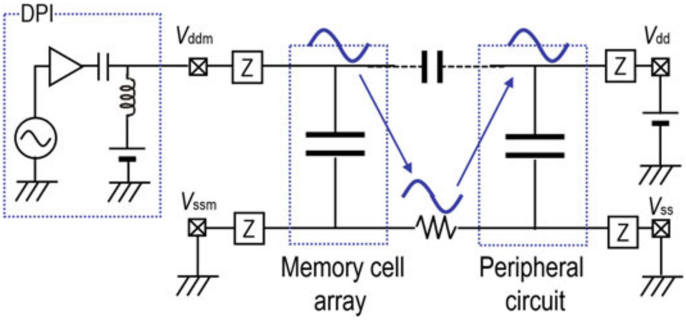


Fig. 4.17 Capacitive coupling in SRAM core [16] (copyright 2011 IEEE)

4.3 Power Noise of IC Chips in Assembly and Its Mitigations

Makoto Nagata, Kobe University

4.3.1 IC Chips in Assembly

An integrated circuit (IC) chip is normally packaged and mounted on a printed circuit board (PCB) in its practical usage in applications. The IC chip-package-board interaction provides a decisive impact on the overall electromagnetic (EM) response of an IC chip in assembly, as discussed in Sects. 4.1 and 4.2. Here, it will be shown that the system-level power delivery network (PDN) exhibits strongly frequency dependent power line impedance that characterizes power noise seen at locations on a PCB and in an IC chip, and specially induces unacceptably large noise components at the frequencies of resonance. The property of PDN is passive and governs not only EM interference (EMI) but also EM susceptibility (EMS), namely outgoing as well as incoming EM noises in wide frequencies, respectively. This section focuses on an autonomous tuning technique of PDN impedance, potentially mitigating both EMI and EMS problems.

A system-level PDN is intentionally embedded with capacitors between V_{DD} and V_{SS} for sustaining power line impedance below a specified level in the frequency range of interest. A large capacitor on the order of µF is placed often around power source terminals on a PCB for suppressing low-frequency power noises. The other capacitors on the order of nF are at the sources of power noise (power current consumptions) within an IC chip for high-frequency ones. As demonstrated in Figs. 4.8, 4.9, and 4.10, such a decoupling capacitor (C_{decap}) effectively reduces power line impedance only within a certain range of frequency. This limitation comes inevitably from the parasitic effective inductance and resistance in series to the capacitor, L_{ESL} and R_{ESL}, respectively. A self-resonance occurs approximately at the frequency of $F_{\mathrm{res}} = 1/(2\pi\sqrt{L_{\mathrm{ESL}}C_{\mathrm{decap}}})$ and the power line impedance enlarges for the frequency larger than F_{res}. A power noise waveform exhibits oscillation at F_{res} with excitations such as active circuit operations, while decaying with the approximate time constant of $L_{\mathrm{ESL}}/2R_{\mathrm{ESL}}$ after the termination of circuit operation.

It is noted that the power line impedance is fixed after the assembly of an IC chip, and therefore there is a need of post-silicon manufacturing techniques to optimize power line impedance over the frequencies of interest. An IC chip-package-board co-analysis/co-simulation technology has been intensively developed as a tool used in search of remedy for this purpose by the community of IC manufacturers, application system producers, and EDA software vendors. This demands a chip-level equivalent model of PDN and an electrical model of a package lead frame as well, and is still under active discussions for generalization. Another approach is to provide a chip-level adaptability of on-chip PDN parameters for an IC chip in actual operation environment. Design examples will be discussed in this section.

4.3.2 Power Noise Mitigation by Evading PDN Resonance

A PDN exciter intentionally brings about the resonance in the PDN of interest of an SoC die in assembly, as illustrated in Fig. 4.18. The exciter induces a pulse-like power current in the PDN by transistor switches to connect V_{DD} and V_{SS} for a very short period of time. An on-chip waveform monitor (OCM) captures power noise waveforms after the excitation. The waveforms are postprocessed by an on-chip PDN analyzer for deriving electrical characteristics of the PDN.

The system-level construction of an IC chip using the PDN analyzer is given in Fig. 4.19 [9]. There are PDNs with different voltage domains for the SoC core

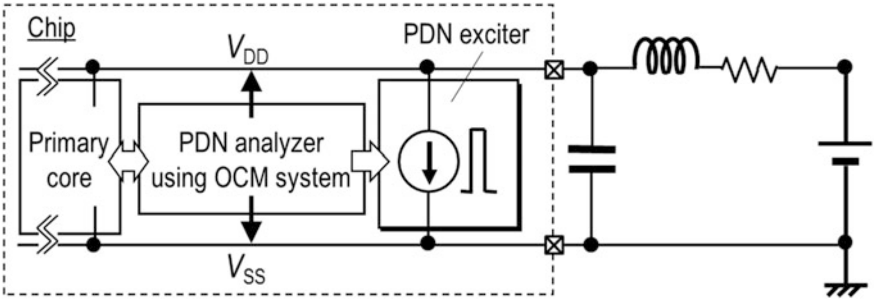


Fig. 4.18 PDN system having a PDN exciter for in-place analysis of PDN resonance

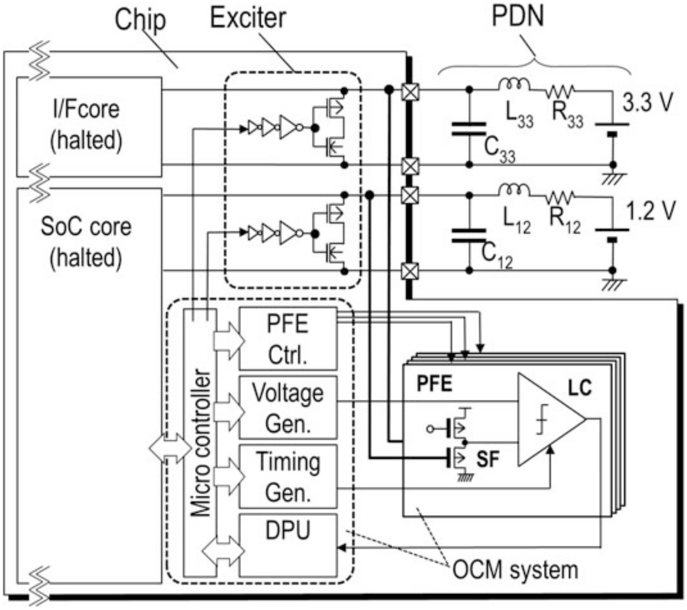
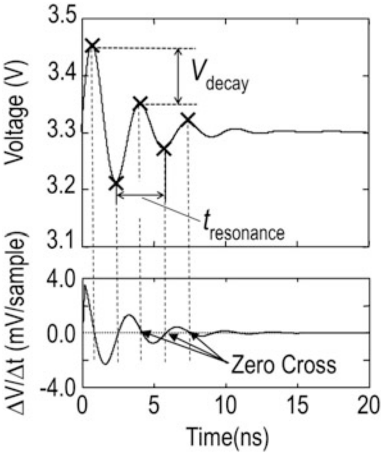


Fig. 4.19 Construction of system-on-chip embedding PDN analyzer and PDN exciter

Fig. 4.20 PDN resonance waveform and characterization [9] (copyright 2011 IEEE)



(e.g., 1.2 V) and interface (I/F) core (e.g., 3.3 V) circuits. The SoC and I/F circuits are properly supplied with power while halted or in a reset mode to eliminate naturally continuous excitations in the background. The PDN with parasitic L, C, and R components suffers from oscillatory voltage variation with decaying its amplitude by time after this single excitation, as demonstrated in a typically

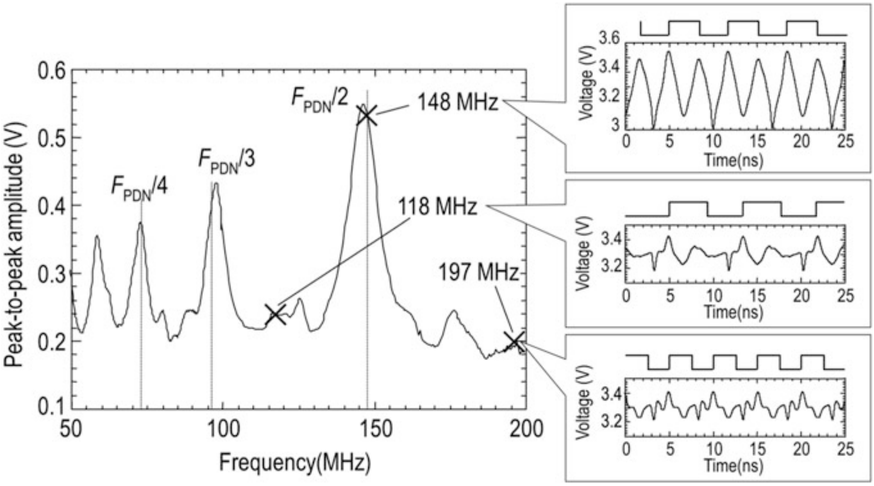


Fig. 4.21 Measured V_{pp} of power noise in digital circuits versus operating frequency of F_{clk} [9] (copyright 2011 IEEE)

measured waveform of Fig. 4.20. The analyzer determines the oscillating period of resonance ($t_{resonance}$) and the decay constant (t_{decay}) from the series of timings at maximum or minimum voltage and the decay in voltage (V_{decay}), respectively. The OCM functionality of Fig. 4.7 is enhanced with an on-chip monitor controller to execute automated sequences of the PDN excitation, waveform acquisition and analysis.

The periodical PDN excitation leads to intentionally stationary oscillation due to the PDN resonance. The peak-to-peak voltage of the oscillation is drawn against the frequency of excitation, from 50 to 200 MHz, as shown in Fig. 4.21. PDN oscillation exhibits a considerable increase when the excitation frequency matches the integer inverse of the resonance frequency, $F_{PDN} = 1/t_{resonance}$. This provides a scenario for an SoC die to autonomously search the resonating frequencies in its practical usage environment after assembly, with the support of enhanced OCM functionality, and also select the frequency of operation evading from the PDN resonance. The operating frequency of circuits, F_{clk}, can be chosen in this example such that it does not lie in the vicinity of F_{PDN} and its integer inverse frequencies, F_{PDN}/i ($i = 1, 2, 3, \ldots$). This will avoid the enlargement of power noise due to the PDN resonance. The reduction of F_{clk} from the nominal operating frequency at 148 to 118 MHz −19%) results in a 55% decrease in the power noise amplitude, as shown in Fig. 4.21 (measured waveforms are also shown). Similarly, with the increase of F_{clk} to 197 MHz (+30%), the noise amplitude is reduced by 64%. The former is chosen under the constraints of power consumption while the latter under

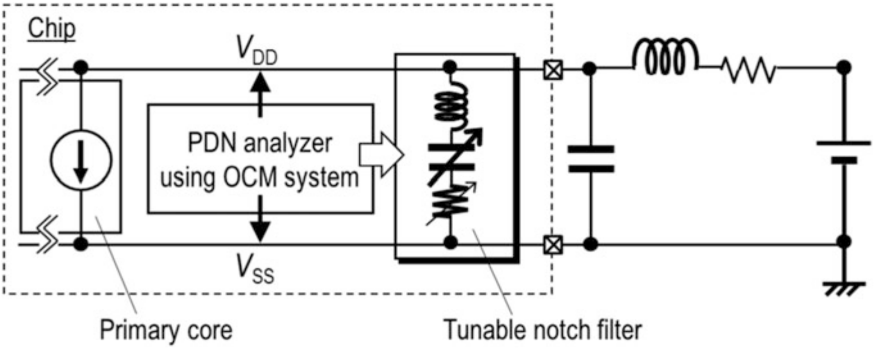


Fig. 4.22 PDN system embedding tunable notch filter for power noise reduction

the performance. These frequencies are reasonably located at the mid-point of adjacent pairs of F_{PDN}/i and $F_{\mathrm{PDN}}/(i-1)$ and can be computed during the on-chip PDN characterization.

4.3.3 Power Noise Mitigation by Suppression of PDN Resonance

The peak height of power noise at the frequency of PDN resonance can be suppressed by a tunable notch filter, given in Fig. 4.22. The filter consists primarily of bonding wire inductance in a package and an on-chip configurable capacitor in series, as shown in Fig. 4.23 [19]. A programmable resister is also included. The capacitor uses the gate capacitance of metal-oxide-semiconductor (MOS) transistors. The number of effective transistors are set by forcing each gate electrode to the high (turn on) or the low (cut off) bias condition, according to the digital codes of C_{code} for capacitance. The coupled bonding wires effectively increase their inductance, owing to the flow of power supply current. The structure is essentially passive and avoids the increase of power current consumption associated with noise suppression, in contrast to the use of active circuits [20–22]. The effect of noise suppression is maximized by searching C_{code} of the filter in response to V_{pp} measured by the PDN analyzer. Another code of R_{code} for resistance is only used for the additional dumping that is needed in power noise waveforms. The power supply noise was on-chip measured as the voltage variation on V_{DD} at the location of the filter and the associated suppression is demonstrated in Fig. 4.24, achieving 43% reduction of the height of voltage noise peak.

The power noise mitigation techniques of Sects. 4.3.2 and 4.3.3 are evaluated by on-chip power noise waveforms. They are simultaneously effective for the EM noise on power traces of PCB, since their essential constructions remain to be a passive PDN network.

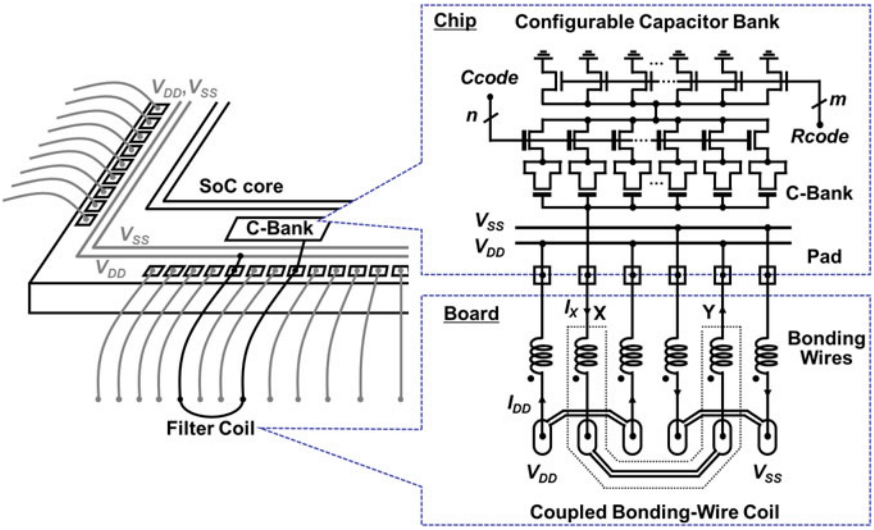


Fig. 4.23 Construction of tunable notch filter

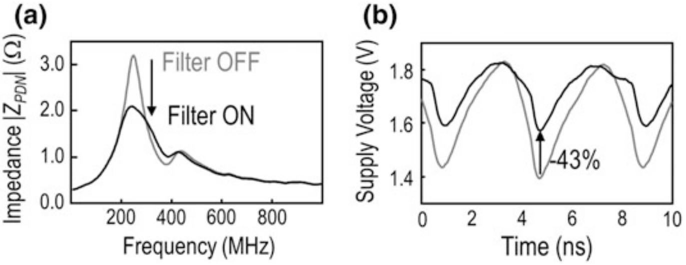


Fig. 4.24 Measured power noise waveforms [19] (copyright 2014 IEEE)

4.4 Responsive Link for Noise-Tolerant Real-Time Communications

Nobuyuki Yamasaki, Keio University
Yusuke Kumura, Keio University
Shuma Hagiwara, Keio University
Masayuki Inaba, The University of Tokyo

4.4.1 Noise-Tolerant Real-Time Communication

Recently, complex distributed control systems such as humanoid robots have appeared in various fields. In order to make the distributed control systems dependable, internode communication with real-time capability and dependability is crucial. Especially, noise tolerance is indispensable, since noise has a huge influence on communication quality. For example, our target system is driven by high voltage (80 V) and high current (200 A) that can generate huge noises. For noise-tolerant real-time communication, we have been researching and developing a communication standard, called *Responsive Link* [23] that can meet the requirements of real-time capability and noise tolerance. This chapter introduces brief introduction of *Responsive Link* and shows evaluations of the noise tolerance.

4.4.2 Responsive Link

A real-time network, guaranteeing communication deadlines, is now an indispensable element in distributed real-time systems. There are many communication standards for various applications, including Ethernet [24], IEEE 1394 [25], and USB [26].

Ethernet is a cheap and popular communication interface used by most PCs. When communication collisions occur, the packets are retransmitted, as CSMA/CD is used. Therefore, it is difficult to bound the worst case communication time.

IEEE 1394 enables isochronous data transfer among computers, peripherals, and consumer electronics products. IEEE 1394 has some problems as a real-time communication in distributed real-time systems. Error correction is not supported at the isochronous data transfer mode. The maximum node number is limited up to 63 nodes. All networks are reset in case of hot plug and play. Network topology is fixed (chain, star, and tree), and the loop topology is not allowed.

USB is widely used to connect peripherals to PCs so that various I/O devices can be easily connected to PCs. USB has also some problems as a real-time communication in distributed real-time systems. The maximum node number is limited up to 127 nodes. Network topology is fixed to the tree structure. The loop topology is not allowed. And the root controller is required.

Therefore, these communication standards are not suitable for distributed real-time systems, and hence new real-time communication standard is required.

Responsive Link is an internode communication standard (ISO/IEC 24740:2008) [27] that accommodates separated communication channels for events and data, preemptive packet overtaking and switching, and error correction for some purposes. *Responsive Link* is implemented on responsive multithreaded processor (RMT Processor) [28, 29] designed for distributed real-time systems. The detail of RMT processor is described in Chap. 9, Sect. 9.2.

4.4.2.1 Separation of Communication

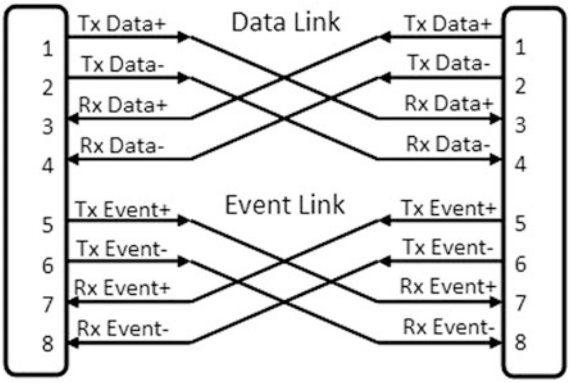
There are two types of real-time communication: hard real-time communication and soft real-time communication. On one hand, hard real-time communication requires strict time constraints allowing no delay to deadline. Control systems require this type of communication, putting more emphasis on latency than throughput. On the other hand, soft real-time communication is more tolerant to delay, and requires higher bandwidth. For example, a multimedia system requires this type of communication, putting more emphasis on throughput than latency, because the amount of data processed is large and the latency is not severe in the system. There is a trade-off between throughput and communication delay in real-time communication, and requirements of hard and soft real-time applications including a degree of time constraints are different. Therefore, *Responsive Link* is designed to support both hard and soft real-time communication by physically separating communication lines: Event link and data link. Because it is difficult to build a hard real-time system by using conventional communication standards that share a single communication line for both data and events, making the estimation of the communication latency of events more difficult.

Communication line for hard real-time communication is called event link. The other communication line for soft real-time communication is called data link. These transmission lines are separated as shown in Fig. 4.25. The specification of Responsive Link connector is as follows:

- Tx Data+/Data−, which is a differential signal, transmits data packets.
- Rx Data+/Data−, which is a differential signal, receives data packets.
- Tx Event+/Event−, which is a differential signal, transmits event packets.
- Rx Event+/Event−, which is a differential signal, receives event packets.

The fixed size packet is desirable in order to estimate the latency accurately and make hardware simpler. On one hand, if the packet size becomes larger, the throughput becomes higher. However, the packet latency becomes longer. On the other hand, if the packet size becomes smaller, the packet latency becomes shorter, while the throughput becomes lower, because the overhead relatively increases. Considering this trade-off, on one hand, the packet size used in event link is small 16 bytes in order to shorten the communication latency. On the other hand, data link packet is larger 64 bytes to achieve higher throughput as shown in Fig. 4.26.

Fig. 4.25 Interface of Responsive Link



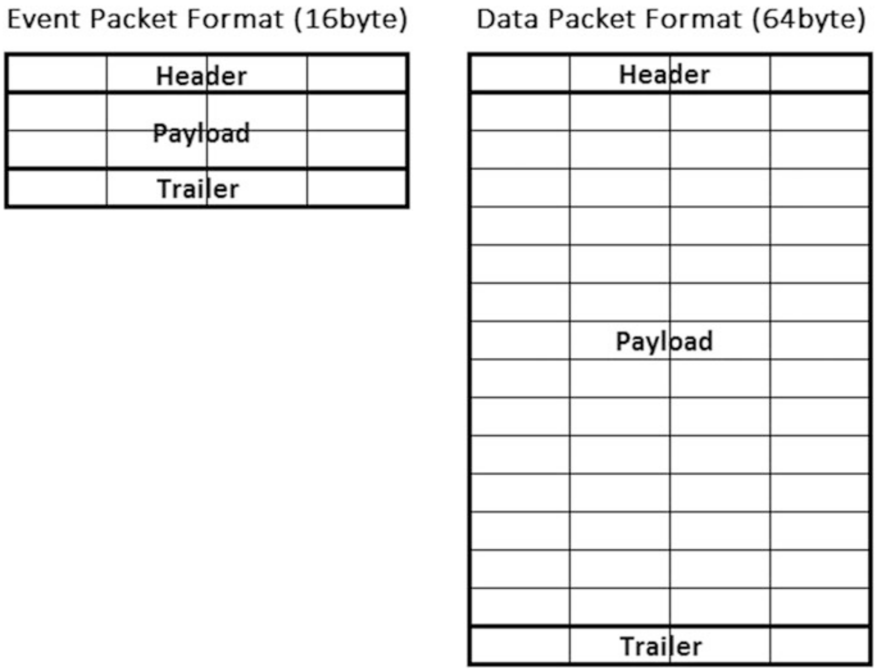


Fig. 4.26 Packet format in Responsive Link

4.4.2.2 Priority-Based Packet Overtaking

In the field of real-time task scheduling, preemptive context switching is required to process real-time tasks. In the same way, preemptive communication, a packet with higher priority overtakes other packets with lower priority, is required so that real-time scheduling algorithms can be applied to real-time communications. Therefore, priority-based packet preemption function is designed and implemented on *Responsive Link*.

Figure 4.27 shows a 5 by 5 Responsive Link switch. Port 0 is connected to a local device, such as the node processor, and Ports 1–4 are connected to external ports. A packet arriving at an input port without collision is transferred to an output port specified by the routing table. When a collision occurs, i.e., multiple packets request the same output port simultaneously, the packet with the higher priority is transmitted first and other packets are stored temporally in the overtaking buffer. A packet with higher priority overtakes the packets with lower priority at every hop of nodes.

The header of an arriving packet is stored in the overtaking buffer. Its output port (s) is/are looked up from the routing table, and each output port finds the packet with the highest priority. If a conflict occurs, packets with lower priority are stored in the overtaking buffer until packets with higher priority to be transmitted. In addition to the overtaking buffer, off-chip backed-up memory is designed and implemented to prevent packet overflow in the overtaking buffer. On one hand,

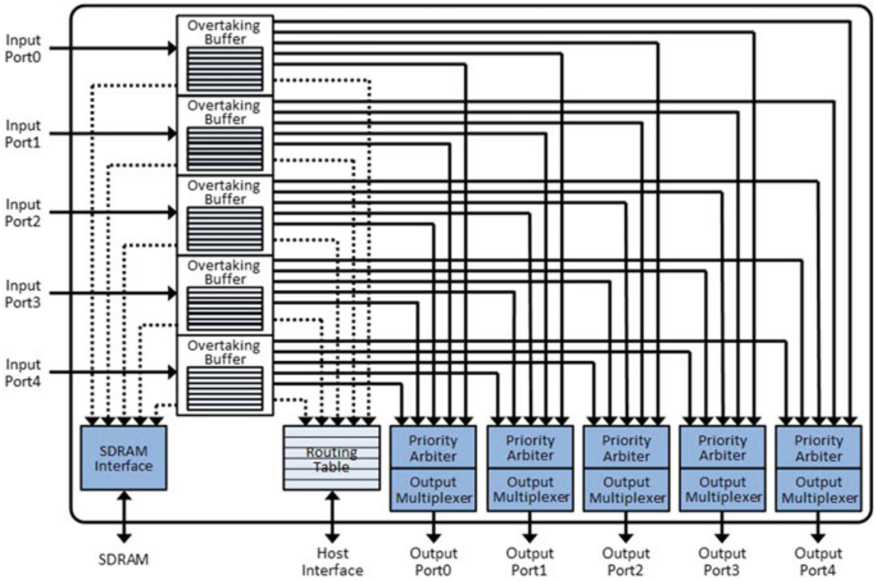


Fig. 4.27 Network switch

when the entry of an overtaking buffer runs out, the lowest priority packet in the overtaking buffer is saved into the off-chip memory (DRAM) automatically. On the other hand, when the entry of the overtaking buffer becomes available, it restores the saved packets to the overtaking buffer in priority order. With this functionality, preemptive communication, existing real-time scheduling algorithms can be applied to real-time communication.

4.4.2.3 Priority-Based Routing

End-to-end connection can be established with *Responsive Link* by setting routing tables of all nodes along the path from a source node to a destination node. *Responsive Link* can connect up to 2^{32} nodes with an arbitrary network topology, and the supported priority level is 256.

Each node has a routing table to control the packet routing and the priority replacement function. Figure 4.28 shows the routing table of a network switch with five inputs and five outputs.

In addition to network address, priority bits in the packet are also used to match the routing table as shown in Fig. 4.29. Therefore, different route can be set to the same network address for different priorities. For example, detours and exclusive communication lines can be set. The route with priority “0” is used as the default route for the network address.

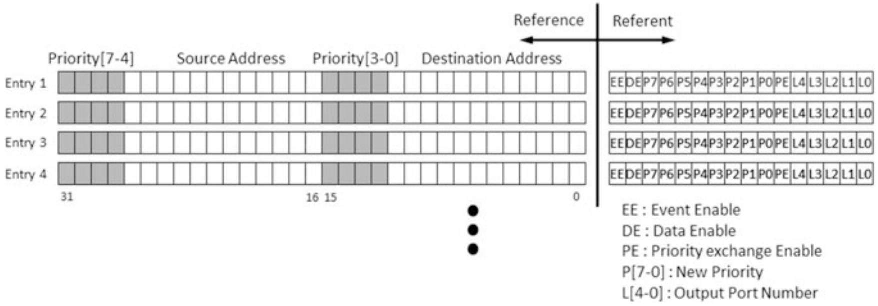
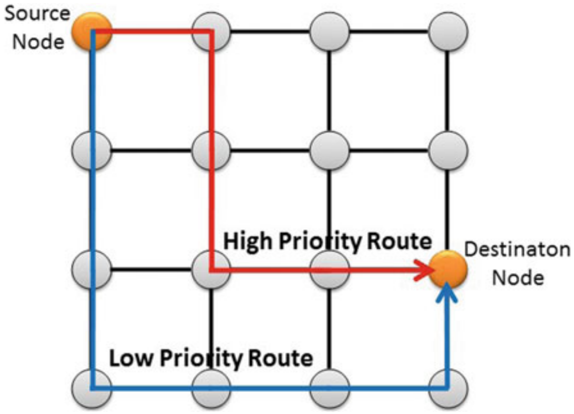


Fig. 4.28 Routing table

Fig. 4.29 Packet routing with priority



In addition, *Responsive Link* can accelerate and decelerate packets by changing the their priorities. The priority of a packet can be replaced with a new priority level at each node, and the new priority is used at next node. This packet control can be realized by setting the routing table appropriately by software.

4.4.2.4 Communication Speed and Adaptive Codecs

The link speed can be dynamically changed (800, 400, 200, 100, and 50 Mbaud). The *Responsive Link*'s communication latency per hop is 0.27 μs (800 Mbaud) to 76.8 μs (50 Mbaud), which satisfies the communication requirement (that is, less than 100 μs) even when several tens of controllers are connected. *Responsive Link* employs embedded clock serial communication. Also, multiple error detection and correction codes are employed to improve communication dependability. Appropriate code intensity and code rate can be selected as a function of given characteristic of transmission channel [29]. Internode communication is affected by the noise in the system. In order to improve the reliability in communication, *Responsive Link* supports any pair of ECC and line codes listed in

Table 4.1 Error-Correcting Code (ECC) and line codes

Type	Coding	ECC capability	Code rate
Byte level ECC	Reed solomon	1-byte error correction for 6 bytes	4 bytes are coded as 6 bytes
Bit-level ECC	Hamming	1-bit error correction for 12 bits	8 bits are coded as 12 bits
	BCH	2-bit error correction for 16 bits (random) 3-bit error correction for 16 bits (burst)	8 bits are coded as 16 bits
Line code	Nonreturn-to-zero-inverted (NRZI) + bit stuffing	N/A	8 bits are coded as 8–9 bits
	8b10b	N/A	8 bits are coded as 10 bits
	4b10b	1-bit error correction for 10 bits	4 bits are coded as 10 bits

Table 4.1. *Responsive Link* can dynamically configure any pair of ECC and line codes in response to the given priority and noise parameters. Basically, to configure a pair of ECC and line codes, we need a given environment's bit error rate, the communication cycle and deadline, and the communication data rate. The software uses these parameters to select the optimal combination that satisfies the time constraints and sufficient noise tolerance.

4.4.3 *Noise-Tolerant Real-Time Communication with Responsive Link*

4.4.3.1 Evaluation of Noise-Tolerant Error Correction Code: 4b10b

In order to build a highly dependable distributed system with real-time communication, a data transmission error fatally impacts the system. It is required to guarantee the data to be transferred correctly by using error correction codes. There exists a trade-off of code intensity and throughput. Therefore, the system has to have transmission lines with the appropriate ECC and line code under given circumstances including the noise level and the importance of transferring data. There are several advantages to be able to select various combinations of the ECC and line code and switch the settings depending on the given variable circumstances.

With a conventional line code such as nonreturn-to-zero-inverted (NRZI) and 8b10b, transferred data can be detected as multiple bits error even if the actual data on the line has 1-bit error. Therefore, we designed a new line code with ECC, called 4b10b that has higher noise tolerance by embedding error correction functionality to line code itself. The 4b10b employs embedded clock signaling, DC balancing

Table 4.2 4b10b translation table

4b	10b	4b	10b	4b	10b	4b	10b
0000	1100101100	0100	0111010001	1000	1001110001	1100	1011010010
0001	1011001100	0101	1100011001	1001	0111000110	1101	1001100110
0010	1100110010	0110	0101110100	1010	1010110100	1110	1010101001
0011	0110011100	0111	1101000101	1011	1101001010	1111	0110101010

and error detection and correction. Other codecs do not support all these functions, especially pertaining to error correction. The 4b10b is the first codec (line code) with ECC to fulfill them simultaneously. Each 4-bit data is transformed into 10-bit data using the lookup table as shown in Table 4.2. The 4b10b fulfills embedded clock signaling by not having three consecutive bits of "0" or "1" in encoded 10-bit data and five consecutive bits when 1-bit error occurs. In addition, it maintains the number of "0" and "1" in the 10-bit data to be the same for DC balancing. The hamming distance among every encoded 10-bit data is longer than 3. When decoding, transferred 10-bit data is looked up in the table, and decoded with minimum distance decoding. Error correction is possible because transferred data with 1-bit error can be uniquely determined with minimum distance decoding. Data with 2-bit error cannot be uniquely mapped to the original code, so error correction is not possible, but error detection is possible. Transferred data with more than 2-bit error cannot be detected as error. The 4b10b line code has been standardized at IPSJ as IPSJ-TS 0015:2015 [30].

Responsive Link supports Hamming code, BCH code, and Reed–Solomon code as error correction codes. For line code, NRZI with Bit Stuffing, 8b10b, and 4b10b that supports ECC can be selected.

4.4.3.2 Evaluation of Noise Tolerance with Responsive Link

In order to evaluate the noise tolerance of *Responsive Link*, we measured the packet error rate using the transmission lines with noise. Bit errors are defined as a bit inversion, and bit errors are inserted into the transmission packets. We generated random bit errors with the varying rate of error from the range 10^{-6} to 10^{-1}. The first 10 packets were transferred as warm-up, which we did not count in the results. And the next transferred 1,024 packets are measured and calculated as actual error.

We evaluated *Responsive Link* with a noise generator, constructing the environment with noise equivalent to an 80 V and 200 A motor driver. Dependable data communications in the highly stressed environment have been confirmed as shown in Fig. 4.30.

Figure 4.31 shows the packet error rates of three combinations of codecs. The line code heavily affects the noise tolerance. There is a trade-off between the noise tolerance and coding rate, i.e., effective throughput. In order to take a balance of noise tolerance and throughput, the application can configure an appropriate pair of ECC and line codes according to the given system environment. HAM4b10b means a combination of Hamming error correction code and 4b10b line code, HAM8b10b

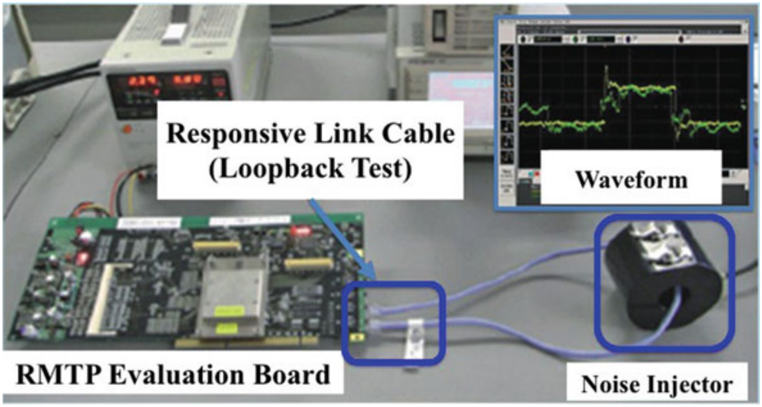
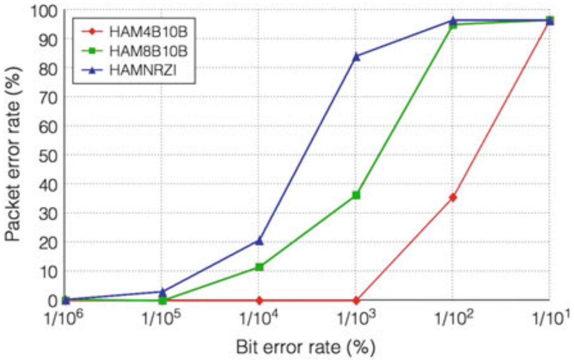


Fig. 4.30 Environment

Fig. 4.31 Bit error rate



means a combination of Hamming error correction code and 8b10b line code, and HAMNRZI means a combination of Hamming error correction code and NRZI line code. HAM4b10b with the largest ECC size has the lowest packet error rate in all codes. However, the throughput of HAM4b10b is the lowest due to the largest ECC size. Therefore, application developers can select and use these error correction codes and line codes with considering a trade-off between throughput and noise tolerance.

4.4.3.3 Noise Tolerance with Ferrite Core

Now the reinforcement technology to improve noise tolerance in *Responsive Link* is introduced. A ferrite core, which is a magnetic core, can help noise-tolerant real-time communication in *Responsive Link*. Figures 4.32 and 4.33 show examples of communication failure/success without/with a ferrite core. The yellow and purple waves are the differential signals of an event link measured by the single-end probe, which are noisy. Figures 4.32 and 4.33 measure communication signals at single edge trigger mode and at continuous auto run mode respectively. The blue wave is

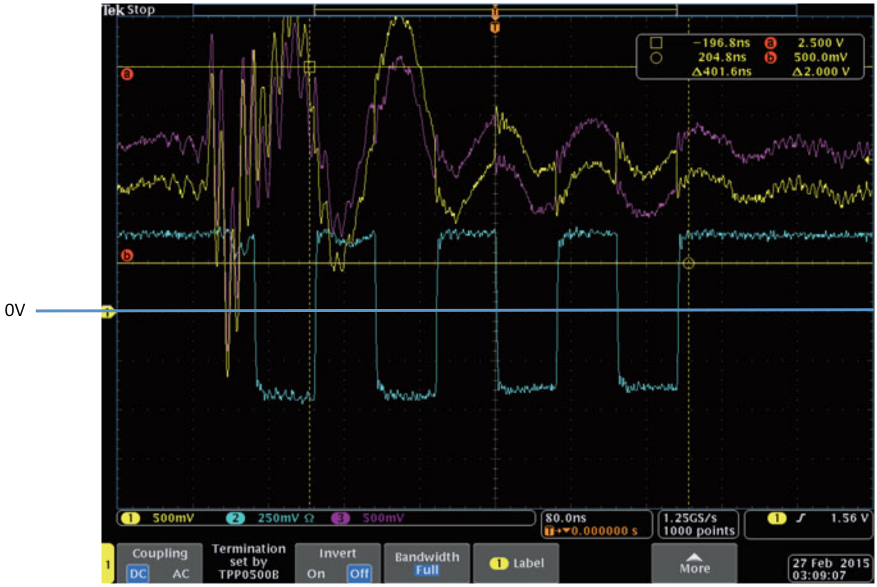


Fig. 4.32 Communication failure without ferrite core

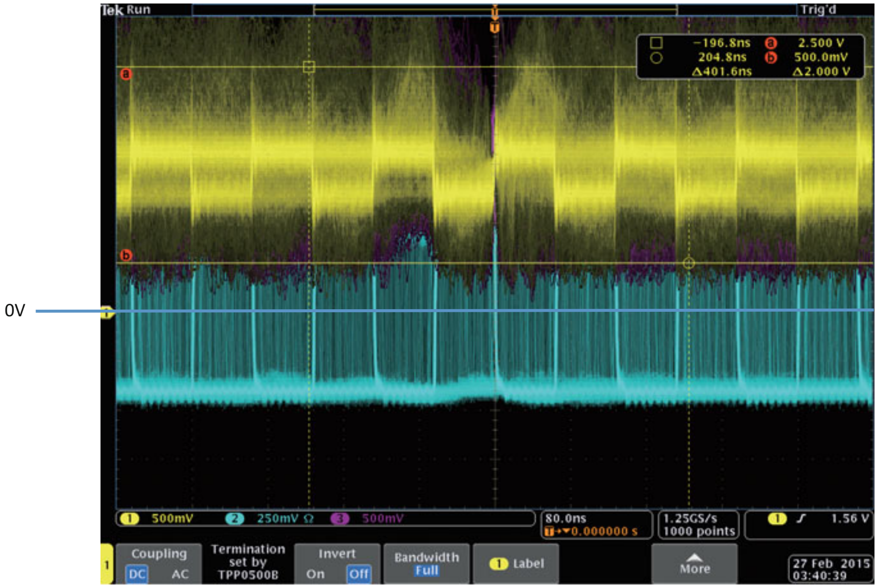


Fig. 4.33 Communication success with ferrite core

the same signal measured by the differential probe, which seems to be stable. In Fig. 4.32, the signal voltage sometimes becomes negative (under 0 V) by noise, and hence the communication becomes failure despite the differential communication line. In contrast, in Fig. 4.33, the signal voltage is always positive (over 0 V), and hence the communication is successful, thanks to the ferrite core.

References

1. K. Yoshikawa, Y. Sasaki, K. Ichikawa, Y. Saito, M. Nagata, Measurements and co-simulation of on-chip and on-board ac power noise in digital integrated circuits, in *Proceedings of 8th International Workshop on the Electromagnetic Compatibility of Integrated Circuits* (*EMC Compo 2011*), pp. 76–81, Nov 2011
2. C. Lochot, J-L. Levant, ICEM: a new standard for EMC of IC definition and examples, in *Proceedings of the 2003 IEEE International Symposium on EMC*, pp. 892–897, Aug 2003
3. H.H. Park, S.-H. Song, S.-T. Han, T.-S. Jang, J.-H. Jung, H.-B. Park, Estimation of power switching current by chip-package-PCB cosimulatoin. IEEE Trans. Electromagn. Compat. **52**(2), 311–319 (2010)
4. T. Steinecke, M. Gokcen, J. Kruppa, P. Ng, N. Vialle, Layout-based chip emission models using RedHawk, in *Proceedings of the IEEE EMC Compo* (2009)
5. T. Matsuno, D. Kosaka, M. Nagata, Modeling of power noise generation in standard-cell based CMOS digital circuits. IEICE Trans. Fundam. **E93-**A(2), 440–447 (2010)
6. K. Yoshikawa, Y. Sasaki, K. Ichikawa, Y. Saito, M. Nagata, Co-simulation of on-chip and on-board AC power noise of CMOS digital circuits. IEICE Trans. Fundam. **E95-A**(12), 2284–2291 (2012)
7. IEC 61967-1: *Integrated Circuits—Measurement of Electromagnetic Emissions*, *150 kHz to 1 GHz—Part 1*: *General Conditions and Definitions*
8. IEC 61967-6: *Integrated Circuits—Measurement of Electromagnetic Emissions, 150 kHz to 1 GHz—Part 6*: *Measurement of Conducted Emissions—Magnetic Probe Method*
9. T. Hashida, M. Nagata, An On-chip waveform capture and application to diagnosis of power delivery in SoC integration. IEEE J. Solid-State Circ. **46**(4), 789–796 (2011)
10. L.D. Smith, R.E. Anderson, T. Roy, Chip-package resonance in core power supply structures for a high power microprocessor in *Proceedings of the Pacific Rim ASME International Electronic Packaging Technical Conference and Exhibition* (IPACK) (2001)
11. N. Azuma, T. Makita, S. Ueyama, M. Nagata, S. Takahashi, M. Murakami, K. Hori, S. Tanaka, M. Yamaguchi, In-system diagnosis of RF ICs for, in *Proceedings of the 2013 IEEE International Test Conference* (ITC) (2013)
12. IEC 62132-4: *Integrated Circuits—Measurement of Electromagnetic Immunity, 150 kHz to 1 GHz—Part 4*: *Direct RF Power Injection Method*
13. K. Ichikawa, Y. Takahashi, Y. Sakurai, T. Tsuda, I. Iwase, M. Nagata, Measurement-based analysis of electromagnetic immunity in LSI circuit operation. IEICE Trans. Electron. **E91-C** (6), 936−944 (2008)
14. M.P. Robinson, K. Fischer, I.D. Flintoft, A Simple model of EMI-induced timing jitter in digital circuits, its statistical distribution and its effect on circuit performance. IEEE Trans. Electromagn. Compat. **45**(3), 513–519 (2003)
15. S.B. Dhia, A. Boyer, B. Vrignon, M. Deobarro, T.V. Dinh, On-chip noise sensor for integrated circuit susceptibility investigations. IEEE Trans. Instrum. Meas. **61**(3), 696–707 (2012)
16. T. Sawada, T. Toshikawa, K. Yoshikawa, H. Takata, K. Nii, M. Nagata, Immunity evaluation of SRAM core using DPI with on-chip diagnosis structures, in *Proceedings of the 8th*

International Workshop on the Electromagnetic Compatibility of Integrated Circuits (*EMC Compo 2011*), pp. 65–70, Nov 2011

17. T. Sawada, H. Takata, K. Nii, M. Nagata, False operation of static random access memory cells under alternating current power supply voltage variation. Japan. J. Appl. Phys. **52** (04CE14), pp. 1–5, Apr 2013
18. T. Sawada, K. Yoshikawa, H. Takata, K. Nii, M. Nagata, An extended direct power injection method for in-place susceptibility characterization of VLSI circuits against electromagnetic interference. IEEE Trans. Very Large Scale Integr. VLSI Syst. **23**(10), 2347–2351 (2015)
19. T. Hayashi, N. Miura, K. Yoshikawa, M Nagata, A passive supply-resonance suppression filter utilizing inductance-enhanced coupled bonding-wire coils, in *Proceedings of the IEEE 2014 International Symposium on VLSI Design*, *Automation and Test* (*VLSI-DAT*), pp. 121–124, Apr 2014
20. J. Xu, P. Hazucha, M. Huang, P. Aseron, F. Paillet, G. Schrom, J. Tschanz, C. Zhao, V. De, T. Karnik, G. Taylor, On-die supply-resonance suppression using band-limited active damping, *in* Digest of Technical Papers, IEEE International Solid-State Circuits Conference (ISSCC), pp. 286–287, Feb 2007
21. S. Pant, D. Blaauw, A charge-injection-based active-decoupling technique for inductive-supply-noise suppression, *in* Digest of Technical Papers, IEEE International Solid-State Circuits Conference (ISSCC), pp. 416–417, Feb 2008
22. Cicalini et al., A 65 nm CMOS SoC with embedded HSDPA/EDGE transceiver, digital baseband and multimedia processor, *in* Digest of Technical Papers, IEEE International Solid-State Circuits Conference (ISSCC), pp. 368–369, Feb 2011
23. N. Yamasaki, Responsive Link for distributed real-time processing, In *Proceedings of the 10th International Workshop on Innovative Architecture for Future Generation High-Performance Processors and Systems*, pp. 20–29 (2007)
24. IEEE: IEEE 802.3 Ethernet Working Group, http://grouper.ieee.org/groups/802/3/
25. Association, T.: IEEE 1394, http://1394ta.org/
26. Universal Serial Bus, http://www.usb.org/home
27. ISO/IEC: ISO/IEC 24740:2008 Information Technology—Responsive Link, http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50352
28. N. Yamasaki, Responsive multithreaded processor for distributed real-time systems. J. Robot. Mechatron. **17**(2), 130–141 (2005)
29. K. Suito, R. Ueda, K. Fujii, T. Kogo, H. Matsutani, N. Yamasaki, Dependable responsive multithreaded processor for distributed real-time systems. IEEE Micro **32**(6), 52–61 (2012)
30. IPSJ: IPSJ-TS 0015:2015 Dependable Line Code with Error Correction Capability: 4b/10b, https://www.itscj.ipsj.or.jp/ipsj-ts/ts0015/main.htm

Chapter 5
Variations in Device Characteristics

Hidetoshi Onodera, Yukiya Miura, Yasuo Sato, Seiji Kajihara, Toshinori Sato, Ken Yano, Yuji Kunitake and Koji Nii

Abstract Ever increasing variability in device characteristics is a major threat to the dependability, since it could give rise to faults and failures in VLSI circuits and systems. The variability arises from the variation in device parameters, such as geometry and doping densities, that is inherently associated with the technology scaling. This chapter deals with the variability of scaled devices and countermeasures to enhance dependability both at the device and circuit levels. First, in Sect. 5.1, variations in transistor characteristics are overviewed with measured variability from 0.35 μm down to 40 nm technologies. The rapid increase in within-die random variations is clearly shown. Possible scaling scenarios, which are device-level strategies to reduce variability, are explained. In the following sections, we discuss countermeasure techniques at the circuit level. In Sect. 5.2, on-chip monitor circuits for variability measurement and performance compensation by localized body biasing are proposed and verified by silicon measurements. In Sects. 5.3 and 5.4, two techniques for predicting and preventing timing faults during runtime are introduced. The first technique in Sect. 5.3 relies on accurate delay-time measurement by an on-chip monitor circuit. Timing margins reduced by

H. Onodera (✉)
Kyoto University, Kyoto, Japan
e-mail: onodera@vlsi.kuee.kyoto-u.ac.jp

Y. Miura
Tokyo Metropolitan University, Hino, Japan

Y. Sato · S. Kajihara
Kyushu Institute of Technology, Iizuka, Japan

T. Sato
Fukuoka University, Fukuoka, Japan

K. Yano
Tokyo Institute of Technology, Tokyo, Japan

Y. Kunitake
Panasonic Corporation, Kadoma, Japan

K. Nii
Renesas Electronics Corporation, Tokyo, Japan

S. Asai (ed.), *VLSI Design and Test for Systems Dependability*,
https://doi.org/10.1007/978-4-431-56594-9_5

aging effects such as negative-bias-temperature instability (NBTI) can be evaluated and compensated. The second technique in Sect. 5.4 proposes a warning flip-flop that can predict possible timing errors before they actually happen, thus enables dependable operation throughout the whole life cycle of the circuit. Finally in Sect. 5.5, variability-aware circuit architectures are discussed for Static Random Access Memories (SRAMs). The proposed SRAM achieves expanded operating margins by fine-grain assist bias control at low supply voltages.

Keywords Device variation • Process variation • On-chip monitor
Variation-aware design • Timing error prediction and compensation

5.1 Overview of Device Variations

Hidetoshi Onodera, Kyoto University

5.1.1 Device Variation and Overview of This Chapter

With the device dimensions in the nanometer regime, variability in device performance becomes a crucial problem in LSI design. The variability comes from the physical-level fluctuations in device structures, and appears as the fluctuations in device characteristics such as drain currents and threshold voltages, and leads to the variations in circuit-level performances such as delay and power dissipation. These “faults” may cause “errors” which eventually result in malfunctions (“failures”) of LSI circuits and systems.

The variability, however, is not a new problem and it has been always an issue in circuit design. In the past, the variability mainly came from imperfect control of fabrication processes. Device performance varied from a lot to lot and from a wafer to wafer, while the variation within a die was relatively small. We can say that the variability had a “global” nature and a local fluctuation within a die could be neglected in many cases except for certain analog designs. Although the amount of global variation could be large, the global nature allows us to evaluate the effect of variation by the worst-case analysis where all the devices are assumed to have the performance of the same extreme corner. In this way, the global variability has been managed mainly considering the performance at all the worst-case corners of device performances. On the other hand, the variability in the present and the future have different statistical characteristics. As device dimensions have been approaching atomic scales, intrinsic atomistic variations such as line edge roughness and discrete random dopant fluctuations become prominent [1, 2]. Those atomistic variations are random in nature and result in a random within-die variation of device performances. The random variation cannot be handled by the worst-case analysis since the possibility of all the devices being at the same worst corner becomes extremely small. The worst-case design becomes unrealistically pessimistic and results in the reduced advantage of scaling. It is, therefore, important to establish a new design methodology that considers the statistical nature of the variation.

This section, focusing on MOS transistors in scaled technologies, gives an overview of device variations and possible solutions at the device level. In Sect. 5.1.2, we classify the variations from a standpoint of spatial distributions. In Sect. 5.1.3, we explain the sources of variations. In Sect. 5.1.4, we show examples of measured variations from 0.35 μm to 40 nm technologies which indicate the statistical nature of the variation is changing from the global to local, in other words, from die-to-die to within-die. In Sect. 5.1.5, we discuss the variability trend and possible scaling scenarios for the future, which provides a countermeasure against variability at the device level. Section 5.1.6 summarizes this section.

Following sections cover a variety of circuit-level proposals that cope with device variations. Section 5.2 explains a method for monitoring variations and a countermeasure for compensating the variations. Section 5.3 proposes an on-chip monitor circuit for accurate delay-time measurement and Sect. 5.4 introduces a warning flip-flop that can predict timing errors due to delay variation in a critical path. Section 5.4 introduces a circuit design technique and a clocking scheme that can overcome timing faults due to variations. The last section of this chapter, Sect. 5.5, proposes design techniques that enhance the operating margins of Static Random Access Memory (SRAM) under device variations.

5.1.2 Classification of Variation

Components of performance variations can be classified into “global” one and “local” one from a standpoint of spatial distributions. The global component gives a uniform variation in the same direction to all the transistors on a die, and is called a D2D (Die-to-Die) variation. Lot-to-lot and wafer-to-wafer variations correspond to D2D variations. The local component arises in each individual transistor and is called a WID (Within-die) variation. From a standpoint of statistical nature, WID variations can be further classified into those that gradually fluctuate over a chip and those that randomly fluctuate [2].

5.1.3 Sources of Variation

The width of the gate, the oxide thickness, and the dopant density of a transistor have direct effects on the transistor performance. Fluctuations in the dimension of device structures mainly appear as D2D variations. It is important that those fluctuations should be maintained within the worst corners so that enough yields are achieved. In a scaled technology, besides those historical sources of variations, atomistic-level variations in an individual transistor such as discrete random dopant fluctuations (RDF: Random Dopant Fluctuation) and fluctuations in a sidewall of gate material (LER: Line Edge Roughness) have a strong impact on performance variations. Due to the statistical nature of those sources, they appear as random components in WID variations. Stress variations in strained Si and STI (Shallow Trench Isolation) processes, dopant density fluctuations near well boundaries due to dopant scattering during well-forming processes, and local temperature variations during rapid thermal annealing come into play as the sources of variation. Those sources contribute to location-specific components in WID variations. Aggressive scaling and increasing technology complexity lead to an explosion in the magnitude of variability while also introducing new sources of variations.

5.1.4 Observation of Variation

We examine variability trend from measured characteristics of five different fabrication technologies: 0.35 μm, 180 nm, 90 nm, 65 nm, and 40 nm. We can see a growing trend of WID variability as the scaling advances.

5.1.4.1 Evaluation of Variation

As an example of variations in the past technology, we show variations of transistor characteristics in a 0.35 μm process. The drain saturation current ($I_{\mathrm{d\_sat}}$) and the threshold voltage (V_{th}) of 16 PCM (Process Control Module) transistors distributed over a wafer have been measured for 58 lots with 797 wafers. Figure 5.1 shows the distribution of drain current characteristics reconstructed from the measured $I_{\mathrm{d\_sat}}$ and V_{th}. If we superimpose characteristics for all lots, the 3σ width of $I_{\mathrm{d\_sat}}$ variations becomes about 15% of the mean $I_{\mathrm{d\_sat}}$ value. If we build up for a single lot only, the average of the 3σ width is reduced to about 6%. If we consider 16

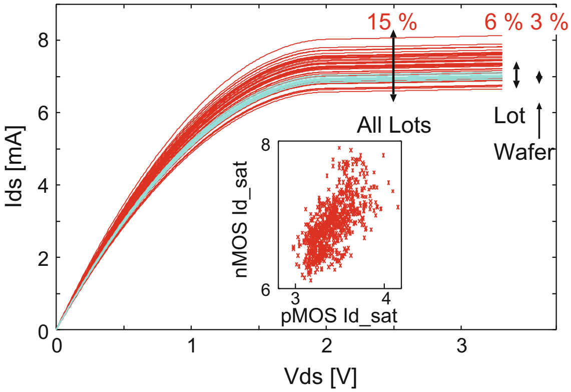


Fig. 5.1 Drain current variations in a 0.35 μm process

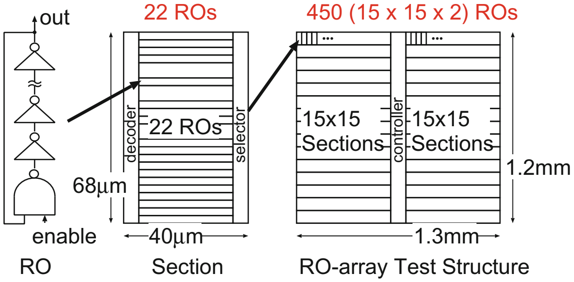


Fig. 5.2 RO (Ring Oscillator)-array test structure for variability characterization

transistors over a single wafer, the average of the 3σ width becomes 3%. We do not have data for estimating within-die variation. However, it is expected that the D2D component dominates over the WID component. A scatter plot inside Fig. 5.1 shows a distribution of nMOS $I_{\text{d\_sat}}$ and pMOS $I_{\text{d\_sat}}$. In this process generation, we can safely rely on a corner-based design method.

We next show variations of oscillation frequencies that are measured from an array of ROs (Ring Oscillators) fabricated in four technology generations of 180, 90, 65, and 40 nm. An example of the RO array circuit for variability characterization is shown in Fig. 5.2. This circuit is fabricated in a 90 nm technology. A variety of ROs is assembled in a block called "Section." The circuit in Fig. 5.2 includes 22 types of ROs in a Section. The Section is then arranged in two sets of a 15-by-15 array, resulting in 450 ROs for each circuit configuration. The size of the test structure is 1.2 mm by 1.3 mm. If there is no variation in device characteristics, all the ROs with the same circuit configuration should have the same oscillation frequency. However, due to D2D and WID variations, the oscillation frequency of each RO varies. With this test structure, we can estimate the variability of D2D and WID components in a form of the oscillation frequency. Figure 5.3 shows the chip layout and the size of the test structure for each technology generation. Several ROs with identical circuit structures are included in all the test structures, which enables observation of variability trend over four technology generations.

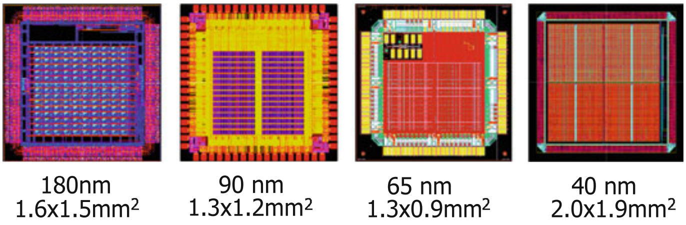


Fig. 5.3 RO (Ring Oscillator)-array test structure in four technology generations

5.1.4.2 Die-to-Die and Within-Die Variation

Table 5.1 lists the amount of D2D and WID components in oscillation frequency variations for 7-stage, 13-stage, 29-stage, and 59-stage inverter ROs. Standard deviations σ of oscillation frequencies normalized by their mean values μ are listed in percentile. The values of D2D components for each generation are almost the same regardless of the number of stages, although those values differ by technology generations. On the other hand, the value of WID components decreases as the number of stages increases. This happens due to the averaging effect of random variations as the number of stages increases.

Taking the 7-stage inverter RO as an example, we further decompose the WID variations into three components of Location-Specific, Across-Chip, and Random, where the location-specific component is a layout-dependent deterministic variation, the across-chip component is a gradually varying variation over the chip, and the random component is a random and uncorrelated variation over the chip [3]. Table 5.2 shows the amounts of standard deviations (σ/μ) for D2D and WID components and their breakdowns. It is clearly seen that the amount of WID random components rapidly increases as the technology scales. We estimate the amount of random variation for a single inverter from the stage-length dependency of random variations. The estimated value for a single inverter is also listed at the last row in Table 5.2. In the 40 nm process, a random variation with 7.5% standard deviation appears. It becomes clear that, in a scaled technology, we should take care of not only D2D variations but also WID variations in the design process.

Table 5.1 Comparison of WID (average) and D2D variations in σ/μ (%)

RO	180 (nm)		90 (nm)		65 (nm)		40 (nm)	
	D2D	WID	D2D	WID	D2D	WID	D2D	WID
INV7	4.6	1.5	3.2	1.5	0.9	1.7	2.0	2.4
INV13	4.3	1.2	3.2	1.2	0.9	1.4	2.2	1.8
INV19	4.1	1.1	3.2	1.1	1.0	1.3	2.2	1.5
INV29	4.2	1.0	3.2	1.0	1.0	1.1	2.2	1.3
INV59	–	–	–	–	0.9	1.1	2.0	1.0

Table 5.2 Variability breakdowns for 7-stage ROs

Variability component	Standard deviation σ/μ (%)			
	180 (nm)	90 (nm)	65 (nm)	40 (nm)
D2D	4.6	3.2	0.95	2.0
WID	1.5	1.5	1.7	2.4
Location specific	1.3	0.7	1.0	0.6
Across-chip	0.1	0.1	0.2	0.2
Random	0.6	1.4	1.3	2.3
A single gate	1.7	4.3	4.0	7.5

5.1.5 Variability Trend and Scaling Scenario

A major source of WID random variations is a discrete random dopant fluctuation (RDF). Due to the RDF, the threshold voltage $V_{\rm th}$ of a transistor fluctuates randomly. The amount of the fluctuation is proportional to the inverse of the square root of the channel area LW, which is expressed by the following equation.

$$\sigma(V_{\rm th}) = \frac{A_{\rm vt}}{\sqrt{LW}}, \qquad A_{\rm vt} \propto t_{\rm ox} N_{\rm A}^{0.25}, \tag{5.1}$$

where L and W are the length and the width of the channel, respectively, and t_{ox} is the oxide thickness, and $N_{\rm A}$ is the dopant density of the channel. A graph that displays the amount of variation as a function of the -0.5-th power of the channel area is called a Pelgrom plot [4]. The gradient of the Pelgrom plot corresponds to $A_{\rm vt}$ which is proportional to the oxide thickness and the 0.25th power of the dopant density. It is, therefore, the shrink of the oxide thickness and the decrease in the dopant density lead to the reduction of variations.

In looking back the evolution of transistor structures in accordance with the progress in technology generations, up to around 45 nm technology nodes, polysilicon is commonly used for the gate material with SiON for the gate oxide material. After around 32 nm technology nodes, metal gates and oxide materials with high dielectric constant (HK MG: High-K Metal Gate) are introduced, which leads to the decrease in the EOT (Effective gate Oxide Thickness). Further, after around 22 nm technology nodes, fully depleted SOI (Silicon On Insulator) transistors and FinFETs that have zero or lightly doped channels are introduced. Those structural changes both contribute to the suppression of variations. Figure 5.4 shows the variability trend in accordance with the evolution of transistor structures. The amount of variations increases with technology scaling while the progress of transistor structures contributes to the abrupt reduction of variations. However, we also should be aware that the evolution of transistor structures introduces new sources of variation. For example in the case of FinFETs, performance variations due to the nonuniformity of metal-gate granularity become a big concern.

As shown in Sect. 5.1, the amount of random variations is related to device dimensions such as the area of the channel and the oxide thickness. The lower limit

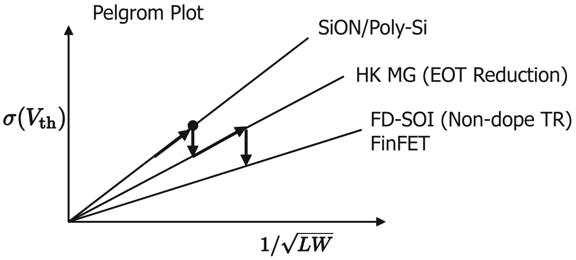
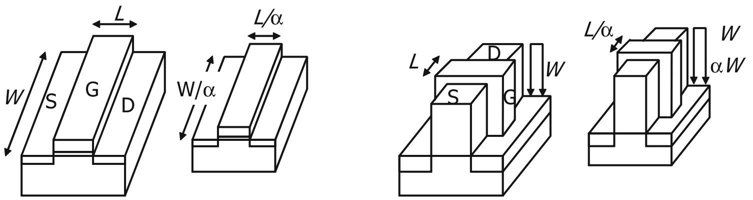


Fig. 5.4 Variability trend and the evolution of transistor structures



	LP	HP
L	$1/\alpha$	$\leftarrow$
W	$1/\alpha$	$\leftarrow$
W/L	1	$\leftarrow$
LW	$1/\alpha^2$	$\leftarrow$
t_{ox}	$1/\sqrt{\alpha}$	$1/\alpha$
$\sigma(V_{\mathrm{th}})$	$\sqrt{\alpha}$	1

Increase

	LP	HP	LP	HP
L	$1/\alpha$	$\leftarrow$	$1/\alpha$	$\leftarrow$
W	α	$\leftarrow$	1	$\leftarrow$
W/L	α^2	$\leftarrow$	α	$\leftarrow$
LW	1	$\leftarrow$	$1/\alpha$	$\leftarrow$
t_{ox}	$1/\sqrt{\alpha}$	$1/\alpha$	$1/\sqrt{\alpha}$	$1/\alpha$
$\sigma(V_{\mathrm{th}})$	$1/\sqrt{\alpha}$	$1/\alpha$	1	$1/\sqrt{\alpha}$

Decrease

Fig. 5.5 Scaling scenarios for planar transistors and FinFETs

of the minimum supply voltage V_{ddmin}, which is defined as the minimum voltage that ensures a correct operation, is limited by the amount of variations in transistor characteristics [5]. Lowering the supply voltage for the reduction of power dissipation is essential for enabling a higher level of integration with technology scaling. It is therefore important to establish technology scaling that is compatible with variability reduction.

Figure 5.5 explains the scaling scenarios for planar transistors and FinFETs proposed by Itoh [5]. The left side of Fig. 5.5 shows the scaling scenarios of planar transistors for low-power (LP) applications and high-performance (HP) applications. It is shown that planar transistors cannot be scaled with reduced variations. On the other hand, scaling scenarios of FinFETs, in which the channel width (Fin height) is inversely scaled, are indicated in the second column in the right table of Fig. 5.5. Due to the inverse scaling of the channel width (Fin height), both of low-power (LP) FinFETs and high-performance (HP) FinFETs enable scaling with reduced variations [5]. The third column of the right table in Fig. 5.5 shows other possible scaling scenarios with a constant channel width (Fin height). The suppression of variability increase is achieved by the non-scaling of the channel width.

5.1.6 Section Summary

In this section, performance variability of MOS transistors due to technology scaling is overviewed. After explaining the classification and the sources of variations, observations of measured variations from 0.35 μm to 40 nm technologies are presented. In particular, it is shown that the amount of WID random variations increases rapidly with technology scaling. WID variations cannot be handled by a conventional worst-case design (corner-based design). It is important to develop countermeasure techniques that can consider the specific nature of each variation component.

5.2 Monitoring and Compensation for Variations in Device Characteristics

Hidetoshi Onodera, Kyoto University

5.2.1 On-chip Variability Monitoring and Compensation

Increased variability is an inherent issue associated with device scaling. The variability in device characteristics leads to the variability in circuit performance (“faults”), which may cause “errors” eventually resulting in malfunctions (“failures”). For ensuring higher yields, it is common to adopt the worst-case design method that assumes the device performance being located at the worst corner so that the circuit performance always meets specifications in the whole performance spread. On the other hand, a circuit that is designed under the worst corner inherently has an overhead in all aspects of speed, power, and area, except for the case that all the device variations are really located at their worst corners. Performance spread has been expanding especially for lower voltage operation. Based on a simulation assuming a model circuit in a 65 nm process, under the nominal supply voltage of 1.2 V, the spread in operating speed between the fast corner and the slow corner is 67%. When the supply voltage is decreased to 0.6 V, the performance spread becomes 200%. This means that huge overheads in power dissipation and area have to be compromised in order to guarantee the speed performance at the slow corner. The expanded performance spread associated with lower supply voltage becomes prominent even in WID (Within-Die) variations, as well as D2D (Die-to-Die) variations. According to a performance measurement of a NoC (Network-on-Chip) with regularly tiled 80 cores, it is reported that the variation of the maximum operating frequency $F_{\max}$ of each core is 28% under the nominal supply voltage of 1.2 V. It, however, expands to 62% for 0.8 V operation [6]. Besides D2D variations, WID location-specific variations should be considered for the target of variability modeling and compensation.

For coping with the performance variations, promising approaches include circuit-level techniques that mitigate the variations at the device level. An example is a method that monitors the delay of a critical-path replica [7]. Variations of device performances are evaluated by the delay time of the monitored path and the operating speed is controlled to the target value by adjusting the supply voltage and/or body (substrate) bias voltage. This method evaluates the variation by mapping both of nMOSFET variations and pMOSFET variations into a delay variation. It is, therefore, difficult to obtain the variation of each transistor independently. Even in a case where an nMOS transistor and a pMOS transistor vary in opposite directions, the same compensation has to be applied to both transistors. It, therefore, may happen that a leak current unnecessarily increases after compensation.

In order to overcome the variability issue, we have developed a method that monitors performance variations of an nMOSFET and a pMOSFET independently and compensates each performance by adjusting each body bias voltage. Applying this technique to a small region-by-region on a chip, we can compensate not only D2D variations but also WID variations.

This section is organized as follows. In Sect. 5.2.2, we explain the variability monitoring and compensation technique by localized body biasing. The developed circuit consists of a body bias generator and digital monitors that evaluate performance variations of an nMOSFET and a pMOSFET independently. A noticeable feature of the circuit is that it can be implemented in a cell-base design. The effectiveness of the proposed technique has been verified by a test chip fabricated in a 65 nm process. Details will be given in Sect. 5.2.3.

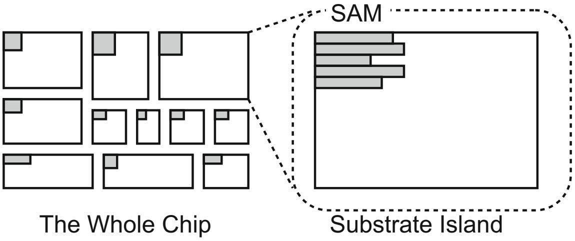
5.2.2 *Variability Monitoring and Compensation by Localized Body Biasing*

We have developed a variability compensation scheme that divides a chip into small regions and the variability of each region is compensated region-by-region [8]. After explaining the compensation scheme, variability monitoring circuits and a body bias generator are presented [8, 9].

5.2.2.1 Localized Body Biasing

In order to compensate D2D variations and WID variations as well, we divide the whole chip into small regions called “substrate islands” and variability monitoring and compensation of each region are performed by a self-monitoring and self-compensation circuit called SAM (Self-Adjustment Module). Figure 5.6 shows

Fig. 5.6 Self-monitoring and self-compensation of transistor performance by localized body biasing



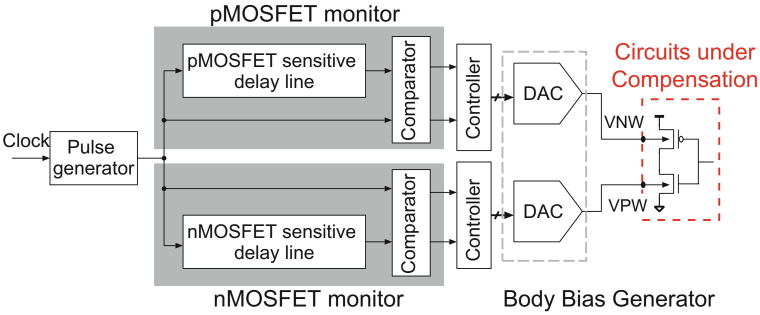


Fig. 5.7 Self-monitoring and self-compensation circuit

the compensation scheme by chip partitioning. Figure 5.7 illustrates the circuit configuration of the self-monitoring and self-compensation circuit SAM. It monitors performance variations of an nMOSFET and a pMOSFET independently by all-digital monitors. Based on the monitored results, a body bias generator supplies n-well and p-well bias voltages so that the performance of each type of transistors meets the target. The self-monitoring and self-compensation circuit (SAM) can be implemented in a cell-base design. Assuming the area of the substrate island is 0.1 mm^2, the area overhead of SAM is around 3% in our experiment. Due to its cell-base design, SAM can be integrated with a target circuit under compensation. By embedding SAM into white spaces of the target circuit, effective overhead can be further reduced.

5.2.2.2 Variability Monitoring

In order to measure performances of an nMOSFET and a pMOSFET independently, we have developed a monitor circuit sensitive only to an nMOSFET and a circuit sensitive only to a pMOSFET. Figure 5.8 shows the schematics of those circuits. Both circuits consist of path-transistor-inserted inverters followed by conventional

Fig. 5.8 Performance monitor circuits for pMOSFETs and nMOSFET

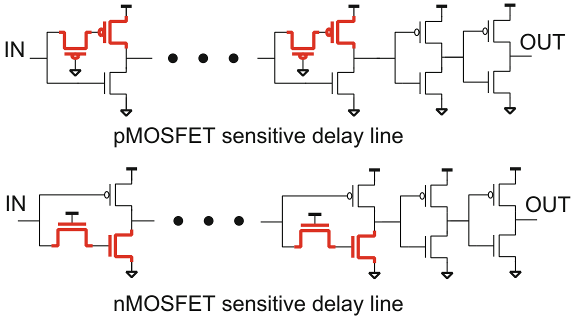
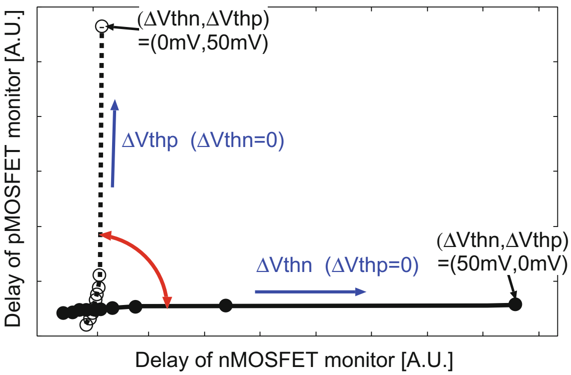


Fig. 5.9 Delay times of a pMOSFET monitor and a nMOSFET monitor when the threshold voltage of nMOSFET or pMOSFET is shifted



inverters. The path-transistor-inserted inverter in the upper circuit of Fig. 5.8 has a pMOS path-transistor inserted between the input of the inverter and the gate of the pMOS pull-up transistor, and it is sensitive only to the performance of pMOSFETs. The path-transistor-inserted inverter in the lower circuit of Fig. 5.8 has an nMOS path-transistor inserted between the input of the inverter and the gate of the nMOS pull-down transistor, and it is sensitive only to the performance of nMOSFETs.

The delay times of each monitor circuit are simulated and plotted in Fig. 5.9 by changing the threshold voltage of each type of transistor. The delay time of the nMOSFET monitor is sensitive to the threshold voltage change of nMOSFETs while it is not sensitive to that of pMOSFETs. The delay time of the pMOSFET monitor is sensitive only to the threshold voltage change of pMOSFETs. It is, therefore, possible to evaluate the performance variations of an nMOSFET and a pMOSFET independently from the measured delay time of each monitor circuit.

5.2.2.3 Variability Compensation by Adaptive Body Biasing

Based on the measured results of performance variations, the variations can be compensated by applying proper body (substrate) bias to each well. In this study, we have developed a body bias generator that supplies forward bias voltages so that performance compensation in the speeding-up direction can be possible. The circuit does not need an external voltage such that it generates body bias voltages only from a core voltage and a clock signal. Figure 5.10 shows the circuit topology. It consists of charge redistribution serial DACs (Digital-to-Analog Converters) of 6-bit accuracy and voltage followers by operational amplifiers. The circuit topology of the operational amplifier is shown in Fig. 5.11. For reducing power dissipation, a class-B output stage is applied. For enabling operation at the supply voltage of 0.6 V, the common mode level of input voltages is fixed to the half of the supply voltage.

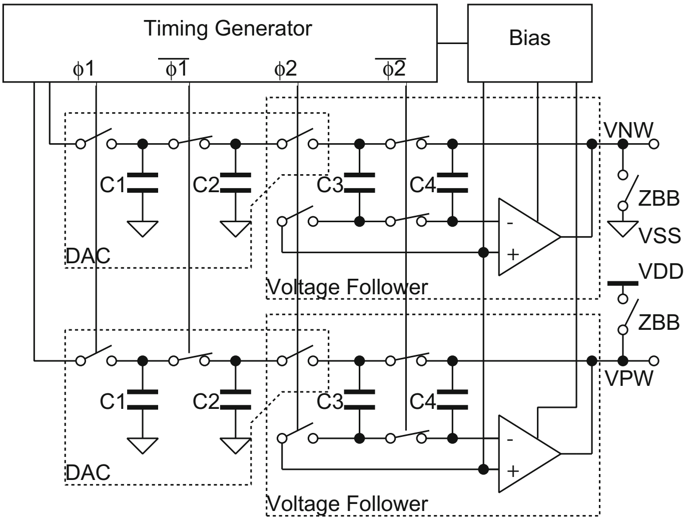


Fig. 5.10 Body bias generator circuit

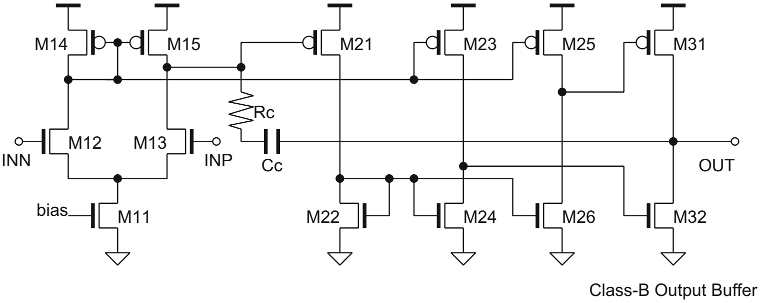


Fig. 5.11 Low-voltage and low-power operational amplifier with class-B output stage

When we apply a body bias voltage of up to 0.5 V, we can control the threshold voltage up to 100 mV assuming a 1/5 magnitude of drain current controllability compared to the gate. This amount is enough for compensating the device performance at the slow corner to the typical case, as shown in the next subsection.

5.2.3 Experimental Verification

The effectiveness of the proposed self-compensation scheme has been verified by a test circuit fabricated in a 65 nm process. Figure 5.12 shows a chip photograph of the test circuit together with a layout plot of the self-compensation circuit SAM.

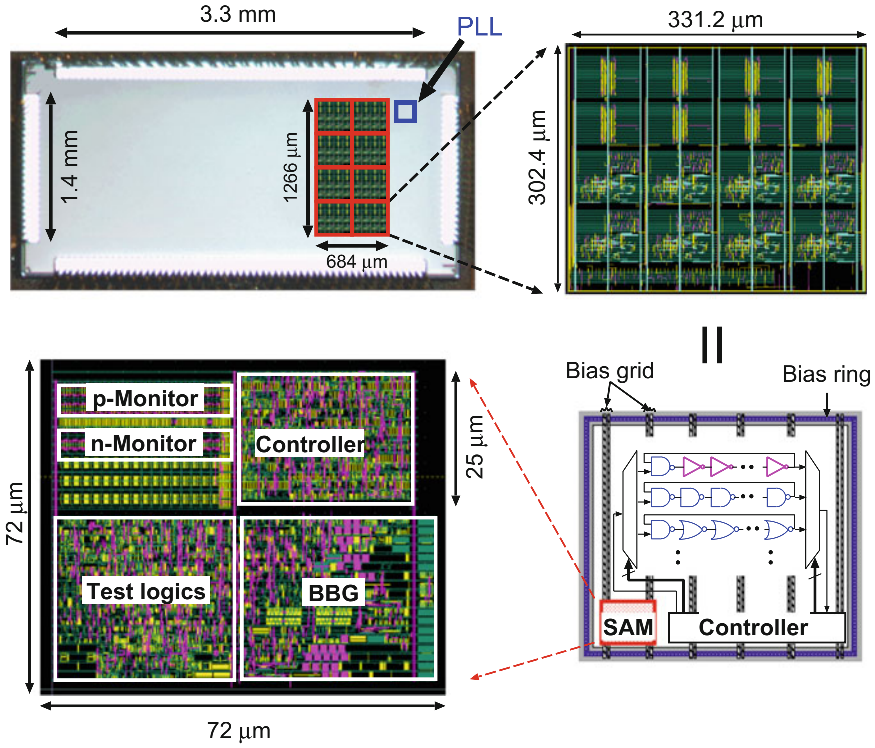


Fig. 5.12 Chip photograph and layout plot of a self-monitoring and self-compensation circuit

A substrate island of 0.1 mm^2 area (around 330 µm by 300 µm) is assumed. Eight substrate islands are integrated on the test chip. The self-monitoring and self-compensation circuit (SAM) is assembled in a 72 µm-by-72 µm space together with other logic gates. The total cell area of the self-monitoring and self-compensation circuit (SAM) is 2628 µm^2 which corresponds to the area overhead of 2.6%. Figure 5.13 shows the layout plot of the body bias generator. Colored cells are those that compose the body bias generator. They are integrated with other logic gates.

The test circuit has been fabricated under the typical condition ("TT"), and also under the four different process corners. Those corners correspond to four combinations of the fast corner (F) and the slow corner (S) for each type of transistor, and called "SS", "FF", "FS", "SF," respectively.

Operating speed of the test chip has been measured at the supply voltage of 0.7 V. It has been found that, except for the "FF" case, circuits in four other conditions do not meet the target speed without self-compensation. After enabling the self-measuring and self-compensation circuit (SAM), operating speed has been recovered in all the four conditions. Figure 5.14 shows the operating speeds of the nMOSFET monitor and the pMOSFET monitor before and after the self-compensation for "SS", "TT", "SF", and "FS" chips. Generated body bias voltages are also indicated in the figure. In

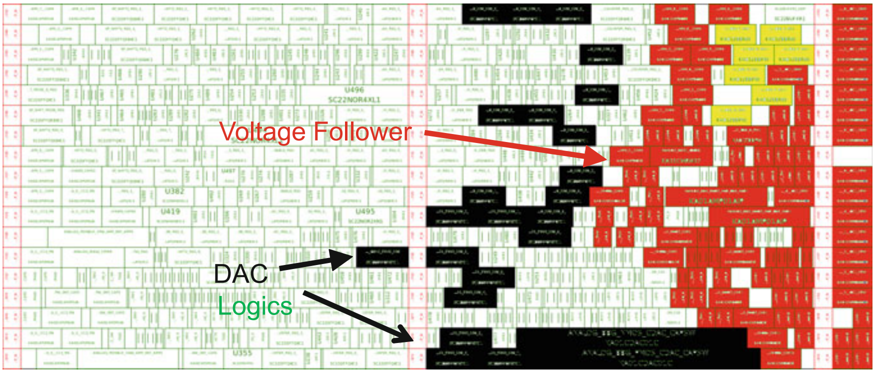
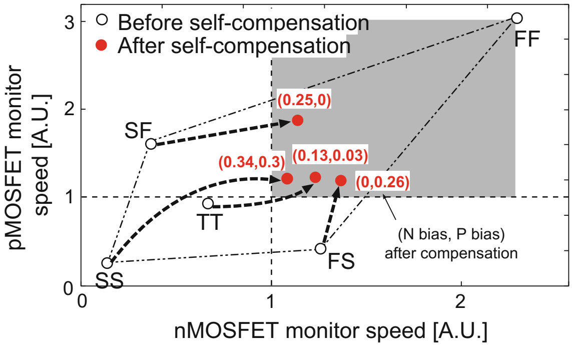


Fig. 5.13 Layout plot of a body bias generator (colored cells) integrated with other logic gates

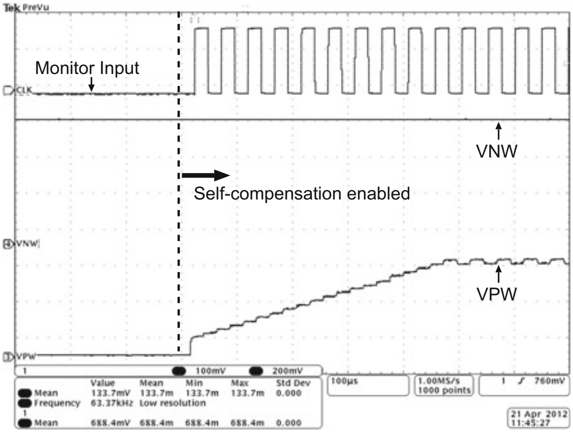
Fig. 5.14 Operating speeds of nMOSFET monitors and pMOSFET monitors before and after self-compensation for "SS", "TT", "SF", and "FS" chips



the cases of "FS" and "SF" chips, forward body bias is applied only to the body of the slow transistor. Figure 5.15 shows a transient response of the self-measuring and self-compensation circuit of an "SF" chip. Only the p-well voltage (VPW) for the slow nMOSFET ramps up until the target speed is recovered.

5.2.4 Section Summary

We have developed a variability monitoring and compensation scheme in which performance variations are self-monitored and self-compensated by body bias control so that the target speed is achieved. The whole chip is divided into a collection of small regions called "substrate islands," and each substrate island accommodates a self-monitoring and self-compensation circuit, thereby WID variations as well as D2D variations can be compensated. For performance monitoring, all-digital monitor circuits have been developed that can detect performance shifts of an nMOSFET and a pMOSFET independently. A body-bias generator that



```
1                          100mV        200mV
            Value      Mean     Min      Max      Std Dev   100µs   1.00MS/s      1  ƒ  760mV
  Mean      133.7mV    133.7m   133.7m   133.7m   0.000             1000 points
  Frequency 63.37kHz   Low resolution
1                                                                               21 Apr 2012
  Mean      688.4mV    688.4m   688.4m   688.4m   0.000                         11:45:27
```

Fig. 5.15 Transient response of a self-measuring and self-compensation circuit of an "SF" chip

is compatible with cell-base design has been proposed. The proposed scheme has been verified and demonstrated by test circuits fabricated in a 65 nm process under five process corners of "TT", "SS", "FF", "SF", and "FS", where all the corner chips that do not meet the speed target have been successfully compensated to meet the speed goal.

5.3 Highly Accurate On-chip Measurement of Circuit Delay Time for Dependable VLSI Systems

Yukiya Miura, Tokyo Metropolitan University
Yasuo Sato, Kyushu Institute of Technology
Seiji Kajihara, Kyushu Institute of Technology

5.3.1 Purpose of Delay-Time Measurement

As semiconductors continue to be scaled down, process variation and circuit aging (degradation) affect the operation speed of the LSI [10, 11]. Variation and aging cause the change in the circuit delay time and result in a serious threat to LSI dependability. To enable a dependable design and preventive maintenance of a system, this section focuses on a method for measuring the delay time of the LSI accurately using an on-chip measurement circuit. To evaluate effects of variation and aging and to ensure correct operation of the system, the delay time (operation speed) of the LSI must be measured when the system is running. For the purpose, this section describes on-chip delay-time measurement that can measure the delay time of the LSI in the field where the LSI is used. In the on-chip measurement, an easy implementation and a small area overhead for the measurement circuit and a flexible path selection method for the delay-time measurement in the field as well as time resolution of the measurement circuit are needed. As the reasonable solution for satisfying those, a delay-time measurement method utilizing scan design is applied. In addition to variation and aging, the environmental parameters in the field such as temperature or voltage significantly affect the measured delay time. This section also describes a method to compensate for the effect of the environment on the measured delay time. This method can accurately evaluate the delay time due to variation and aging.

5.3.2 Overview of On-chip Delay-Time Measurement

Variation and aging affect the operation speed of the LSI. The LSI generally has enough margins for required specifications when it is designed, and it is shipped only if it has passed the production tests, including the at-speed test. In addition to the production tests, the burn-in test is applied to highly reliable products to reduce the occurrence of early failure. However, the actual delay time of each product is unknown even if it has passed the tests. Moreover, the effect of circuit aging becomes noticeable as the LSI continues to be used in the field, and the LSI will eventually become faulty (Fig. 5.16). Therefore, the delay time of the LSI in the field needs to be measured continuously to ensure a normal LSI performance and a long-term stable operation of the system.

To measure the delay time of the LSI with high time resolution, an on-chip circuit that measures the delay time of the LSI (e.g., the path delay time) is needed. Table 5.3 compares the main measurement methods using on-chip circuits.

A Vernier delay line (VDL) method measures the delay time using the difference between two buffers with different propagation delay times [12, 13]. A measurement circuit consists of two kinds of buffer chains and flip-flop chains. The time resolution of delay-time measurement by the VDL method is high because it uses the difference in propagation delay times between two buffer chains. However,

Fig. 5.16 Failure rate (bathtub curve)

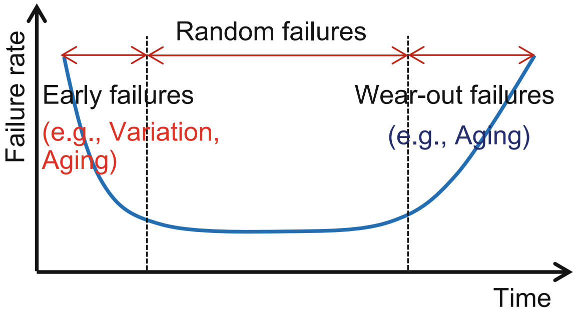


Table 5.3 Comparison of on-chip delay-time measurement methods

	VDL	OSC test	Razor/canary	Scan-based method
Circuit structure	Buffer and FF chains	Ring oscillator	Duplicated FF	Scan circuit
Measurement principal	Difference of delay time between two buffers	Self-oscillation period	Difference of sampling time between two FFs	Variable clock timing
Measurement path	Fix (depending on HW)	Fix (depending on HW)	Fix (depending on HW)	Flexibility (depending on TP)
Circuit overhead	Large (depending on # measuring paths)	Medium (depending on # measuring paths)	Large (depending on # measuring paths)	Small
Time resolution	High	High	Low	Medium

paths for delay-time measurement are fixed to the ones that have been assigned at the LSI design stage, and the amount of area overhead becomes larger as the range for measuring delay time becomes wider.

An oscillation (OSC) test method measures the delay time by using self-oscillation period of a path for delay-time measurement, where a ring oscillator is configured by connecting the input and output lines of the measuring path [14, 15]. From the configuration, time resolution of delay-time measurement is high and the measurement circuit is simple. However, paths for delay-time measurement must be fixed at the LSI design stage.

The Razor FF or the Canary FF uses a duplicated FF whose data sampling timings are slightly different [16, 17]. When values of two FFs are different, their methods result in detection of timing error. The delay time measured by those methods depends on the difference in sampling timings between two FFs. Moreover, the FF at the output of the path for delay-time measurement needs to be duplicated.

The above delay-time measurement methods are ad hoc techniques. On the other hand, for a structured technique, a scan-based delay-time measurement method has been proposed [18, 19]. This method measures the path delay-time of the circuit by scan design. In this method, by using variable clock timing, delay fault testing is applied to a path for delay-time measurement shortening a test clock period step by step. The method can prevent the increment of area overhead because it utilizes the scan architecture built in the chip. Moreover, it can select paths for delay-time measurement flexibly after the LSI is manufactured because the paths to be measured are determined by test patterns (TPs).

5.3.3 Delay-Time Measurement Using Scan Design

In a scan designed circuit, delay testing is applicable for a path (i.e., path under test (PUT)) between a scan-in FF and a scan-out FF (Fig. 5.17, upper). The PUTs are the group of paths that are sensitized by the applied test patterns. If the delay time of the path within the group exceeds a system clock period (i.e., at-speed), the delay fault of the path can be detected.

In a delay-time measurement method using scan design, variable launch clock timing or variable capture clock timing is used. Delay testing is applied to the PUT shortening the test clock period step by step. The clock period before the test is first failed is the actual delay time of the PUT (Fig. 5.17). In this method, since the delay test changing the test timing gradually is carried out repeatedly, the delay-time measurement itself takes time. Moreover, the accuracy of delay-time measurement depends on the resolution of the variable timing of the clock generation.

As a method for changing the period of the clock on the LSI chip, a variable clock generation method is usually used, such as the On-Die Clock Shrink (ODCS) technique [20, 21]. In this method, by inserting a buffer chain that can adjust the number of stages into a test clock line supplied to an FF, the generation timing of the test clock is made variable (Fig. 5.18). If the generation timing of the launch clock for scan-in FFs is delayed when scan testing is applied, the test clock period between the launch and capture clocks can be shortened. Therefore, the PUT can be tested by a clock period shorter than the system clock period (Fig. 5.18, right side). Note that, in this example, generation timing of the capture clock for scan-out FFs is fixed. The generation timing of the launch clock for the PUT (i.e., the path for delay-time measurement) is delayed gradually, and this test is carried out

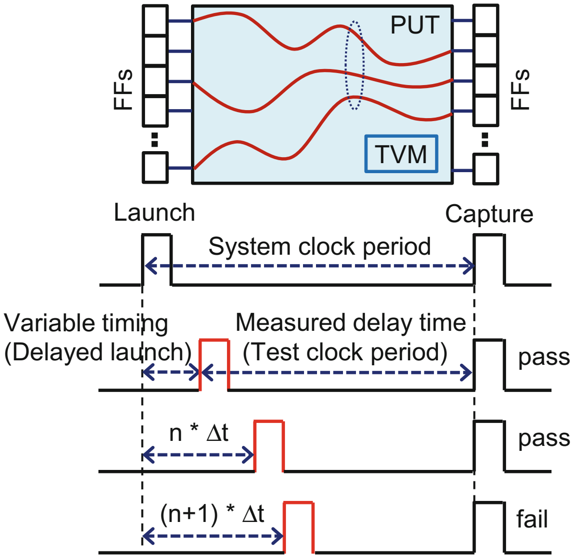


Fig. 5.17 Delay-time measurement by scan test

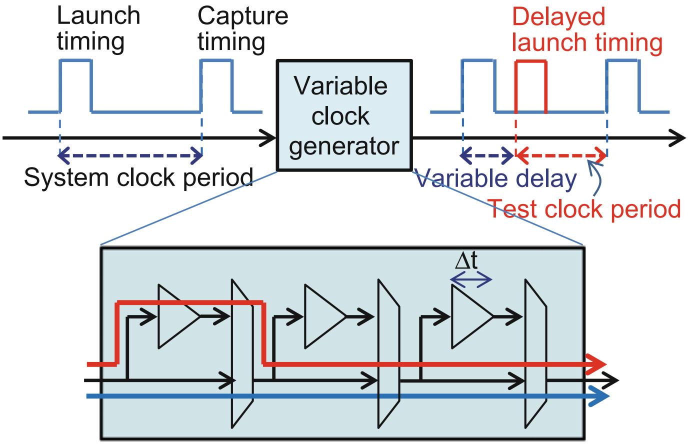


Fig. 5.18 Variable clock timing

repeatedly. When the PUT is identified as faulty (i.e., the test is failed), the timing margin of the path can be calculated as the value of (the system clock period)-(test clock period before first test failure). If the value of the minimum variable delay-time of the launch clock is Δt, as in the example in Fig. 5.17, the timing margin is at least $n * \Delta t$. This method can quantitatively measure the amount of the circuit delay caused by transistor variation and aging as a delay-time margin of a path. Here, note that time resolution for measuring the delay time depends on the change interval of variable clock timing. In addition, since PUTs depend on test patterns, paths for delay-time measurement can be selected after the LSI chip is manufactured. Thus, path selection is more flexible in this method than in other similar methods.

5.3.4 Delay-Time Measurement Considering Measuring Environment

Since delay time of a circuit depends on its operating environment, the measurement environment must be considered when delay time is measured in the field. This section introduces a method for highly accurate delay-time measurement using an aging detection technique in the field called dependable architecture with reliability testing (DART) technology [22]. The DART technology utilizes the function of the scan circuit in the Circuit Under Test (CUT). Delay time of the CUT is measured by using variable test clock timing.

The main purpose of the DART technology is delay-time measurement in the field for preventing delay-related errors (e.g., excessive circuit aging). To realize the field test, the operation environment of the CUT when the delay time is measured, which is

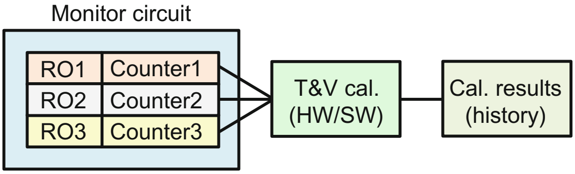


Fig. 5.19 Temperature and voltage monitor

the effect of a temperature and a voltage on the delay time, must be considered. For this purpose, a temperature and voltage monitor (TVM) is built in the CUT. The monitor circuit (sensor part) is a simple and small circuit consisting of three types of ring oscillators (ROs) with different frequency characteristics and counters [23] (Fig. 5.19). The monitor circuit is designed by a CMOS digital standard library. Temperature and voltage are concurrently estimated from RO frequencies (counter values) by fully digital processing, and measuring time is very short (several μs). The monitor circuit can be placed in plural locations and anywhere in a chip because of a small digital circuit. In an environment where temperature and voltage are not controlled, it is possible to compensate for the delay time while considering the measuring environment for the measured delay time by using the built-in TVM. From this technique, the correct timing margin of a circuit is measured. In addition, the technique can hold measured results of temperature and voltage as history data that can be utilized for estimating the busy condition of a chip in the field.

The DART technique has been applied to a circuit consisting of 7.2 M gates and 356 k FFs designed in 90-nm technology [22]. The DART circuit can be implemented with approximately 0.2% area overhead. Under the assumption of the error of the launch clock timing of 20 ps, accuracy of the whole delay-time measurement circuit is estimated as 27 ps by circuit simulation.

5.3.5 Advantages of Delay-Time Measurement by the DART Technology

Since the DART technology measures the delay margin of a circuit in a chip, it can quantitatively evaluate various factors during operation in the field after LSI shipment, such as variation and aging, which affect the circuit delay-time. This technology has the following advantages.

(1) Small area overhead utilizing existing scan circuits
(2) High accuracy of delay-time measurement depending on variable timing of the test clock
(3) Flexible path selection for delay-time measurement depending on test patterns
(4) Measurement of environment factors and compensation of measured delay time by using the temperature and voltage monitor.

The DART technology is considered suitable to be applied to the production test, the field test, the verification tool after manufacture (e.g., the tool for delay margin verification), the failure analysis tool, and analysis of chip use history (temperature and voltage log).

5.4 Timing-Error-Sensitive Flip-Flop for Error Prediction

Toshinori Sato, Fukuoka University
Ken Yano, Tokyo Institute of Technology[1]
Yuji Kunitake, Panasonic Corporation[2]

5.4.1 Timing-Error-Sensitive Flip-Flop

As semiconductor technologies are scaled, a new challenge of parameter variations has emerged. Process variation (P), supply voltage change (V), and temperature fluctuations (T) cause parameter variations (PVT variations) [24, 25]. PVT variations affect each transistor's threshold voltage, resulting in performance variations. Because each of these variations demands its own margin, the total design margins are always overestimated, resulting in wasteful increases in power consumption. In order to eliminate the wasteful power consumption, timing-error-sensitive FFs have been widely studied [16, 17, 26–31]. Because these FFs commonly require additional circuits to detect or to predict timing errors, however, the increase in the chip area, in turn, becomes a big concern. It might significantly enlarge area and power at the chip level. This section shows one possible solution.

First, in this subsection, a novel design philosophy, which is named typical-case design methodology, is introduced. Second, the concept of the timing-error-sensitive FFs, named Canary FF [17, 30], is explained. It is an essential component to make typical-case design practical. After that, an inevitable problem due to Canary FF is considered. Because a Canary FF cell is larger than the conventional D FF cell, it might have a serious impact on area and power in the chip level. And last, the related works are summarized.

Typical-Case Design Methodology

The typical-case design methodology [32] addresses the overestimated design margin due to PVT variations by exploiting the observation that worst cases are rare. LSI designers can focus on typical cases, if there is an insurance mechanism for the worst cases. A single functionality is designed as two circuits. One is a performance-oriented circuit, where the correct functionality in the worst cases is

[1] Part of this work was done while the author was with Fukuoka University, Japan.

[2] Part of this work was done while the author was with Kyushu University, Japan.

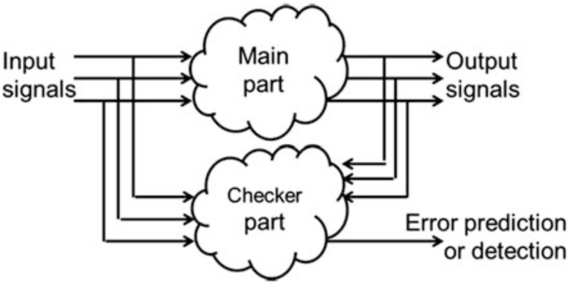


Fig. 5.20 Typical case design

ignored. The other is a function-guaranteed circuit, where optimizing performance in the worst cases is not considered but the logical functions are guaranteed. Since designers should consider only one of the two severe constraints of performance and functionality, their design task becomes simple and easy.

Figure 5.20 explains the concept of the typical-case design. Every critical function (for example, in performance or in power consumption) is designed as two circuits. They are named Main and Checker parts, respectively. Their functionality is equivalent but their roles and implementations are different with each other. The main part realizes the performance-oriented circuit, while the checker part realizes the function-guaranteed one. Hence, some errors might occur in the main part, and in such cases, the checker part supports the main part to guarantee their correct functionality. When an error is detected in the main part, the output of the main part is discarded and replaced with the one of the checker parts and then the state is recovered. In the other case where the error is predicted by the checker part, the possible error is avoided in the main part.

Canary Flip-Flop

In order to reduce the wasteful power, techniques combining Dynamic Voltage Scaling (DVS) with timing-error-sensitive FFs are studied [16, 17]. For example, because one technique decreases the supply voltage as low as possible without causing timing errors by predicting them on the fly, the useless power is eliminated. This section explains the Canary FF [17, 30] as a representative.

Figure 5.21 shows a Canary FF. It includes a redundant FF named shadow FF, a delay element, and a comparator. Due to the delay element, the shadow FF is more

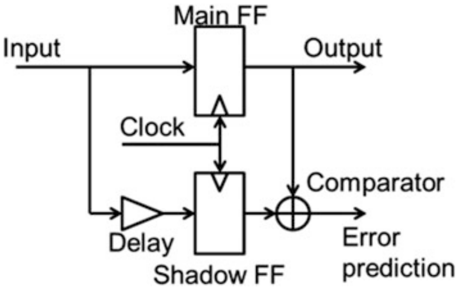


Fig. 5.21 The Canary FF

vulnerable to timing errors than the main FF. If the values kept in the main and the shadow FFs do not match in the comparator, a timing error is predicted. In order to avoid the predicted error, DVS works to increase the supply voltage.

Area Overhead Problem

Because the Canary FF requires the additional circuit elements to detect errors, the area and power overheads in the LSI utilizing the Canary FF might be seriously large. From the preliminary study, it is found that a Canary FF cell is 2.5 times larger than the conventional D FF cell. In order to reduce the area overhead, a special type of scan FFs for production testing can be reused to realize a Canary FF [30]. Because they are already included in some LSIs, there is not any area overhead. However, unfortunately, all LSIs do not utilize special FFs due to cost consideration. In addition, the power overhead is not considered by this technique. Hence, the other solution required is a way to reduce the number of Canary FFs.

Related Works

A lot of timing-error-sensitive FFs are proposed [16, 17, 26–31]. The Razor FF [16] detects timing errors. It also has the shadow FF, where a delayed clock is delivered. In the case when the values kept in the main and the shadow FFs do not match, a timing error is detected. This technique is also applicable to detect soft errors [29]. NEC [28] utilizes the shadow FF to predict aging failures. Instead of delivering delayed clock to the shadow FF, a delay element is inserted between the previous logic stage and the shadow FF as a Canary FF. By detecting timing errors in the shadow FF, the main FF is protected. Agarwal et al. [26] propose a similar technique to predict defects. Intel extends their soft-error resilient FF [27] to support process variation diagnosis [31].

5.4.2 Selective Replacement Method

This subsection explains a technique to reduce the number of Canary FFs, presents its evaluation methodology, and shows evaluation results.

Replacement Strategy

In order to reduce the number of Canary FFs the distribution of path delay is investigated. Depending on the logical depth and wire length, each path has a different delay from the other ones. Timing errors will not occur on paths with small delays, even if PVT variations affect them. It is not necessary to replace any terminal D FFs, which are connected to the end of the short paths, with a Canary FF. Only timing-error-vulnerable FFs on the timing-critical paths should be replaced. This selective replacement method will reduce the chip-level overheads on area and power due to large Canary FF cells.

Figure 5.22 explains how the selective replacement method works [33]. There are three steps. The first step determines the target cycle time. A given RTL is

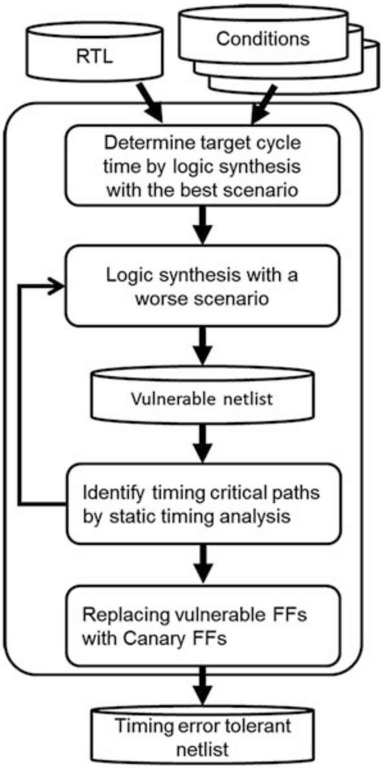

RTL
Conditions
Determine target cycle time by logic synthesis with the best scenario
Logic synthesis with a worse scenario
Vulnerable netlist
Identify timing critical paths by static timing analysis
Replacing vulnerable FFs with Canary FFs
Timing error tolerant netlist

Fig. 5.22 Selective replacement flow

logic-synthesized with the best-case scenario and the reported cycle time is used as the target cycle time. The second step identifies timing-critical paths, which are vulnerable to timing errors. For every worse condition, logic synthesis is performed and its netlist, which is vulnerable to timing errors at the target cycle time, is generated. Static timing analysis is performed on the netlist and the paths, which do not satisfy the target cycle time, are identified as timing-critical paths. This process is continued until all conditions are considered. The last step replaces terminal D FFs connected to the end of the timing-critical paths with Canary FF.

Evaluation Methodology

The selective replacement method is evaluated by two steps. First, a couple of available microprocessor cores are modified by adopting a few different designs. The purpose of the step is to evaluate the impact of Canary FFs on area and power at the chip level. Second, one of the processors is simulated in the instruction set level in order to evaluate how the wasteful power is reduced by DVS.

The first step goes as follows [34]. A tool for the design flow explained in the previous subsection is built [35]. It consists of SYNOPSYS's Design Compiler and an in-house Perl script. Using the tool, netlists of two processor cores, which are Toshiba's MeP [36] and an open-source miniMIPS [37], are generated. The

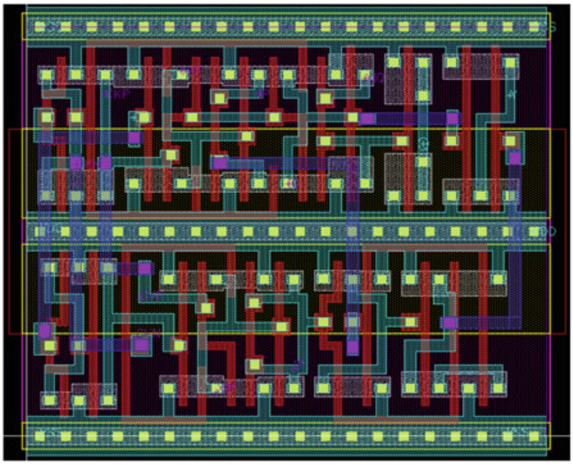


Fig. 5.23 Cell layout of Canary FF [34]

Table 5.4 Comparison between the Canary FF and D FF

	Canary FF	D FF
Area (um$^{2)}$	129.0	51.6
Power (uW)	63.0	25.0

standard cell library from Kyoto University [38] based on Rohm's 0.18 μm technology is used.

The following four netlists are designed.

1. Straightforward (S in Figs. 5.24 and 5.25): Logic synthesis (LS) and Place and Route (P&R) are performed with the typical-delay condition of the library. None of D FFs are replaced with Canary FFs. This design is vulnerable to timing errors and is impractical.
2. Worst-Case (W): LS and P&R are performed with the maximum-delay condition. None of D FFs are replaced with Canary FF. This is the traditional worst-case design result. It relies on a large timing margin so that it is protected from timing errors.
3. Canary (C): LS and P&R are performed with the typical-delay condition. The selective replacement method is used so that only timing-critical D FFs are replaced with Canary FF. This is the typical case design result. It is tolerable to timing errors with the help of the Canary FF.
4. All-Canary (A): LS and P&R are performed with the typical-delay condition and all D FFs are replaced with Canary FFs. While this is tolerable to timing errors, the increase in chip area and in power consumption will be serious.

The second step evaluates DVS based on instruction set simulations [39]. MeP simulator provided by Toshiba is used in order to generate execution traces. It is cycle accurate and models a quad-core processor. Benchmark programs are bubble, matmul, perm, qsort, queen, and sieve, which are selected from Stanford Integer

Table 5.5 Effect of selective replacement method

	Total # of FF (A)	# of Replaced FF (B)	Ratio (B/A) (%)
MeP	3,732	60	1.6
MiniMIPS	1,967	228	11.6

Benchmarks. A multiprogramming environment is assumed and thus the combinations of the programs running on the processor is ${}_6C_4 = 15$. Each trace is injected into an in-house simulator, which models DVS in detail.

Results

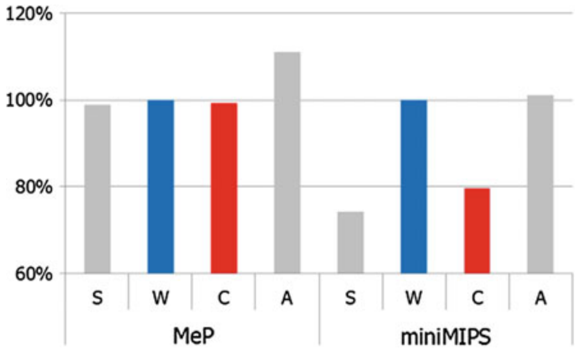
Figure 5.23 represents the hard macro cell of the Canary FF. Table 5.4 compares the cell with a D FF cell. It can be easily seen that both the cell area and the power consumption is 2.5 times larger in the Canary FF than in the D FF.

Table 5.5 presents the experimental results of the selective replacement method. The percentages of the Canary FFs over all FFs are 11.6% for miniMIPS and only 1.6% for MeP. The results confirm that the method works well to minimize the number of Canary FFs.

Figure 5.24 compares the chip areas of the four netlists after P&R. Each bar represents the relative chip area normalized by that of the Worst-Case case. In both processor cores, All-Canary is larger than Straightforward. This means that replacing all D FFs with Canary FF has the serious impact on the chip area. Even when All-Canary is compared with worst-case, both of which are timing-error-tolerant and practical, the difference between the two is not negligible. The selective replacement method successfully reduces the area overhead. The area is significantly reduced from All-Canary to Canary. When Canary is compared with Worst-Case, the chip area is reduced by 0.8% and 20.4% for MeP and miniMIPS, respectively. The reason why Canary is smaller than Worst-Case is that Canary FFs relax timing constraints and thus some of the powerful and large logical gates are not required.

Figure 5.25 summarizes the power consumption results. For each case, the bar is normalized by that of Worst-Case. It should be noted that the supply voltage is

Fig. 5.24 Chip area results



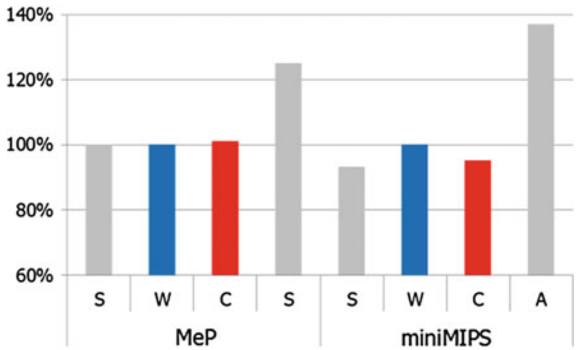


Fig. 5.25 Power consumption results

identical for every case. The selective replacement method works well also for limiting the increase in power consumption. It is considerably reduced from All-Canary to Canary. When Canary is compared with Worst-Case, the power consumption is slightly increased by 1% in the case of MeP and is rather decreased by 5% in the case of miniMIPS. From these results, Canary is superior to Worst-Case from the point of view of area and power.

The wasteful power is the difference between Worst-Case and Straightforward in Fig. 5.25. It is almost 0% for MeP and 7% for miniMIPS. This does not mean the typical-case design is useless. Please remember that the supply voltage is identical for both cases. If DVS was applied to Canary, power consumption would be further decreased. This is possible because Canary FF predicts timing errors and thus the supply voltage can be decreased without causing timing errors. This is evaluated in the second step. The instruction set simulation results of a quad-core MeP show that applying DVS reduces energy consumption by 21.2% and 18.6% on average without and with considering process variation, respectively [39]. The impact on performance is very small and the degradation is less than 2%.

In summary, the typical-case design successfully reduces power consumption without serious impact on chip area or on performance.

5.4.3 Conclusions

This chapter introduces the typical case design with the help of the Canary FF.

Although the Canary FF cell is 2.5 times larger than the conventional D FF, the selective replacement method minimizes the increase in area and power at the chip level. In the case of the single-core MeP, only 2% of D FFs are replaced. The chip-level P&R results show that there are no significant differences in design quality between the traditional worst case design and the typical case design. If DVS is applied to the quad-core MeP, energy consumption is reduced by 18.6% without serious impact on performance. The results show that the timing-error-tolerant design utilizing the Canary FF is practical and is one of the promising design methods for future process technologies vulnerable to PVT variations.

5.5 Fine-Grain Assist Bias Control for Dependable SRAM

Koji Nii, Renesas Electronics Corporation

5.5.1 *Introduction*

For low-power and low-voltage operation below 1.0 V, robust design under process variations is necessary to produce a deep-submicron dependable system-on-chip (SoC). Especially, embedded SRAMs are facing scaling limitations because of increasing V_{th} variation of transistors. To date, many design techniques that introduce SRAM assist circuits to enhance the read/write-margin have been reported [40–46]. These techniques are useful for maximizing the operating margins by controlling the bias of wordlines (WLs), bitlines (BLs), and power supply source lines of bitcells (VDM). These reports are discussed using DC characteristics [47, 48] later in the next subsection. To further improve read/write-margin, some recent assist circuits use the benefits of dynamic stability [49–53]. By using self-adjustable circuits or trimming variable elements with a fuse by memory BIST, each bias is adjusted automatically to optimum bias depending on the PVT (process-originated V_{th}) variations. However, since these approaches are introduced in a unit of large memory macro, the improvement of the minimum operating voltage (V_{min}) of SRAM is smaller or even worse than expected with the increasing number of SRAM capacity. Therefore, an individual bias control for each WL, BL, and VDM is necessary for additional improvement of SRAM V_{min}. As described herein, we propose a fine-grained assist bias control technique for enhancing the read/write-margin under low supply voltage operation: less than 1.0 V.

5.5.2 *Conflicting Issues of Read-Assist*

Figure 5.26 shows a typical schematic of the 6T SRAM bitcell with read- and write-assist circuits. Here, the WL bias lowering technique as a read-assist circuit is introduced to enhance the read-margin. In a write-operation, the VDM bias of the selected column is lowered using a write-assist circuit to improve the write-margin. Figure 5.27a portrays how the butterfly curves are affected by local V_{th} variations when the WL is activated. The static noise margin (SNM) [47] is improved by lowering the WL voltage as a read-assist. Figure 5.27b also shows the

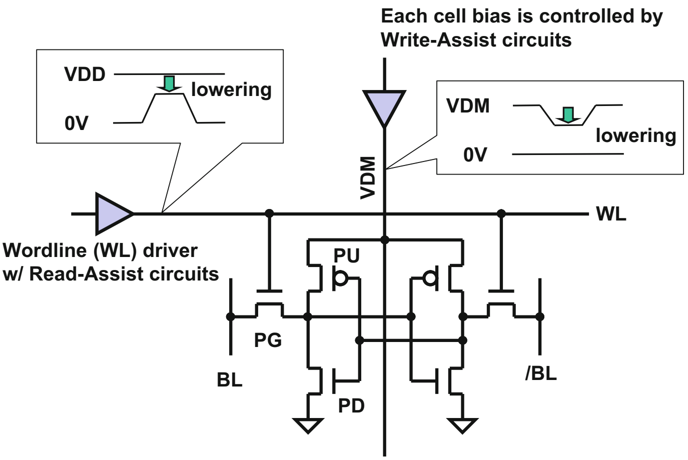


Fig. 5.26 Typical scheme of 6T-SRAM bitcell with read-/write-assist circuits

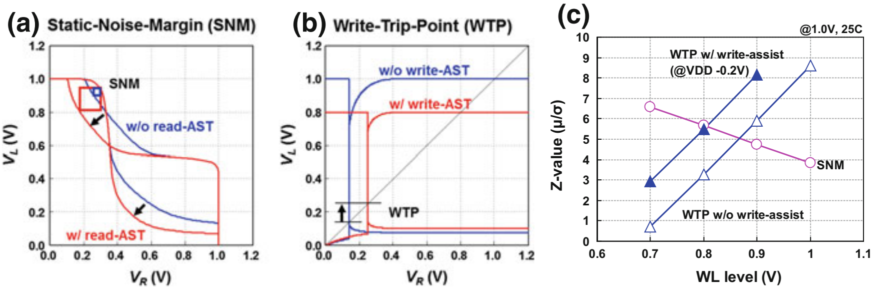


Fig. 5.27 **a** Static noise margin (SNM) [47] of the 6T SRAM w/ and w/o read-assist. **b** Write-trip-point (WTP) [48] of the 6T SRAM w/ and w/o write-assist. **c** SNM and write margin (WTP) of the 6T SRAM depending on WL bias lowering

write-margin, defined as the write-trip-point (WTP) [48] with consideration of local V_{th} variations. Because of the VDM bias lowering in a selected column as a write-assist, the WTP voltage becomes higher, thereby improving the write-margin. Figure 5.27c presents the dependences of SNM and WTP on WL bias. The typical supply voltage (VDD) is 1.0 V and the temperature is 25 °C. The Z-value of the vertical axis is defined by the mean value (μ) over the standard deviation (σ), indicating robustness against V_{th} local variations of the bitcell. Although the WL lowering improves the SNM, the write-margin degrades greatly below 0.8 V, even if the write-assist is introduced. For this reason, the bitcells with smaller write-margin are deteriorated by the WL lowering because of decreased overdrive voltage Vgs of the pass-gate (PG).

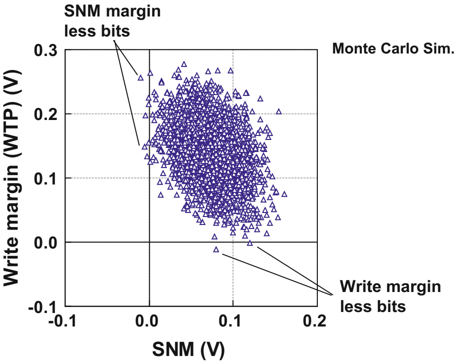
5.5.3 Concept of a Fine-Grained Assist Control

Monte Carlo simulation incorporating local V_{th} variations shows that the read-margin (denoted as SNM) and write-margin (denoted as WTP) are negatively correlated, as portrayed in Fig. 5.28. Note that there is no appearance probability of both read- and write-failure. In addition, read-margin-less bits have sufficient margin for write-operation, whereas write-margin-less bits have sufficient margin for a read operation. Ideally, the WL bias lowering is only introduced for the read-margin-less bitcells; however, that is not feasible because each WL is commonly connected to the bitcells arranged in the same row of the cell array. Thus, we propose the individual assist bias control for a fine-grained cell array region with feasibility. Figure 5.29 presents the concept of the proposed fine-grained assist bias control. A number of rows are grouped as an X-segment for read-assist to suppress the WL bias commonly. Otherwise, several columns are grouped as a Y-segment for write-assist to suppress the cell VDD bias commonly. Each read-assist bias corresponding to X-segment is controlled individually where the read-failure bits exist or not. Each write-assist bias corresponding to the Y-segment is also controlled individually where the write-failure bits exist or not.

5.5.4 Practical Dependable SRAM Macro with Fine-Grained Assist Control

Figure 5.30 shows a schematic diagram of the proposed 128 kb SRAM macro. For read-assist operation, we divided the 256 × 512 cell array into 16 X-segments and 8 Y-segments. Each X-segment has 256 columns by 32 rows; each Y-segment has 32 columns by 512 rows. We assign the two digits as bias conditions in each segment so that the assist bias can be selected with four levels. Consequently, additional 64 registers in all are necessary to set the bias conditions for read-assist and write-assist. A practical read-assist circuit and write-assist circuit are presented

Fig. 5.28 Correlation between SNM and WTP using Monte Carlo simulation for a 6T SRAM bitcell



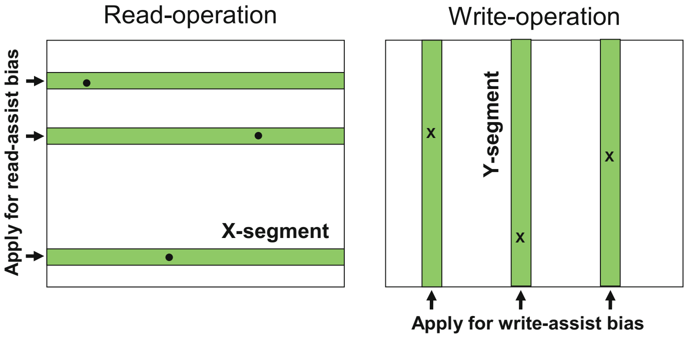


Fig. 5.29 Concept of a fine-grained assist bias control

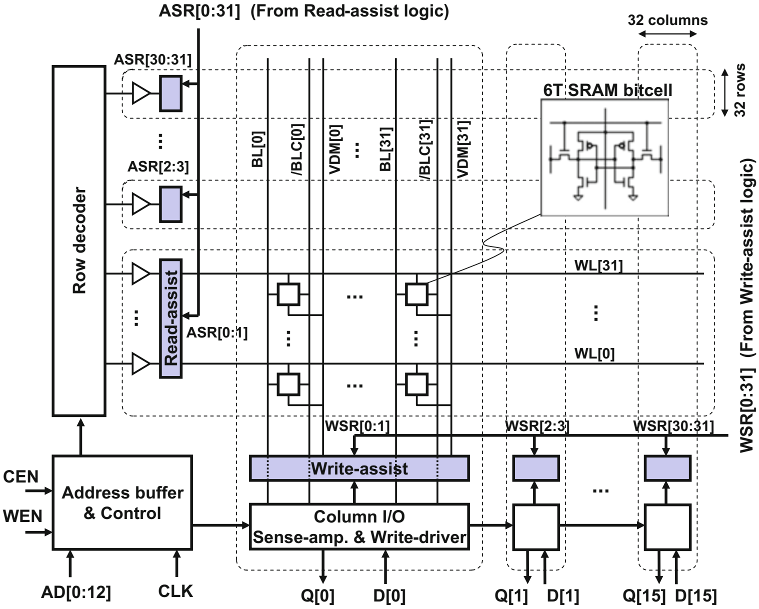
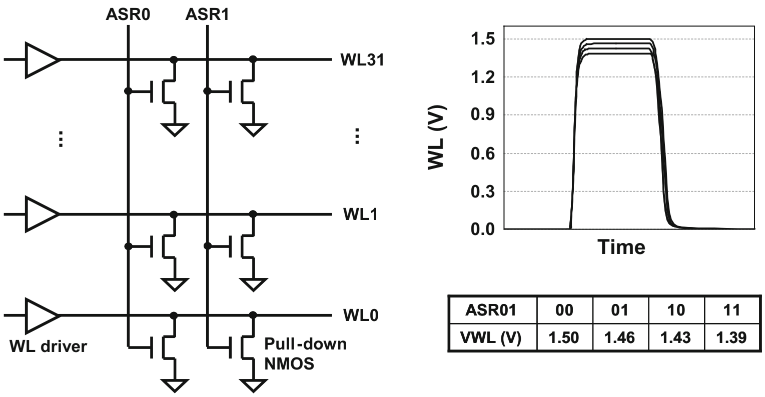


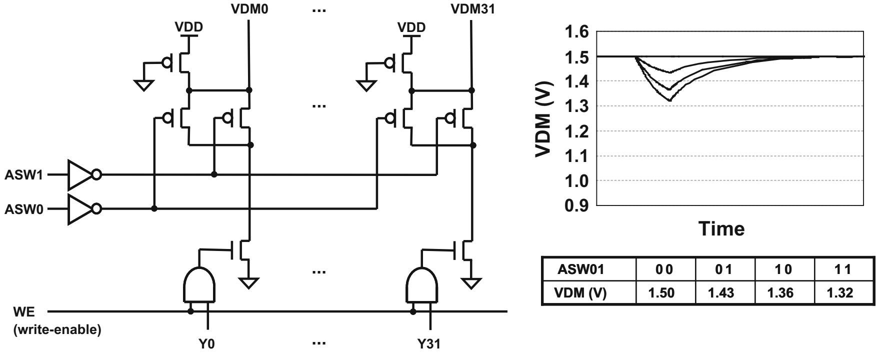
Fig. 5.30 Schematic diagram of proposed SRAM macro

in Fig. 5.31 and Fig. 5.32, respectively. The read-assist circuit has two pull-down NMOS in each row, whose drain and gate are connected to each WL and assist signal: ASR0, ASR1. The biases from WL0 to WL31 have much lower voltage to enhance the SNM if the ASR0 = ASR1 = “H”, reducing by 110 mV as shown in the simulated waveform. On the other hand, when the ASR0 = ASR1 = “L”, they are equal to VDD levels. In such cases, all bitcells within an X-segment have much margin for SNM and originally need not enhance the read-margin any further. Each column has two pull-down NMOS, whose gates are connected to the assist signals



ASR01	00	01	10	11
VWL (V)	1.50	1.46	1.43	1.39

Fig. 5.31 Proposed practical read-assist circuit and its simulated waveform



ASW01	00	01	10	11
VDM (V)	1.50	1.43	1.36	1.32

Fig. 5.32 Proposed practical write-assist circuit and its simulated waveform

ASW0 and ASW1 in Fig. 5.32, respectively. In the write-operation, the write-enable WE and one of the column decode signals from Y0 to Y31 are activated, turning on the footer NMOS corresponding to the selected column. If the assist signals ASW0 and ASW1 are equal to “H”, then both pull-down PMOS turn on. Then the much lower bias for VDM is driven to enhance the write-margin. Otherwise, if the ASW0 and ASW1 are equal to “L”, then VDM remains at a constant level as a supply voltage of VDD. In this case, all bitcells within the Y-segments have good write-margins. There is no need to apply the assist bias further. Each VDM level according to the ASW0 and ASW1 is also shown in Fig. 5.32.

Figure 5.33a presents the proposed dependable embedded SRAM with assist logics and a memory BIST. To control the individual bias, additional registers, which store the bias conditions, are added to the assist logics. Figure 5.33b shows that these registers are set by an assist controller according to the test flows. After

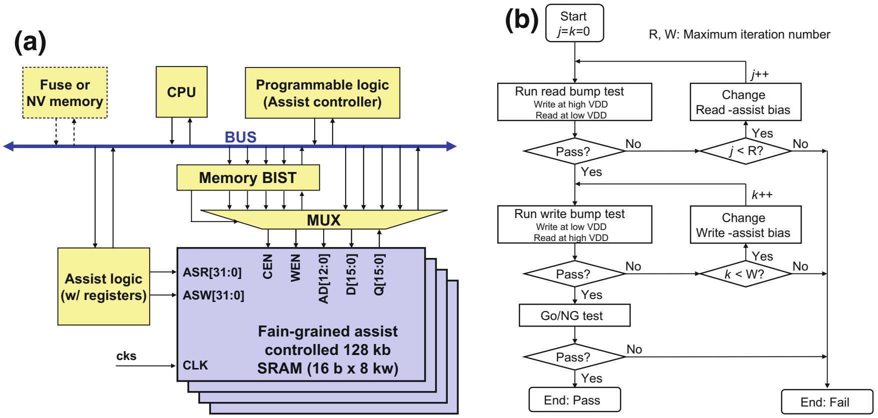


Fig. 5.33 **a** Proposed dependable SRAM with an assist logic and a memory BIST. **b** Test flows of the proposed fine-grained assist bias control with memory BIST

the screening test, the values of registers of the assist logics are stored to the fuse elements located in the same die or to the external nonvolatile memory. In the field, the registers of the assist logic are set merely by loading data from the fuse blocks or external nonvolatile memory at power-on. The assist bias can be turned in the field by running a diagonal memory BIST if a nonvolatile memory is used. This contributes to the improvement of reliability against aging degradation of the drain currents such as NBTI of pull-up PMOS in bitcells.

5.5.5 90 nm Test Chip Implementation and Measurement Results

To evaluate the effect of proposed assist circuits, we design and fabricate micro-controller test chips using 90-nm Low-Standby Power (LSTP) CMOS technology. Figure 5.34a shows a microphotograph and layout plot of the test chip. The die size is 59.3 mm^2. The test chip has a CPU with peripheral logics instruction memories, and an embedded Programmable Logic matrix (ePLX) [54]. It also includes 40 instances of 128 kb proposed SRAM macros, totally embedding 5-Mb storage capability. Memory BIST circuits are also implemented for screening the failure bits. During the setup period after power-on, the ePLX roles as an assist controller to set each assist bias condition to the registers of assist logics, temporarily. These assist logics with registers are placed around the SRAM macros. For the entire embedded 5 Mb SRAM, the logic gate counts including the memory BIST and assist logics are 244 k-gates. Although the overhead of the additional assist logic is 63% of the total logic for 5 Mb SRAM, the area penalty is less than 1% of the die area. Figure 5.34b portrays the layout plot of the proposed 128 kb

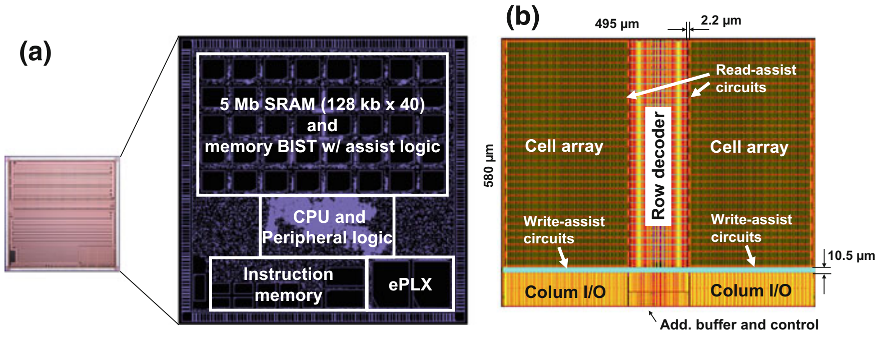


Fig. 5.34 **a** Microphotograph and layout plot of designed and fabricated test chips using 90-nm CMOS technology. **b** Layout plot of the 128 kb SRAM macro with fine-grained R/W assist bias control

Table 5.6 Features of the fabricated test chips

Technology	90-nm LSTP CMOS bulk process with 6 Cu-metals and AL-top-metal
Chip size	7.7 mm × 7.7 mm
Target speed	150 MHz @1.5 V ± 10%, −40 to 125 °C
Key IPs	
(1) Programmable logic	Programmable logic matrix (ePLX) [54]
(2) Embedded SRAM	5 Mb (128 kb × 40 instances)
	128 kb macro size: 580 μm × 495 μm
	6T bitcell size: 1.25 μm^2
(3) Memory BIST w/ Peri. and SRAM assist logic	244 k gates
	(BIST + Peri: 150 k gates, Assist: 94 k gates)

SRAM macro. The fine-grained read-assist circuits are placed between cell array and row decoder, whereas the fine-grained write-assist circuits are inserted between the cell array and column I/O peripheral blocks. The macro is 580 μm × 495 μm; the area overheads of the assist circuits are only 3%. The test chip features are presented in Table 5.6.

Figure 5.35a portrays the measured typical fail-bit-maps (FBM) of 25.5 kb (128 kb × 2) SRAM at 0.7 V and 25 °C. We observed each address of failure bits for read-bump tests; write-bump tests were different from each other. Applying an individual bias for each X-/Y-segment including failure bits enables successful 0.7 V operation. Figure 5.35b shows the measured V_{min} of 1 Mb SRAM for each case: original without assists, conventional assists, and proposed assists. It sometimes happens that the V_{min} of conventional assists becomes worse than the original without assists because all WLs are suppressed to improve the read-margin first

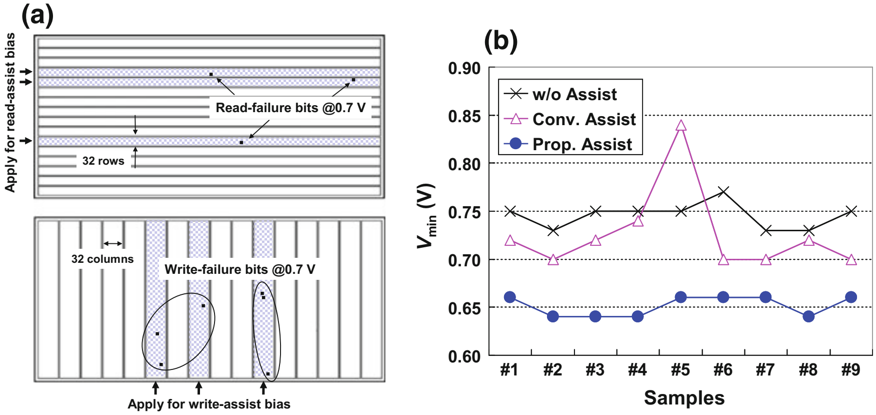


Fig. 5.35 **a** Measured fail-bit-maps (FBMs) of 256 kb (128 kb × 2) SRAM for read-/write-bump tests. **b** Measured $V_{\min}$ of 1 Mb SRAM

despite the existing write-margin less bits. In this conventional case, the write-margin gets worse adversely, resulting in the $V_{\min}$ degradation. Although the proposed fine-grained assist bias control technique suppresses the WL bias for some segments, resulting in further $V_{\min}$ improvement, which is from 70 to 110 mV compared to the original one. The results show that the minimum $V_{\min}$ of 1 Mb SRAM is achieved as 0.64 V, which is improved by 21% at most compared to the conventional assist circuits.

5.5.6 Summary

In this section, a fine-grained assist bias control technique for enhancing read-/write-margins of an embedded SRAM [55] is introduced. Further improvement of $V_{\min}$ of SRAM macro was presented with a small area overhead. We designed and fabricated test chips with plural 128 kb SRAMs using 90 nm CMOS technology. The evaluation results demonstrated that $V_{\min}$ was 0.64 V, which is 21% better than that achieved using conventional techniques.

Acknowledgments This work was supported in part by JST CREST DVLSI project, by JSPS Grant-in-Aid for Exploratory Research, and by the fund from Central Research Institute of Fukuoka University. It was also supported by VDEC of the University of Tokyo in collaboration with Synopsys Inc., Cadence Design Systems Inc., and Rohm Co. Ltd. The cell library used in this research was developed by Tamaru and Onodera laboratory, Kyoto University and is released by Kazutoshi Kobayashi of Kyoto Institute of Technology. The authors sincerely appreciate Shunitsu Kohara of Toshiba Corporation for helping them use MeP simulator.

References

1. J.K. Kuhn et al., Process technology variation. IEEE Trans. Electron Devices **58**(8), 2197–2208 (2011)
2. H. Onodera, Variability modeling and impact on design, in *Proceedings of IEDM*, pp. 701–704, Dec 2008
3. H. Onodera, H. Terada, Characterization of WID delay variability using RO-array test structure, in *Proceedings of ASICON,* pp. 658–661, Oct 2009
4. M. Pelgrom et al., Matching properties of MOS transistors. IEEE J. Solid-State Circ. **24**(5), 1433–1440 (1989)
5. K. Itoh, Adaptive circuits for the 0.5-V nanoscale CMOS era, in *IEEE ISSCC Digest of Technical Papers,* pp. 14–20, Feb 2009
6. S. Dighe et al., Within-die variation-aware dynamic-voltage-frequency-scaling with optimal core allocation and thread hopping for the 80-core teraFLOPS processor. IEEE J. Solid-State Circ. **46**(1), 184–193 (2011)
7. M. Floyd et al., Introducing the adaptive energy management features of the power 7 chip. IEEE Micro **21**(2), 60–75 (2011)
8. N. Kamae et al., A body bias generator compatible with cell-based design flow for within-die variability compensation, in *Proceedings of ASSCC*, pp. 389–392, Nov 2012
9. A built-in self-adjustment scheme with adaptive body bias using P/N-sensitive digital monitor circuits. in *Proceedings of ASSCC*, pp. 101–104, Nov 2012
10. X. Lu, Z. Li, W. Qiu, D.M.H. Walker, W. Shi, PARADE: parametric delay evaluation under process variation, in *Proceedings of International Symposium on Quality Electronic Design*, pp. 276–280, Mar 2004
11. W. Wang, V. Reddy, A.T. Krishnan, R. Vattikonda, S. Krishnan, Y. Cao, Compact modeling and simulation of circuit reliability for 65-nm CMOS technology. IEEE Trans. Device Mater. Reliab. **7**(4), 509–517 (2007)
12. T.E. Rahkonen, J.T. Kostamovaar, The use of stabilized CMOS delay lines for the digitization of short time intervals. IEEE J. Solid-State Circ. **28**(8), 887–894 (1993)
13. R. Datta, A. Sebastine, A. Raghunathan, J.A. Abraham, On-chip delay measurement for silicon debug, in *Proceedings of Great Lakes Symposium of VLSI*, pp. 145–148, Apr 2004
14. K. Arabi, H. Ihs, C. Dufaza, B. Kaminska, Dynamic digital integrated circuit testing using oscillation-test method. Electron. Lett. **34**(4), 762–764 (1998)
15. X. Wang, M. Tehranipoor, R. Datta, Path-RO: a novel on-chip critical path delay measurement under process variations, in *Proceedings of International Conference on Computer-Aided Design*, pp. 640–646, Nov 2008
16. D. Ernst, N.S. Kim, S. Das, S. Pant, T. Pham, R. Rao, C. Ziesler, D. Blaauw, T. Austin, T. Mudge, K. Flautner, Razor: a low-power pipeline based on circuit-level timing speculation, in *Proceedings International Symposium on Microarchitecture*, pp. 7–18, Dec 2003
17. T. Sato, Y. Kunitake, A simple flip-flop circuit for typical-case designs for DFM, in *Proceedings of International Symposium on Quality Electronic Design*, pp. 539–544, Mar 2007
18. B.I. Dervisoglu, G.E. Stong, Design for testability: using scan path techniques for path-delay test and measurement, in *Proceedings of International Test Conference*, pp. 365–374, Oct 1991
19. S. Jin, Y. Han, H. Li, X. Li, Unified capture scheme for small delay defect detection and aging prediction. IEEE Trans. Very Large Scale Integr. Syst. **21**(5), 821–833 (2013)
20. S. Tam, S. Rusu, U.N. Desai, R. Kim, J. Zhang, I. Young, Clock generation and distribution for the first IA-64 microprocessor. IEEE J. Solid-State Circ. **35**(11), 1545–1552 (2000)
21. T. Xanthopoulos (ed.), *Clocking in Modern VLSI Systems* (Springer, New York, 2009)
22. Y. Sato, S. Kajihara, T. Yoneda, K. Hatayama, M. Inoue, Y. Miura, S. Ohtake, T. Hasegawa, M. Sato, K. Shimamura, DART: dependable VLSI test architecture and its implementation, in *Proceedings of International Test Conference*, 15.2, Nov 2012

23. Y. Miura, Y. Sato, Y. Miyake, S. Kajihara, On-chip temperature and voltage measurement for field testing, in *Proceedings of European Test Symposium*, p. 181, May 2012
24. S. Borkar, T. Karnik, S. Narendra, J. Tschanz, A. Keshavarzi V. De, Parameter variations and impact on circuits and microarchitecture, in *40th Design Automation Conference*, pp. 338–342, June 2003
25. O. Unsal, J. Tschanz, K. Bowman, V. De, X. Vera, A. Gonzales, O. Ergin, Impact of parameter variations on circuits and microarchitecture. IEEE Micro **26**(6), 30–39 (2006)
26. M. Agarwal, B.C. Paul, M. Zhang, S. Mitra, Circuit failure prediction and its application to transistor aging, in *25th VLSI Test Symposium*, pp. 227–286, May 2007
27. S. Mitra, N. Seifert, M. Zhang, Q. Shi, K.S. Kim, Robust system design with built-in soft-error resilience. IEEE Comput. **38**(2), 43–52 (2005)
28. T. Nakura, K. Nose, M. Mizuno: Fine-grain redundant logic using defect-prediction flip-flops, in *IEEE ISSCC Digest of Technical Papers*, pp. 402–402, Feb 2007
29. M. Nicolaidis, Time redundancy based soft-error tolerance to rescue nanometer technologies, in *17th VLSI Test Symposium*, pp. 86–94, Apr 1999
30. T. Sato, Y. Kunitake, Canary: a variation resilient ff to eliminate design margin for energy reduction. IPSJ J. **49**(6), 2029–2042 (2008) (in Japanese)
31. M. Zhang, T.M. Mak, J. Tschanz, K.S. Kim, N. Seifert, D. Lu, Design for resilience to soft errors and variations, in *13th International On-Line Testing Symposium*, pp. 23–28, July 2007
32. T. Sato, I. Arita, in *Constructive Timing Violation for Improving Energy Efficiency*, ed. by L. Benini, M. Kandemir, J. Ramanujam. Compilers and Operating Systems for Low Power (Springer, 2003), pp. 137–153
33. Y. Kunitake, T. Sato, H. Yasuura, T. Hayashida, A selective replacement method for timing-error-predicting flip-flops. J. Circ. Syst. Comput. **21**(6), 14 (2012)
34. K. Yano, T. Hayashida, T. Sato, Improving timing error tolerance without impact on chip area and power consumptions, in *15th International Symposium on Quality Electronic Design*, pp. 389–394, Mar 2013
35. K. Yano, T. Yoshiki, T. Hayashida, T. Sato, An automated design approach of dependable VLSI using improved Canary FF, in *7th International Workshop on Unique Chips and Systems*, pp. 34–39, Feb 2012
36. A. Mizuno, K. Kohno, R. Ohyama, T. Tokuyoshi, H. Uetani, H. Eichel, T. Miyamori, N. Matsumoto, M. Matsui, Design methodology and system for a configurable media embedded processor extensible to VLIW architecture, in *International Conference on Computer Design*, pp. 2–7, Sept 2002
37. OpenCores: miniMIPS, http://opencores.org/project,minimips. Accessed 16 Sept 2013
38. H. Onodera, A. Hirata, T. Kitamura, K. Tamaru, P2lib: process-portable library and its generation system, in *Custom Integrated Circuits Conference*, pp. 341–44, May 1997
39. T. Sato, T. Hayashida, K. Yano, Dynamically reducing overestimated design margin of multicores, in *10th International Conference on High Performance Computing & Simulation*, pp. 403–409, July 2012
40. M. Yamaoka, N. Maeda, Y. Shinozaki, Y. Shimazaki, K. Nii, S. Shimada, K. Yanagisawa, T. Kawahara, 90-nm process-variation adaptive embedded SRAM modules with power-line-floating write technique. IEEE J. Solid-State Circ. **41**(3), 705–711 (2006)
41. S. Ohbayashi, M. Yabuuchi, K. Nii, Y. Tsukamoto, S. Imaoka, Y. Oda, T. Yoshihara, M. Igarashi, M. Takeuchi, H. Kawashima, Y. Yamaguchi, K. Tsukamoto, M. Inuishi, H. Makino, K. Ishibashi, H. Shinohara, A 65-nm soc embedded 6T-SRAM designed for manufacturability with read and write operation stabilizing circuits. IEEE J. Solid-State Circ. **42**(4), 820–829 (2007)
42. M. Yabuuchi, K. Nii, Y. Tsukamoto, S. Ohbayashi, S. Imaoka, H. Makino, Y. Yamagami, S. Ishikura, T. Terano, T. Oashi, K. Hashimoto, A. Sebe, G. Okazaki, K. Satomi, H. Akamatsu, H. Shinohara, A 45 nm low-standby-power embedded SRAM with improved immunity against process and temperature variations, in *IEEE ISSCC Digest of Technical Papers*, pp. 326–327, Feb 2007

43. K. Nii, M. Yabuuchi, Y. Tsukamoto, S. Ohbayashi, Y. Oda, K. Usui, T. Kawamura, N. Tsuboi, T. Iwasaki, K. Hashimoto, H. Makino, and H. Shinohara, A 45-nm single-port and dual-port SRAM family with robust read/write stabilizing circuitry under DVFS environment, in *Symposium on VLSI Circuits Digest of Technical Papers*, pp. 212–213, June 2008
44. Y. Fujimura, O. Hirabayashi, T. Sasaki, A. Suzuki, A. Kawasumi, Y. Takeyama, K. Kushida, G. Fukano, A. Katayama, Y. Niki, T. Yabe, A configurable SRAM with constant-negative-level write buffer for low-voltage operation with 0.149 um^2 cell in 32 nm high-k metal gate CMOS, in *IEEE ISSCC Digest of Technical Papers*, pp. 348–349, Feb 2010
45. T. Yabe et al., Circuit techniques to improve disturb and write margin degraded by MOSFET variability in high-density SRAM cells, in *Symposium on VLSI Circuits Digest of Technical Papers*, June 2011
46. H. Pilo, I. Arsovsi, K. Batson, G. Braceras, J. Gabric, R. Houle, S. Lamphier, C. Radens, A. Seferagic, A 64 Mb SRAM in 32 nm high-k metal-gate SOI technology with 0.7 V operation enabled by stability, write-ability and read-ability enhancements. IEEE J. Solid-State Circ. **47** (1), Jan 2012
47. E. Seevinck, F.J. List, J. Lohstroh, Static-noise margin analysis of MOS SRAM cells. IEEE J. Solid-State Circ. **SC-22**(5), 748–754 (1987)
48. R. Heald, P. Wang, Variability in sub-100 nm SRAM designs, in *IEEE/ACM ICCAD Digest of Technical Papers*, pp. 347–352, Nov 2004
49. M. Khellah, Y. Ye, N. Kim, D. Somasekhar, G. Pandya, A. Farhang, K. Zhang, C. Webb, V. De, Wordline & bitline pulsing schemes for improving SRAM cell stability in low-Vcc 65 nm CMOS designs, in *Symposium VLSI Circuits Digest Technical Papers*, pp. 9–10, June 2006
50. H. Pilo, C. Barwin, G. Braceras, C. Browning, S. Lamphier, F. Towler, An SRAM design in 65-nm technology node featuring read and write-assist circuits to expand operating voltage. IEEE J. Solid-State Circ. **42**(4), 813–819 (2007)
51. M. Yamaoka, K. Osada, T. Kawahara, A cell-activation-time controlled SRAM for low-voltage operation in DVFS SoCs using dynamic stability analysis, in *Proceedings of European Solid-State Circuits Conference* (*ESSCIRC*), pp. 286–289, Sep 2008
52. H. Nho, P. Kolar, F. Hamzaoglu, Y. Wang, E. Karl, Y. Ng, U. Bhattacharya, K. Zhang, A 32 nm high-k metal gate SRAM with adaptive dynamic stability enhancement for low-voltage operation, in *IEEE ISSCC Digest of Technical Papers*, pp. 346–347, Feb 2010
53. E. Karl, Y. Wang, Y.-G. Ng, Z. Guo, F. Hamzaoglu, U. Bhattacharya, K. Zhang, K. Mistry, M. Bohr, A 4.6 GHz 162 Mb SRAM design in 22 nm tri-gate CMOS technology with integrated active VMIN-enhancing assist circuitry, in *IEEE ISSCC Digest of Technical Papers*, pp. 230–231, Feb 2012
54. H. Nakano, T. Iwao, T. Hishida, H. Shimomura, T. Izumi, T. Fujino, Y. Okuno, K. Arimoto, An embedded programmable logic matrix (ePLX) for flexible functions on SoC, in *IEEE ASSCC Digest of Technical Papers*, pp. 219–222, Nov 2006
55. K. Nii, M. Yabuuchi, H. Fujiwara, H. Nakano, K. Ishihara, H. Kawai, K. Arimoto, Dependable SRAM with enhanced read/write-margins by fine-grained assist bias control for low-voltage operation, in *Proceedings of IEEE International SOC Conference*, pp. 519–524, Sept 2010

Chapter 6
Time-Dependent Degradation in Device Characteristics and Countermeasures by Design

Takashi Sato, Masanori Hashimoto, Shuhei Tanakamaru, Ken Takeuchi, Yasuo Sato, Seiji Kajihara, Masahiko Yoshimoto, Jinwook Jung, Yuta Kimi, Hiroshi Kawaguchi, Hajime Shimada and Jun Yao

Abstract Advancement of process technologies has significantly improved the performance of semiconductor devices and consequently of circuits. Device lifetime, on the other hand, has been unavoidably compromised through the introductions of new materials, new process technologies, etc. Mitigating measures against transient degradation of circuit performance are now what all circuit designers should know. In this chapter, techniques to monitor device degradation

T. Sato (✉)
Kyoto University, Kyoto, Japan
e-mail: takashi@i.kyoto-u.ac.jp

M. Hashimoto
Osaka University, Suita, Japan
e-mail: hasimoto@ist.osaka-u.ac.jp

S. Tanakamaru · K. Takeuchi
Chuo University, Tokyo, Japan

Y. Sato · S. Kajihara
Kyushu Institute of Technology, Iizuka, Japan
e-mail: sato@aries30.cse.kyutech.ac.jp

S. Kajihara
e-mail: kajihara@cse.kyutech.ac.jp

M. Yoshimoto · J. Jung · Y. Kimi · H. Kawaguchi
Kobe University, Kobe, Japan
e-mail: yosimoto@cs.kobe-u.ac.jp

H. Kawaguchi
e-mail: kawapy@godzilla.kobe-u.ac.jp

H. Shimada
Nagoya University, Nagoya, Japan
e-mail: shimada@itc.nagoya-u.ac.jp

J. Yao
Huawei Technologies, Beijing, China

S. Asai (ed.), *VLSI Design and Test for Systems Dependability*,
https://doi.org/10.1007/978-4-431-56594-9_6

are introduced. By periodic monitoring, functional failures induced after fabrication can be detected. Practical circuit designs that mitigate, predict, diagnose, and recover from faults in the running systems are proposed to achieve an ultimate design goal of realizing dependable VLSIs.

Keywords Integrated circuit reliability • Multilayer aging mitigation Degradation sensing • Error correction • Error prediction and restoration

6.1 Time-Dependent Device Degradation; Mechanisms and Mitigation Measures

Takashi Sato, Kyoto University

Masanori Hashimoto, Osaka University

Long-term reliability of integrated circuits, which serve as the essential core of information systems, is becoming a serious concern. Information and communication systems are now regarded as indispensable social infrastructures and its importance will become even more significant than ever before. In order to support growing demands to process a huge amount of data that is generated in all around the world, the performance of the integrated circuits has been improved in an exponential manner following the so-called Moore's law. The aggressive scaling of device dimensions are supported by the introduction of new materials, new fabrication technologies, new device structures, etc., but these new technologies also cause adverse effects on the reliability of semiconductor devices and integrated circuits. Circuit designers and electronic system engineers need to seriously consider lifetime extension of electronic instruments as a mandatory design constraint. This constraint is particularly stringent in the circuits whose maintenance is difficult to perform. Examples are found in satellites or the devices deep under the sea. Improving the reliability of systems that affect people's lives, such as automotive and medical applications, is also crucially important.

In general, the failure probability of electronic components follows a specific trend. The trend as a function of time is illustrated in Fig. 6.1. Because of its

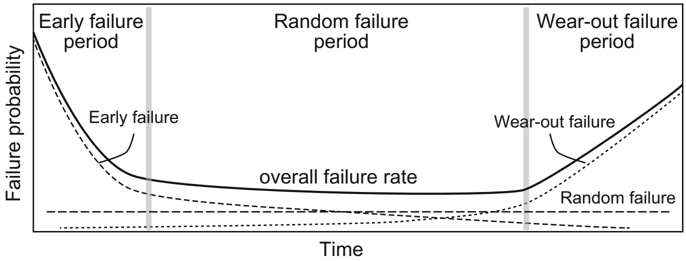


Fig. 6.1 Bathtub curve: changing failure rate as a function of time

bowl-like shape having a flat basin in the middle and the upward edges on both ends, the curve is often called *bathtub curve*. The curve comprises of three periods: early failure, random failure, and wear-out failure.

The early failure period is also called initial failure period or infant mortality. The dominant failure in this period is dominated by early failures. This period begins immediately after the first use of a chip. High failure probability, followed by decreasing failure probability, is observed. When a supply voltage is first applied, potential defects in a chip, such as partially narrowed wires or nearly shorted wires formed due to small particles on a semiconductor wafer during a manufacturing process, become apparent as an observable fault. The use of the chip containing latent defects will further damage the already weakened part because the current in the narrowed wire further enhances migration around that part due to increased current density. The failure rate gradually decreases (approximated by Weibull distributions with a shape parameter of $\beta < 1$) because the chip containing more serious latent defects fails earlier than less serious ones. Typically, through the *burn-in* testing process, in which high voltage and high temperature are applied, early failures are mostly detected.

After the early failure period, the random failure period follows wherein random failure mode is dominant. In this period, almost constant failure rate or very slow degradation of the failure rate is observed, and thus this is typically the period for the chip to be in-field use. The constant failure rate tends to become higher as more complicated process technologies or device structures are employed. The cause of the random failure also includes the latent defects that were not filtered out in the earlier period. The failure in this period arises in a random manner, which makes it difficult to predict exactly when the failure may occur. Hence, it is one of the main objectives of optimizing device structures and fabrication process to reduce the failure rates in the early failure and random failure periods.

The last part of the failure curve is the wear-out failure. The failure rate in this period increases (again approximated by Weibull distributions with $\beta > 1$) largely due to the aging or fatigue of the devices contained in a chip. In addition to the traditional shipping tests in which a chip is classified as defective or not, special consideration has to be paid to modern semiconductor devices because transient performance degradation due to aging may occur earlier than it was originally expected. It is significantly difficult to screen short lifetime chip in terms of wear-out failure with the traditional testing framework.

As process technology advances, both random defect probability and wear-out failure probability increase substantially. A paradigm shift in the integrated circuit design—*countermeasure by design*—becomes important. The inclusion of unreliable circuit components is unavoidable. In order to maintain a high level of reliability in information and communication systems, multilayers of mitigation, i.e., device-level, circuit-level, and system-level mitigation are required. Particularly, dependability of the integrated circuits, as the core of those systems, needs to be sustained for their entire lifetime by the interlayer design even when unreliable circuit components are incorporated in it.

In this section, we first explain major aging mechanisms that affect the operation of integrated circuits, and give an overview of the countermeasures to the aging effects. Thereafter, in the succeeding sections, recent advancements in aging-aware design methodologies are introduced.

6.1.1 Representative Aging Effects and Their Impact on Integrated Circuits

We first explain five representative aging effects that are listed in Table 6.1 and the problems they cause. Timing failure is a problem of which a chip becomes inoperable at a required clock frequency due to device performance degradation. Leakage increase means an increase in power dissipation, mainly through off-state transistors. The leakage current flows independently of the computation. Memory failure induces failure bits that cannot be read or written. Hard failure is an unrecoverable failure that causes a permanent malfunction.

The aging effects in integrated circuit can be categorized into two: the effects upon transistors and those upon wires. First, three representative phenomena observed in transistors are reviewed.

Time-dependent dielectric breakdown (TDDB) [1, 2] is an aging phenomenon that thin gate insulator film of a transistor becomes unable to maintain electrical isolation even within its normal ranges of operational voltage (Fig. 6.2). In addition to the initial defects formed at the time of fabrication, new defects are generated during the normal operation of the transistor by the vertical electrical field in the gate insulator film. Gate leakage current, as a consequence, gradually increases and then starts to conduct more current, which is commonly called as soft breakdown [3]. When the application of electrical field continues or becomes stronger, the number of defects further increases and the transistor finally reaches the point where the gate terminal and channel become conductive. This is called hard or complete breakdown [4]. Soft breakdown not only increases leakage current but also degrades switching performance, and hence timing and memory failures are invoked. Once hard breakdown arises, the functionality of a transistor as a switch gets totally lost, resulting in a hard failure.

Table 6.1 Representative time-dependent degradation phenomena and their impact on the operation of integrated circuits

	Timing failure	Leakage increase	Memory failure	Hard failure
TDDB	✓	✓	✓	✓
HCI	✓			
BTI	✓		✓	
EM	✓			✓
SM	✓			✓

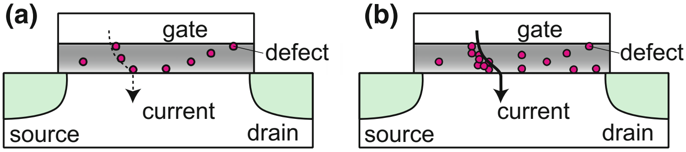


Fig. 6.2 Model of time-dependent dielectric breakdown. **a** Soft breakdown. **b** Hard breakdown. Gate leakage current in (**a**) is sufficiently small, causing almost no effect in the circuit operation. In the case of (**b**), gate leakage current is significant, causing an electrical short circuit and finally looses switching function

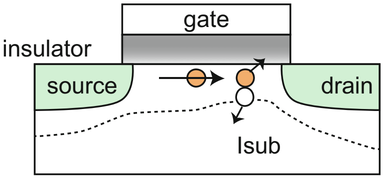


Fig. 6.3 Hot carrier injection in an n-channel MOSFET. High-energy channel carriers depicted using circles generate electron and hole pairs through impact ionization. Some of the electrons having large energy that is beyond the potential barrier of silicon and silicon dioxide interface is injected into the drain end of the gate oxide film, and the hole current is observed as substrate current (Isub)

Hot carrier injection (HCI) [5–7] is another aging effect that gradually reduces drain current of a transistor. It is caused by the charge accumulation in the oxide film. Its mechanism is pictorially illustrated in Fig. 6.3. A carrier accelerated by the electric field between source and drain hits an atom that forms a crystal near the drain region under gate insulator film, and then a high-energy electron is generated. The electron having high energy that exceeds an energy barrier of silicon and silicon dioxide interface is injected into the gate insulator film. It becomes a trapped charge that changes threshold voltage of a transistor. The decrease in device current slows down the logic operation, which degrades maximum operational frequency of a circuit [8].

Bias temperature instability (BTI) is yet another aging phenomenon in which a transistor ages while it is kept in an on state and at an elevated temperature [9, 10]. BTI decreases drain current of a transistor and hence deteriorates circuit speed with the similar mechanism to TDDB and HCI—carriers are trapped in existing or newly generated interface states in the silicon–dielectric interface, which is an explanation based on measurements [11]. BTI in an PMOS transistor is called negative BTI (NBTI) and BTI in a NMOS transistor is called positive BTI (PBTI). A differentiating characteristic of BTI from that of TDDB and HCI is that the degradation can partially recover once a transistor becomes in an off state. Aging mitigation and lifetime extension methods that exploit this feature are intensively studied.

Next, aging effects for wires are introduced.

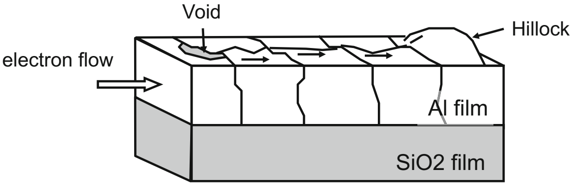


Fig. 6.4 Electromigration in Al interconnect. Strong electron flow causes the displacement of atoms that are forming the metal wires. Deformations called hillock or void may lead to short or open failure between wires

Electromigration (EM) [12, 13] is a phenomenon in which metal atoms that compose signal and power wires move due to collisions of electrons at high current densities. As a result of momentum exchange between conducting electrons and metal ions, the shape of metal wires changes, forming vacancy of metals called void or metal growth called hillock (Fig. 6.4) [14]. Resistance increases at the narrowed part of the wire due to the growth of void. Signal propagation through that part consequently becomes slower than that of the normal wires. In the case of a power wire, supply voltage drop occurs, which again results in slower operation speed. Current density also increases at the narrowed part of the wire, which eventually causes wire disconnection that results in hard failure.

Stress migration (SM) [15] is caused by tensile stress which originates from different coefficients of thermal expansion of materials, creating voids in metal wires. The impact of shape variation is the same with that of EM.

6.1.2 Device-Level Mitigation

Above-mentioned degradation phenomena are fundamentally unavoidable when the circuits are designed for advanced technology nodes. It is hence becoming increasingly important to consider better design strategy of integrated circuits so that they can maintain the original functions even after the performance degradation occurs. From that point of view, setting design margin and design guidelines, such as limiting the narrowest width of a wire, is crucially important. The design margin and guidelines facilitate integrated circuits to operate satisfying required specifications without suffering from hard error even after the system's lifespan has run out. In order to realize such robustness, understanding of physical mechanisms behind the aging phenomena is important.

Because degradation is in general accelerated at high temperatures and under high supply voltage conditions, engineers who design electronic systems that heavily employs integrated circuits can possibly inhibit degradations to prolong their lifetime by adequately controlling operation temperature and supply voltage. Such operation eventually expands systems' lifetime. Examples of the effective means include: to choose a package that efficiently removes heat generated in the circuit, to install the system in well-controlled air flows, and to spontaneously lower supply voltage whenever the computational load becomes light.

Also in the device level, predictive modeling efforts that exploit physical reasoning are actively conducted. Let us take a look at an example of BTI modeling. Ring-oscillator-based circuit that can separately measure BTI and HC has been proposed in [16]. Only on-chip counter circuit is necessary to quantitatively characterize device degradation. When statistical variation of the degradation is concerned, measurements on a lot of devices are required. The temporal change of threshold voltage in response to stress application and release has to be measured for each chip to collect statistical information. This requires very long time even if high voltages and high temperatures are given to the devices to accelerate degradation. It is almost intractable to measure the threshold changes on multiple devices under an equal environment and in practical time. In order to ease these processes, an array-like circuit structure that can apply stress and recovery bias voltages for many devices in parallel has been proposed. A measurement in [17] successfully shortens the measurements of threshold voltage shift; the measurement of 128 devices has been conducted in 15 h. Without parallelizing the stress period, this set of measurements would have taken 83 days. Even larger number of transistors has also been measured for statistically characterizing BTI [18]. The measurement results are later analyzed to find the physics behind the threshold voltage shift, and to build a physics-based model [19] that can be used in circuit design phase so that circuit designers can take preventive efforts.

6.1.3 Circuit- and System-Level Mitigation

The measures above are basically considered as *preventive* actions. As device dimensions are extensively miniaturized, effects of the temporal degradation become more pronounced. The achievable performance will hence become severely deteriorated because of the larger design margin that is reserved for possible worst degradation. Recently, the use of sensor-like circuits is considered in order to monitor the change of circuit performances. Research efforts that try to:

- predict temporal degradation so as to issue an early warning,
- detect failures and diagnose their locations, and
- remove or restore from the failures,

are extensively studied. Such measurement-based actions will effectively enhance reliability of the integrated circuits further and prolong the lifetime of electronic systems.

The prediction of temporal degradation is typically realized by implementing a sensor or a replica circuit that evaluates degradation. The circuit components that are proposed for characterizing and modeling device degradations can also be used as the degradation sensors. In [20], gate oxide reliability and degradation sensors are implemented on the chip. Implementation of such sensors by using only digital circuit design flow is becoming increasingly popular. In a large commercial microprocessor [21], ring-oscillator-based sensors to detect BTI degradation are embedded. An in-field monitoring technique to facilitate predictive maintenance will also be explained in Sect. 6.3. The degradation rate of an integrated circuit depends on the given operating condition and the environment in which the integrated circuit is used. That is why the sensor or the replica circuit is necessary to exactly detect the progress of degradation, which can differ for each chip. Just utilizing the prediction techniques gives us an estimation of remaining lifetime of the circuits.

The detection of temporal degradation is typically realized by implementing error detection circuits, which notify us when the device degradation exceeds the margin and the circuit becomes malfunctional. An example can be found in [22]. Such a circuit eliminates the chance for unnoticed faults to exist, which may later lead to a serious accident. Diagnosis that localizes the failure location is critically important to realize restoration of the circuit.

The restoration is the act to remove failures from the circuit to recover the original functionality of the circuit by disconnecting the source of failure. Those are the measures such as an adaptive operational voltage adjustment [23] or those that use redundant circuits that are prepared in advance in its design phase (examples can be found in Sects. 6.4 and 6.5). A method that enables uninterrupted circuit operation by allowing slight performance degradation is another option and major topic of research.

In this section, temporal device degradation, which is becoming more apparent in integrated circuits that utilize advanced device technology, has been briefly reviewed and their effects to circuit operations are explained. In addition to widely conducted preventive design methodologies, more advanced measures including autonomous fault avoidance based on measurement is definitely necessary. In order to realize such fault avoidance under a practical resource constraint and within a limited performance overhead, cooperative measures considering higher layers of electrical systems, such as an application layer, are necessary.

6.2 Degradation of Flash Memories and Signal Processing for Dependability

Shuhei Tanakamaru, Chuo University

Ken Takeuchi, Chuo University

6.2.1 Cell and Circuit Structures of NAND Flash Memory

The NAND flash memory prevails as the nonvolatile memory for universal serial bus (USB) flash memories, solid-state drives (SSDs), etc. A brief description of its

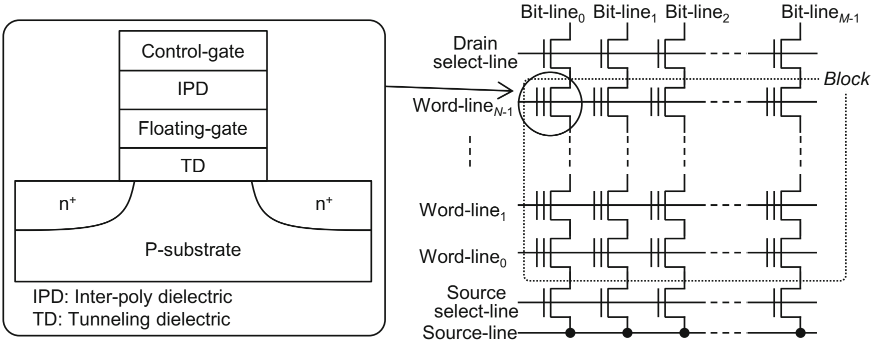


Fig. 6.5 Cell structure of NAND flash memory and schematic of cell array

principle and operation will be given in this subsection. Figure 6.5 shows the cell structure of the NAND flash memory. The basic cell and circuit structures were proposed in [24, 25] (see [26, 27] for the detailed history of development). A floating gate is added to a typical nMOS transistor. A cell is programmed by injecting electrons into the floating gate, which causes the threshold voltage increase. On the other hand, the electrons are ejected from the floating gate to erase the programmed value. Since the floating gate is surrounded by the insulator (tunneling dielectric (TD) and inter-poly dielectric (IPD)), stored electrons in the floating gate can last for a long time, which enables the nonvolatile operation. By controlling the amount of electrons stored in the floating gate, a single memory cell can store more than 1 bit [28], e.g., 2 bits/cell [29–38], 3 bits/cell [39–43], and 4 bits/cell [44, 45].

The schematic of the NAND flash memory array is also illustrated in Fig. 6.5. The memory cells are serially connected, and select gates are placed in the two ends of the cell chain. The extremely symmetrical layout of the NAND flash memory enables the aggressive scaling. Figure 6.6 illustrates the scaling trend of the NAND flash memory from 2006 to 2014, reported at the IEEE International Solid-State Circuits Conference [29–46]. The aggressive scaling has enabled the technology node to reach 16 nm in 2014. What is more, according to the International Technology Roadmap for Semiconductors (ITRS), the NAND flash memory is expected to further scale down to 12 nm [47]. However, according to the ITRS roadmap, the cell size will be stuck at 12 nm. Thus, 3D technology will be adopted to increase the capacity of the NAND flash chip by increasing the number of layers [48]. Therefore, NAND flash is the most suitable memory structure for low-cost, high-density nonvolatile memories.

Since programming and erasing a cell takes a considerably long time (e.g., Program: 1 ms, Erase: 3 ms), many cells are simultaneously programmed, read or erased to enhance the throughput. The programming unit is called a *page* which consists of memory cells in the same word-line. In 1 bit/cell NAND flash memory, a page corresponds to a word-line. On the other hand, *j* logical pages are assigned to a

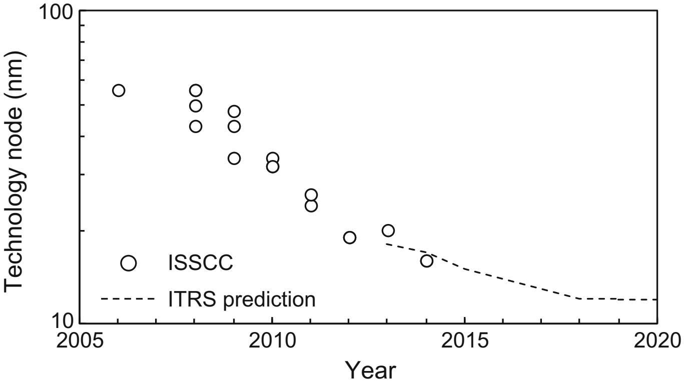


Fig. 6.6 Scaling trend of NAND flash memory [29–46]

word-line in *j* bits/cell NAND flash memory (see [49] for 2 bits/cell case). Reading is also executed to the unit of a page. Erase is performed in a larger unit, a *block*, which consists of a whole NAND flash cell string (also see Fig. 6.5). The program (T_{Prog}) and erase (T_{Erase}) throughput can be represented as follows.

$$T_{\mathrm{Prog}} = N_{\mathrm{Page}}/t_{\mathrm{Prog}},$$

and

$$T_{\mathrm{Erase}} = N_{\mathrm{Block}}/t_{\mathrm{Erase}}.$$

Here, N_{Page}, N_{Block}, t_{Prog}, and t_{Erase} are the number of cells in a page, number of cells in a block, program time, and erase time, respectively. T_{Prog} and T_{Erase} can be 7.8 MByte/s and 333 MByte/s, respectively, if a block consists of 128 8 KByte pages and the program and erase times are 1 and 3 ms.

6.2.2 Reliability Issues of NAND Flash Memory

The severe reliability issues of the NAND flash memory are becoming the main bottleneck for the production of the solid-state storage devices. In this subsection, program disturb, read disturb, data retention, write/erase stress, and scaling effects are introduced.

Figure 6.7 shows the bias conditions during program and read of the NAND flash memory [50]. A high voltage (V_{PGM}), e.g., 20 V [50], is applied to the word-line to program (write ‘0’) memory cells. Not to program a cell (write ‘1’), program inhibit voltage (V_{DD}) is applied to the bit-line of the corresponding memory cell. The channel potential is boosted up to around 8 V due to the

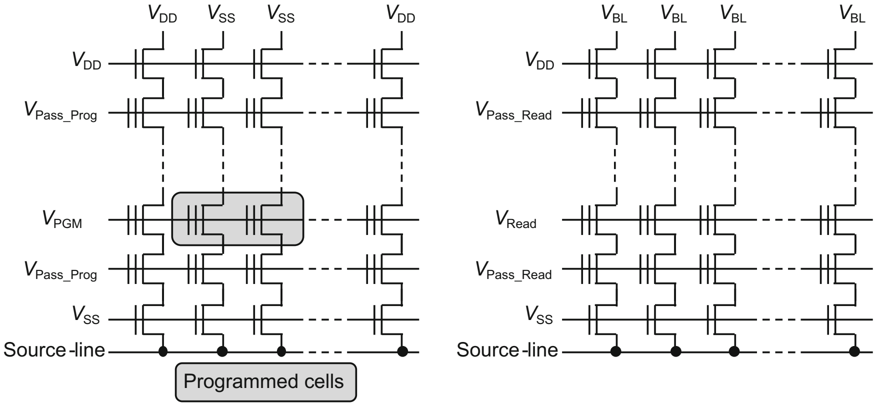


Fig. 6.7 Read and write bias conditions [50]

capacitive coupling between the control gate and the channel [50]. However, a large voltage difference remains between the control gate and the channel to cause unwanted electrons to be injected to the floating gate of the program inhibit cell resulting in increase in its threshold voltage (V_{PGM} disturb). Moreover, V_{Pass_PGM}, e.g. 10 V [50], is applied to the other word-lines to correctly transfer the bit-line voltage to each cell. Therefore, the threshold voltage of those cells also increases (V_{Pass_PGM} disturb). V_{PGM} and V_{Pass_PGM} disturbs are collectively called *program disturb*. On the other hand, during read, V_{Read} is applied to the target word-line to check if the threshold voltage of the corresponding memory cell is higher or lower than V_{Read}. V_{Pass_Read} (4.5 V [50]) is applied to the unselected word-lines to make all of the corresponding cells turned on, which induces the *read disturb*. During data retention, electrons in the floating gate gradually eject and the threshold voltage of the memory cells decreases. When a NAND flash cell is written and erased many times, the tunneling dielectric is damaged [51]. As a result, the reliability issues mentioned above are aggravated after write/erase cycling [52].

As a result of the memory cell scaling, the amount of electrons which can be stored in the floating gate is significantly reduced. Thus, only a few hundred electrons are stored in a 20 nm NAND flash cell [53], which naturally causes reliability issues to become more pronounced in the scaled NAND flash memory. Cell-to-cell interference effects also become significant as a result of memory cell scaling. During programming, the threshold voltage (or the electrons in the floating gate) of the neighboring cells increases the threshold voltage of the target memory cell. This effect is caused by the capacitive coupling of the floating gates [54] or the direct electric filed effect from the floating gate of the neighboring cell to the channel of the target cell [55]. The floating-gate-to-floating-gate capacitance and the electric field to the channel become larger in the scaled NAND flash memory. Thus, the effect becomes more severe during scaling [55]. Moreover, since the memory cells have become so small, the high electric fields during program induce unwanted hot electrons accompanied with the gate-induced drain leakage (GIDL)

[56]. The generated hot electrons are injected into the floating gate and increase the threshold voltage [56]. Although program disturb and cell-to-cell interference effects basically cause the increase in the threshold voltage, negative program disturbs which lowers the threshold voltage are also reported in the scaled NAND flash memories [57, 58]. These negative program disturbs are considered to be caused by the hot hole injection [57] or possibly by the electron leakage [58] to/from the floating gate, which is driven by the excessively strong electric field.

6.2.3 Signal Processing for Dependability

To cope with the reliability issues discussed above, various techniques are applied in various layers. For example, in the device layer, air gap technology is introduced [59]. Not only can the air gap reduce the word-line to word-line capacitance, the reduced inter floating gate capacitance decreases the cell-to-cell coupling effects. On the other hand, the memory cells in both ends of the NAND string are most subject to the GIDL disturb due to the large potential difference between the programmed cell and the select gate [56]. Therefore, dummy cells are put on the top and the bottom of the NAND cell string to alleviate the disturb issues caused by the GIDL current [44]. Problems due to the GIDL current can also be alleviated by adding only one cell in the 2 bits/cell NAND string, which can increase the bit density of the NAND flash chip. The cells in both sides of the NAND string are used as 1 bit/cell [31]. Since 1 bit/cell has the larger memory window than 2 bits/cell, 1 bit/cell is less subject to the GIDL current issue. In the circuit layer, the programming order is carefully controlled to eliminate the cell-to-cell interference effect from the upper and lower cells [45, 60]. Basically, in 2 bits/cell NAND flash, two programming steps are required to split the memory states into four [49]. If memory cells are completely programmed word-line by word-line (first programming in WL_{n+1} is applied after second programming in WL_{n}), the cell-to-cell interference from the cells in the previously programmed word-line becomes large. This is because the cell-to-cell interference is more significant when the threshold voltage shift of the neighboring cell is larger. In the optimized programming order, programming is executed back and forth of the word-line so that the cell-to-cell coupling is caused only by the second programming of WL_{n+1} [60]. The same concept is applicable to 3 bits/cell [45] and 4 bits/cell devices. Despite all the device/circuit-level problem mitigation schemes, bit-error rates (BER) for NAND flash memories down to 10^{-13}–10^{-16} (the required reliability [61]) are hard to reach in production. Therefore, system-level techniques (mainly signal processing) are also required. Error-correcting codes (ECCs), redundant arrays of independent disks (RAID), and data preprocessing are introduced below.

The bit-errors in the NAND flash memory are not burst errors, which mean that the bit-errors are almost randomly observed across the block [62]. Thus Bose–Chaudhuri–Hocquenghem (BCH) code is widely used [59, 63] and well suited in NAND flash memories because it can efficiently correct random bit-errors.

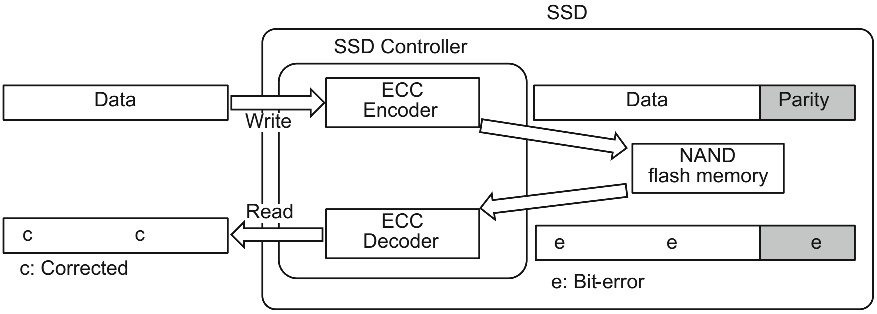


Fig. 6.8 Flow of error correction by ECC

Figure 6.8 depicts the error correction flow with ECC. Inside storage devices with NAND flash memories such as SSDs, ECC encoder and decoder are implemented in the controller. When data is written, ECC encoder adds parity bits and after that, the data is written to the NAND flash memory. Bit-errors occur during program/read/data retention by various reliability problems in the NAND flash memory. As a result, the data read from the NAND flash memory includes bit-errors. The bit-errors are corrected by the ECC decoder and the data without errors is read out.

Figure 6.9 summarizes the trend of the BCH code [59, 63]. From Fig. 6.9, two main results can be confirmed. First is that the reliability of the NAND flash memory degrades when the number of cell levels is increased from 1 bit/cell, 2 bits/cell, to 3 bits/cell (Note: The ECCs applied in the 1 bit/cell can correct only up to four bit-errors in the 512-byte codeword [59]). Second is that since the reliability of the NAND flash memory is degrading as a result of scaling, increasingly stronger BCH code is required to maintain the system reliability. When the reliability of the NAND flash memory becomes even worse, low-density parity-check (LDPC) codes are more suitable [63]. LDPC codes are extremely strong that the error correction capability is close to the theoretical limit [64]. Although LDPC codes are the

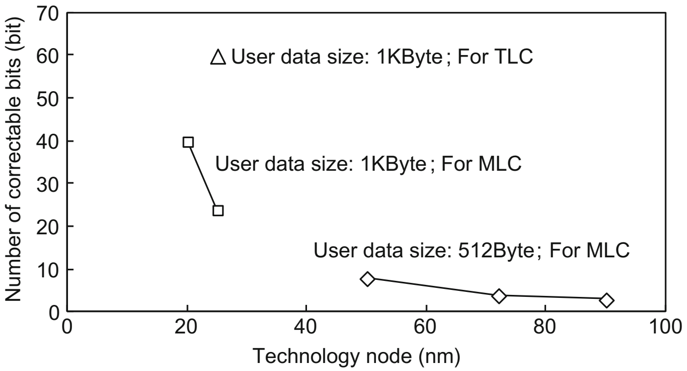


Fig. 6.9 Scaling trend of ECC strength [59, 63]

promising candidates of the ECCs for the scaled NAND flash memory, the requirement for the memory cell's precise threshold voltage information is a problem. This is because to extract threshold voltage from the memory cell, multiple sensing is required [63] and the read performance is significantly degraded. Works are trying to reduce the sensing trials to realize the practical use of the LDPC codes to the NAND flash memories [65, 66].

Although not always necessary, a technology called RAID can be applied to the NAND flash memory storage for further reliability enhancement. RAID, or redundant array of independent disks, was first proposed to enhance the reliability of storage system with multiple hard disk drives in granularities more coarse than ECCs [67]. The concept of RAID is completely compatible with NAND flash memory-based storage. For example, RAID-1 is a mirroring scheme that the data is duplicated in two (solid-state) disks. As a result, when there is an ECC failure in a disk, the data can be recovered from the other disk. There are mainly six levels of the RAID which have different performance, reliability, and storage overhead [67, 68]. Optimum RAID type is selected by considering the application, reliability, cost, and performance. SSD-specific RAID is also proposed (*Differential RAID*) which takes into account the reliability degradation during write/erase cycling [69]. By applying Differential RAID which can recover one disk failure, the write/erase cycles of the SSDs are intentionally graded to prevent errors in more than two disks. Note that the failure rate is strongly correlated to the write/erase cycles.

The preprocessing of the data is also effective to improve the reliability. Coding methods are proposed to reduce the cell-to-cell interference effect during programming [70, 71]. In [70], the cell-to-cell coupling is canceled by calculating least squares. In 3 bits/cell, constrained coding eliminates the data pattern that causes the consecutive highest–lowest–highest threshold voltage cells (highest cell-to-cell interference case) [71]. Asymmetric Coding and Stripe-Pattern Elimination Algorithm are also preprocessing techniques to reduce bit-error rate and maximum write current [72], which is further explained in Chap. 18.

6.3 In-Field Monitoring of Device Degradation for Predictive Maintenance

Yasuo SATO, Kyushu Institute of Technology

Seiji KAJIHARA, Kyushu Institute of Technology

6.3.1 Prognosis of Failures in Field

Preventing system failures due to decreasing delay margins is becoming a crucial issue, and device aging is known to be one of the major causes of such phenomena

[19, 73, 74]. As path delays in a circuit become longer by the aging, the delay margins which are differences between the path delays and the system clock cycle consequently decrease. Then, the possibility of failures becomes nonnegligible because the circuit with small delay margins is prone to cause logical failures even on small environmental variations (e.g., voltage instability, thermal-related delay increase, clock skew variation, etc.). Although many electronic safety-related systems require high reliability, it is becoming harder and harder to achieve it because of such aging-induced failures [75–77].

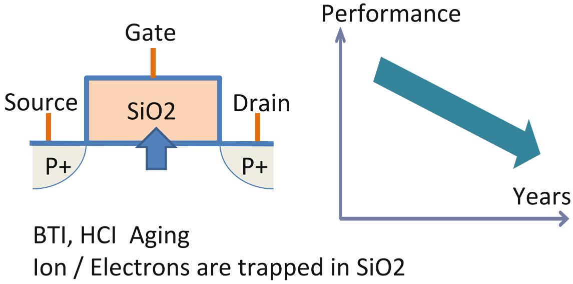
A very promising approach to tackle this issue is a prognostic method. We propose a novel technique that periodically measures the increases of the circuit delays and predicts future failures remaining enough time for maintenance [78, 79] (Sects. 5.3, 11.3, 12.3, Chap. 16). This preventive maintenance will drastically improve the system reliability. The proposed technique is based on a field test that enables accurate measurement of delay margins using BIST (Built-In Self-Test) concurrently monitoring temperature and voltage by ring-oscillator-based sensors [79] (Sect. 5.3). The BIST identifies the longest path delay of the circuit as the minimum test timing at which the test passes. The timing values are corrected to the ones on the standard temperature and voltage conditions, and such normalized values are able to provide the accurate information of decreasing delay margins. Furthermore, the values thus obtained are not affected by incidental factors such as temperature or supply voltage.

6.3.2 *Factors that Affect Delay Margins*

The trend in the latest VLSI design is that the delay margins are cut down to the minimum to obtain a faster operating speed in lower power and lower supply voltage as well as in increasing process variations [73]. Therefore, the increases of circuit delays due to device aging should be considered more carefully.

Several physical aging mechanisms such as BTI (Bias Temperature Instability), HCI (Hot Carrier Injection) or TDDB (Time-Dependent Dielectric Breakdown) threaten system reliability (Sect. 6.1). Physical aging phenomena such as BTI or HCI accumulate undesirable electrons in a gate oxide film, which result in consecutive performance degradations as time elapses (Fig. 6.10). In the case of NBTI

Fig. 6.10 Performance degradation caused by physical aging phenomena



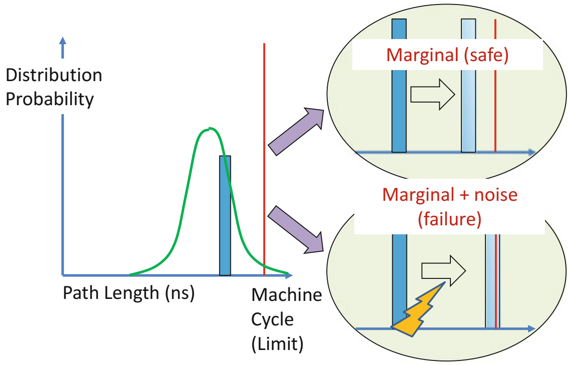


Fig. 6.11 Failure probability increase due to performance degradation

(Negative Bias Temperature Instability), which degrades PMOS transistor performance (or delay), the aging speed is rather fast at the early stage and becomes slower as time passes [19, 74]. Therefore, it can be a part of early failure causes as well as those of wear-out failures. This delay degradation will reduce the delay margin of each logic path in the circuit, and will increase the possibility of failures caused by a sudden voltage noise or an unexpected large temperature variation in the field (Fig. 6.11). These physical phenomena are hard to detect or quantify at the shipment stage. Therefore, a new approach that handles this problem in the field is strongly required.

6.3.3 Related Technologies to Overcome Delay Margin Problems

Currently, a variety of sensors are embedded in VLSIs to enable monitoring process variations, temperature variations, IR-drops, aging effects, or timing margins. The methods [80–84] make a measurement on a few typical paths or their replicas. As the degradation speed of each path on a chip differs according to its activation ratio [19, 74], these methods are not enough in regard to their coverage. The methods [85–89] measure the longest path delay using conventional test technologies, but temperature variations during test are not taken into consideration. As the temperature affects path delays quite directly, these methods cannot measure the delay degradation accurately.

Moreover, redundancy techniques such as TMR (Triple Modular Redundancy) [75–77] are hard to avoid the aging-induced failures. The TMR has been used for safety-related systems to detect and recover from errors on line. The redundancies work very well especially for random error events such as radiation-induced soft errors or electromagnetic-noise-induced errors by momentarily stopping the system in a safe state to avoid the worst situation. However, it is useless for what is known as “*common cause failures*”, which takes place in more than two subsystems at the

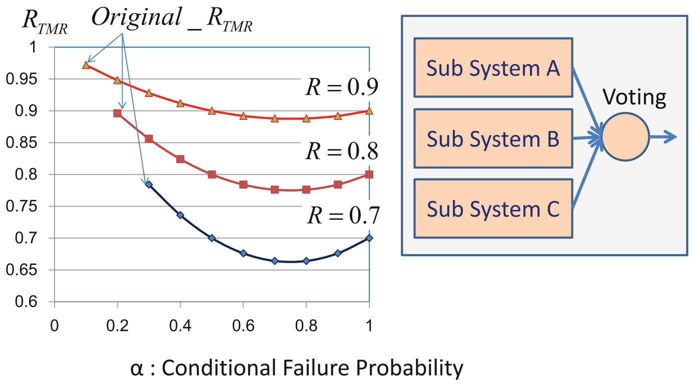


Fig. 6.12 Reliability variation of TMR affected by common cause failure [78]

same time due to the same root cause. In such case, the system is likely to produce wrong outputs. The aging-induced failures can be "*common cause failures*".

Figure 6.12 shows the reliability curves of the TMR considering the conditional probability α, which is the probability that two subsystems fail concurrently [90]. It demonstrates how the TMR's capability is limited in protection against the aging-induced delay failures. Therefore, an additional technique to compensate for this weakness is required.

6.3.4 Precise Monitoring of Delay Increase

The proposed method of precise circuit delay monitoring is part of the technology named DART (Dependable Architecture with Reliable Testing) [78] (Chap. 16). It consists of several techniques for measuring delay with high precision. Since the detailed application of DART will be discussed in Chap. 16 covering safety-related ASIC designs and FPGA designs, this subsection will begin by the background and focus on the precise delay measurement.

(1) Physical Aging Phenomena Considered

It should be noted that the delay margin decrease means the increase of path delays in a circuit. Figure 6.13 shows three types of physical aging phenomena classified by delay increase characteristics. Figure 6.13a shows a rapid increase of a path delay value, which might be due to an electromigration or a stress migration. The migration of substance in metallic conductors is an aging process that progresses very slowly, therefore, cannot be observed as an electric abnormality until it results in an abrupt short or open of metal interconnects. It can be detected by a periodical DC-level test. Figure 6.13b shows a rather slow increase of a delay value, which is focused on in this section. This type of delay increase can be detected by the

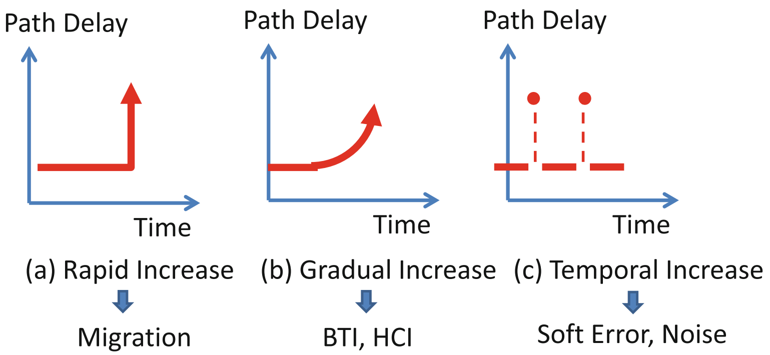


Fig. 6.13 Relation between physical aging phenomena

periodical and precise monitoring of delay increase that enables predictive maintenance. Although LSIs duration of uses differs from several years to 50 years depending on system applications, the amount of delay increase during the time should be controlled within the tolerable range. Figure 6.13c depicts a sudden temporal delay increase, which might happen due to a soft error or a transient noise. Redundancy system techniques such as ECC (Error Correction Codes), redundant flip-flops [91, 92], and TMR are available for these errors.

(2) Concept of Delay Measurement

Figure 6.14 illustrates the concept of delay measurement in DART. First, the minimum test timing at which the test passes is measured by BIST. Then, analysis will be done as follows. As the measured delay values could be affected by environmental noise or random noise such as temperature or voltage variations (Fig. 6.15), they are corrected to the ones on the standard temperature and voltage conditions. Here, temperature and voltage during delay measurement are monitored using the dedicated temperature and voltage sensors (TVMs) [79] (Sect. 5.3). The

Fig. 6.14 Concept of delay measurement in DART [78]

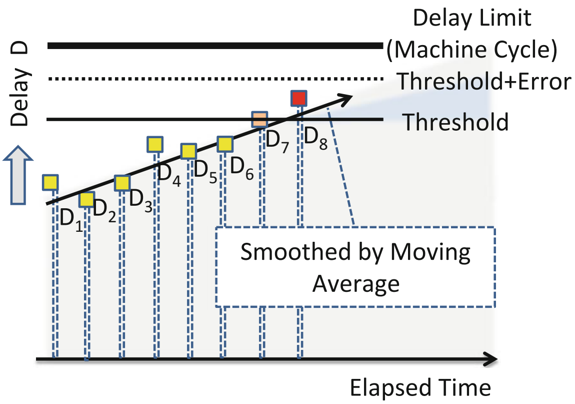
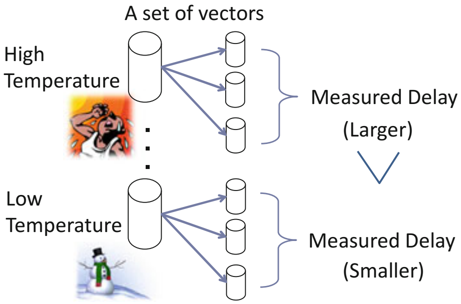


Fig. 6.15 Temperature effect on measured delay



effect of random measurement noise can be reduced using a statistical averaging method (i.e., moving average). Finally, an alarm will be sent to the system when the amount of degradation becomes beyond the threshold. The handling of the alarm depends on each individual system. For example, a board repair may follow the alarm during a planned outage time to minimize damages on the system. In another case, the system can be kept running with an increased power supply voltage, which will compensate for the delay degradation. The threshold of the path delay should be carefully determined considering measurement errors.

(3) Required Features for Implementation

The following features are required for the predictive maintenance.

- High Precision Delay Measurement

Measurement accuracy affects the precision of degradation analysis. The gap between the alarm threshold and the system operation limit has to be larger than the measurement error to avoid a false alarm. On the other hand, too large gap (i.e., too low threshold) will bring a too long time to a real error, which might make the method impractical

- Restrictions on Test Time and Resources

The measurement by BIST is performed in a nonoperational mode such as power-on/off time or dedicated test time of the system; therefore, the time required for the test has the minimum impact on the system. The size of the memory for test and logging need to be minimized as well (Sects. 11.3, 12.3).

- High Test Coverage

The aging may occur in any part of the chip. Therefore, the BIST needs to scan the system with high test coverage. In DART, a set of test vectors is applied in an assigned time (i.e., a test chance). A different set of test vectors is applied in the next test chance. With each set of test vectors with the maximized coverage, this sequence of test sets provides very high overall test coverage (Sect. 11.3).

Temperature and voltage monitors (TVMs) are embedded on a chip. They are placed in each clock domain or hot spots, where the temperature might be the

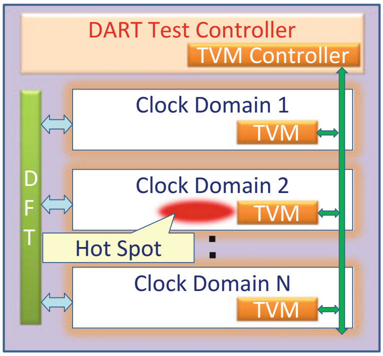


Fig. 6.16 Temperature and voltage monitors [78]

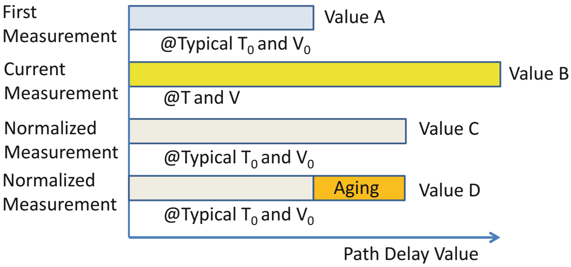


Fig. 6.17 Path delay value analysis

highest (Fig. 6.16). Their area granularity is determined depending on a trade-off between their area overhead and monitoring resolution. The monitored values are stored into a log memory such as an embedded flash memory or an off-chip non-volatile memory. The analysis of measured path delay values using temperature and voltage normalization is shown in Fig. 6.17. A is the measured value at the first time under a well-controlled environment of the typical temperature T_0 and voltage V_0. B is a current measured value at a temperature T and a voltage V, which are monitored by the TVMs. Then, B is corrected to the value (i.e., Value C) at T_0 and V_0 using the precalculated temperature and voltage characteristics by the circuit simulation (i.e., HSPICE). Comparing A and C, the difference is concluded as an amount of degradation.

6.3.5 *Aging Estimation in Field*

This subsection addresses characteristics of NBTI aging from a model view and from an experimental view using an FPGA device to confirm the slow delay increase shown in Sub-Section 4(1). Both results demonstrate the usefulness of the proposed prognostic technique [90, 93].

(1) Estimation using Models

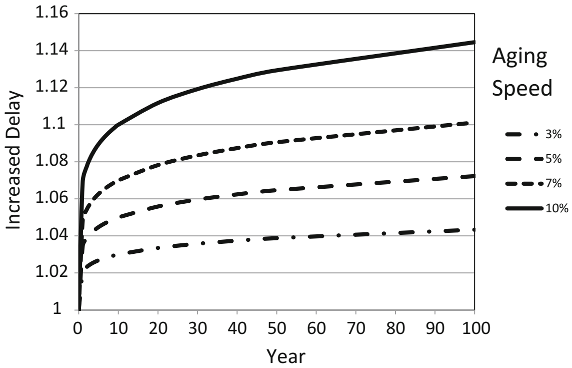
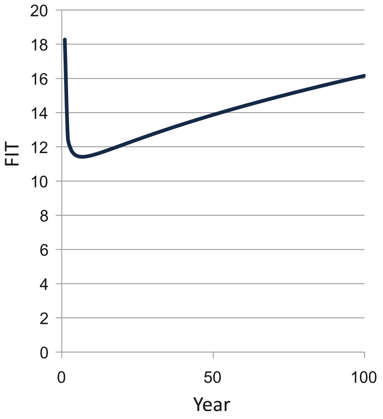


Fig. 6.18 Delay degradation estimation due to NBTI [90], Y-axis is the relative ratio of aged delay to the original delay

Two transistor-level aging models of NBTI are known, one is the reaction diffusion (RD) model [74] and the other is the trapping/de-trapping (TD) model [19]. Although there are some differences in physical behaviors, both models show almost the same speed of delay degradation. Figure 6.18 illustrates an estimation of path delay degradation using the RD model, where X-axis is the elapsed time and Y-axis is the normalized increased delay of the path. Four different aging speeds are plotted. For instance, the aging speed of 3% means a 3% increase in delay (i.e., degradation) in 10 years. This parameter should be easy to understand as severity because 10-year lifetime is adopted in many applications. The aging speed is known to be proportional to *n*th power of time *t*, where *n* is less than 1 (here, $n = 0.16$) [73]. As seen in the figure, a path delay increases rapidly at the early stage, then the speed becomes slower. In actual manufacturing, burn-in test or other substitute tests (e.g., faster-than-at-speed test) are applied to screen out the early-stage failures.

Figure 6.19 shows the failure rate of a circuit that corresponds to a chip-level delay degradation model [90] extracted from the transistor-level model. The failure



Process variation + margin=58%

Aging speed =8%

Fig. 6.19 Failure rate estimation due to NBTI [90]

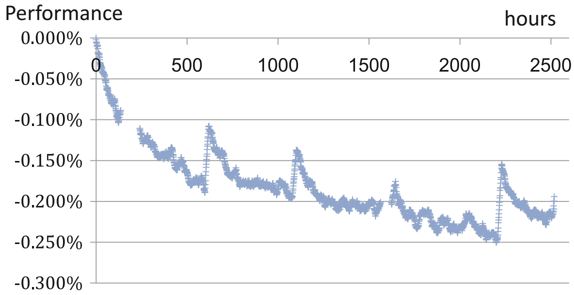


Fig. 6.20 Performance degradation measurement using a ring oscillator [93]

rate depends on the distribution of logic path lengths, design parameters such as delay margins, physical parameters, and process variation. Here, a typical delay distribution of 30% in process variation (i.e., 3σ), and 28% in delay margins were assumed. Therefore, the failure rate is kept at rather a low level. In the first 2 or 3 years, it shows a high failure rate (note: this is the target of the burn-in test), which corresponds to rapid delay increase in Fig. 6.18.

(2) Experiment on FPGA

An actual aging was measured using ring oscillators on an FPGA in Fig. 6.20 [93]. An Altera Cyclone IV chip (60 nm technology) was used for the experiment. Ring oscillators were placed on the chip, and heated in a constant temperature chamber. It was kept at 85° during the daytime (nearly 8 h each day), and was powered off at night for a safety reason. The frequencies of the oscillators were measured every minute while the chip was powered on. The ratio of the oscillator–frequency degradation was plotted against the accumulated powered-on time. It is rather fast at the early stage and gradually becomes slower as described in the literature [73, 74]. Some amount of degradation recovery was also observed during the powered-off times.

6.3.6 Conclusion

As discussed in this section, the conventional technologies are not good enough at preventing the failures due to the aging phenomena. A sudden system error or a sudden stop will have the big impacts on our society.

The proposed DART technology has the capability of reducing the failure rate in field. For instance, test sets of 80% coverage will reduce the failure rate to 20%. The application to a safety-related system is discussed in [78] and Chap. 16, wherein the hardware overhead is 0.2% of the total gates, the test time in each test chance is 200 ms, and the measurement error is within 27 ps.

6.4 A Reconfigurable SRAM Cache Design for Wide-Range Reliable Low-Voltage Operation

Masahiko Yoshimoto, Kobe University

Jinwook Jung, Kobe University,

Yuta Kimi, Kobe University,

Hiroshi Kawaguchi, Kobe University,

6.4.1 Variation- and Degradation-Tolerant SRAM Design

Feature sizes in transistors continue to shrink along with the advance of process technology, achieving higher density, higher performance, and lower cost. Technology scaling, however, makes transistors more vulnerable and sensitive to negative bias temperature instability (NBTI) which induces a significant fluctuation of transistor threshold voltage (V_{th}). Also the technology scaling induces a significant spread in transistor threshold voltage (V_{th}) mainly because of random dopant fluctuation (RDF), which has a deviation that is inversely proportional to the square of a channel area [94]. The above V_{th} variations strongly impact on reliability in deep sub-micron technology [95].

This situation yields serious problems particularly in SRAM because minimum sized transistors are used in its design.

The V_{th} variations make a minimum operating voltage (V_{min}) of SRAM rise, resulting in degradations of voltage fluctuation tolerance and bit-error-rate increase. To make matter worse, SRAMs occupy a substantial fraction of the total die area and transistor count in processors [96]. The V_{min} of the entire processor is determined by the circuit that has the highest V_{min}. Consequently, on-chip instruction cache and data cache, which is a large SRAM block, determine the V_{min} of the entire processor.

Here an associativity-reconfigurable cache using 7-Transistor/14-Transistor (7T/14T) SRAM cell [97] is described, which resolves the above issues and enhances the operating margin for marginal SRAM cells. The associativity-reconfigurable cache improves the V_{min} of the entire cache by trading off its associativity (the number of cache ways) and capacity. The cache can be reconfigured depending on the required degree of reliability and processor performance.

6.4.2 7T/14T Bit-Enhancing SRAM

The 7T/14T SRAM cell has a pair of conventional 6T SRAM bit cells. The internal nodes of the cell pair (N00 and N10, N01 and N11) are directly connected by two additional PMOS transistors (M20 and M21) as presented in Fig. 6.21. This structure provides an additional operating mode designated as the enhancing mode along with the normal mode.

Table 6.2 summarizes the operating modes of 7T/14T SRAM. In the normal mode, a one- bit datum is stored in one memory cell, which is more area efficient. In the enhancing read mode, only one word-line is asserted to gain a large β ratio (a ratio of two driver transistors' total size to one access transistor size). A memory cell with no static noise margin [98] is recovered by the other memory cell through the two additional PMOS transistors. In the enhancing write mode, both word-lines

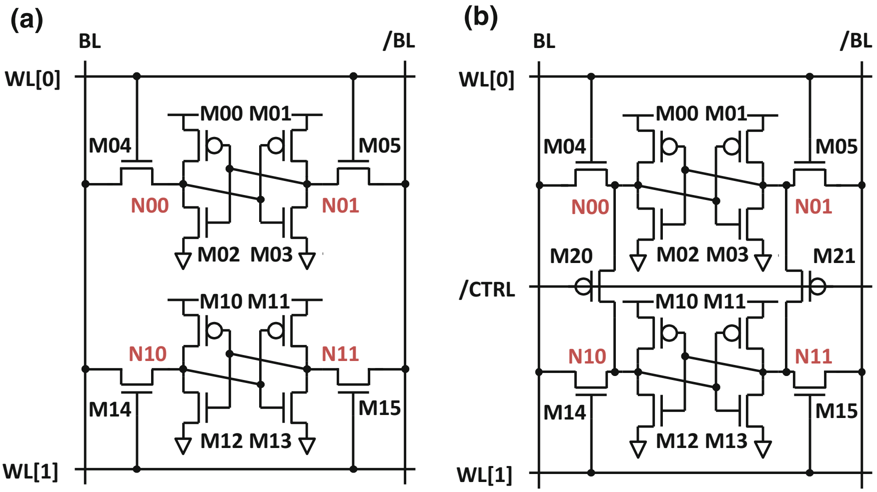


Fig. 6.21 Schematics of SRAM cell pairs. **a** Conventional 6T SRAM and **b** 7T/14T bit-enhancing SRAM

Table 6.2 Two modes of 7T/14T bit-enhancing SRAM

Mode	# of memory cells comprising 1 bit	# of WL drivers	CTRL
Normal	1 (7 transistors/ bit)	1	Off ("H")
Enhancing (write)	2 (14 transistors/ bit)	2	On ("L")
Enhancing (read)	2 (14 transistors/ bit)	1	On ("L")

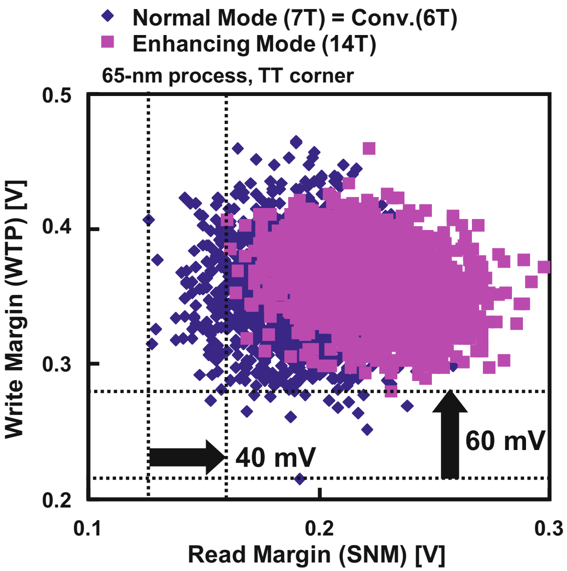


Fig. 6.22 Static noise margins (SNMs) and write trip points (WTPs) of conventional 6T SRAM, 7T/14T bit-enhancing SRAM in the normal mode and in the enhancing mode

are asserted to write into a pair of memory cells. The write margin degradation is averaged and mitigated.

The two operating modes of 7T/14T SRAM can be switched according to the required operating margin. This mode transition of 7T/14T SRAM can be conducted by appropriate control of CTRL line in Fig. 6.21 without rebooting the entire system.

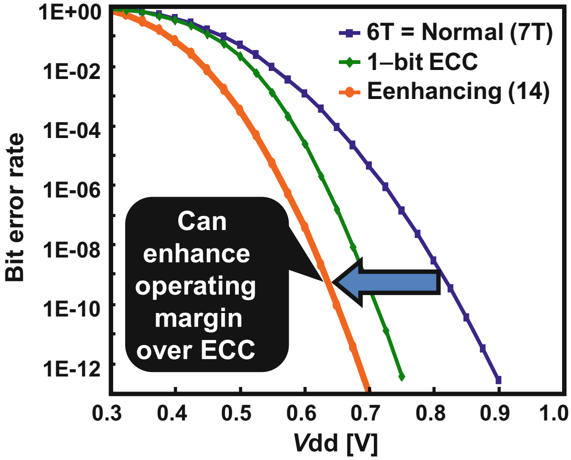
Figure 6.22 shows read margins and write margins of conventional 6T SRAM and 7T/14T SRAM. The read margins are evaluated by static noise margins (SNMs) and the write margins are evaluated by write trip points (WTPs) [98, 99]. The number of Monte Carlo simulation samples is 2,000. The 7T/14T SRAM cell in the enhancing mode achieves large SNM and WTP by 40 mV and 60 mV, respectively, compared with the conventional 6T SRAM.

Figure 6.23 shows bit-error rates in 7T/14T SRAM and in the other scheme. In enhancing mode, the 7T/14T SRAM features reliable operations especially at low voltages by combining two bit cells and is lower in bit-error rate than the conventional 6T SRAM with error correction code (ECC).

6.4.3 Associativity-Reconfigurable Cache

In the associativity-reconfigurable cache which we propose here, consecutive odd–even cache ways are paired up by exploiting the structure of the 7T/14T SRAM cell. Switching modes in 7T/14T SRAM is conducted with respect to these way pairs. Two ways in a way pair are combined with the enhancing mode and form one

Fig. 6.23 Bit error rates: 6T SRAM, 6T SRAM with 1-bit ECC and 7T/14T bit-enhancing SRAM in the normal mode and in the enhancing mode



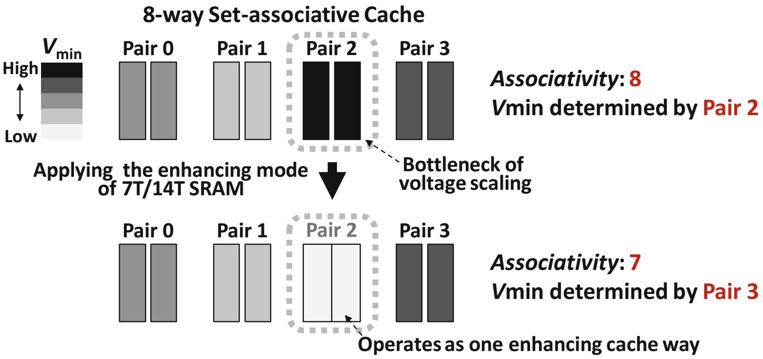

8-way Set-associative Cache
Vmin
High
Low
Pair 0
Pair 1
Pair 2
Pair 3
Associativity: 8
Vmin determined by Pair 2
Bottleneck of voltage scaling
Applying the enhancing mode of 7T/14T SRAM
Pair 0
Pair 1
Pair 2
Pair 3
Associativity: 7
Vmin determined by Pair 3
Operates as one enhancing cache way

Fig. 6.24 Conceptual view of the V_{min} reduction by the associativity-reconfigurable cache

enhancing way. Although the associativity of the cache is decreased by one, V_{min} of the way pair is improved. Therefore, the associativity of the proposed N-way set-associative cache can be chosen between $N/2$ and N achieving the desired V_{min} for end performance.

Figure 6.24 shows the cache V_{min} reduction mechanism of the associativity-reconfigurable cache. The cache V_{min} reduction is achieved by application of the enhancing mode of 7T/14T SRAM to the way pair with the highest value of V_{min}. If all the way pairs enter the enhancing mode, the associativity-reconfigurable cache can fully exploit the margin enhancement feature of 7T/14T SRAM, resulting in the lowest value of the V_{min}.

The ways in a pair operate independently in the normal mode, is shown in Fig. 6.25. Figure 6.26 illustrates the case that pair 0 operates in the enhancing mode. Odd–even ways in the pair are logically bound together and constitute the

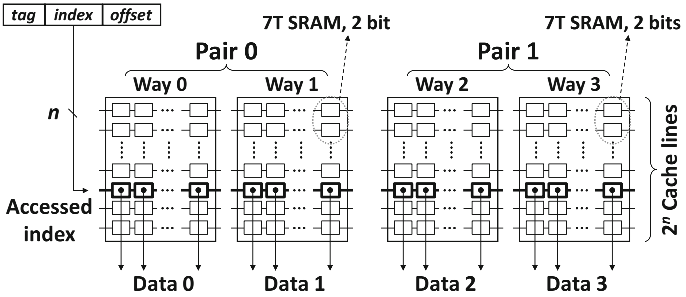


Fig. 6.25 The associativity-reconfigurable cache organization when all way pairs operate in the normal mode

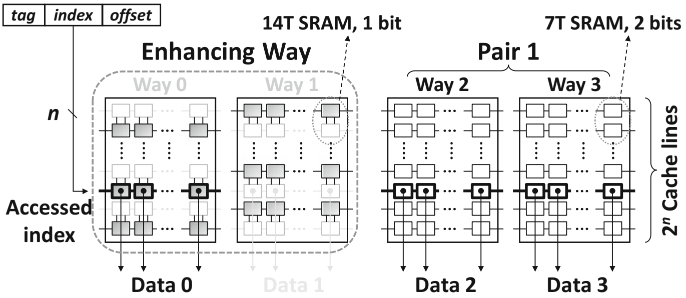


Fig. 6.26 The associativity-reconfigurable cache organization when pair 0 operates in the enhancing mode

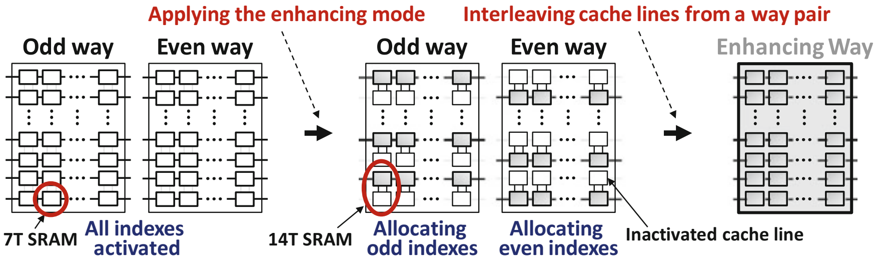


Fig. 6.27 Logical allocation of cache lines in the enhancing way

enhancing cache way that features enhanced operating margin, thereby allowing more reliable operation.

The way switched to the enhancing mode has only half index and the capacity is halved because one-bit data is made up of a pair of memory cells (14T). To comprise the enhancing way which has a complete index, the two ways in the way pair is combined by interleaving odd–even cache lines, as shown in Fig. 6.27. The

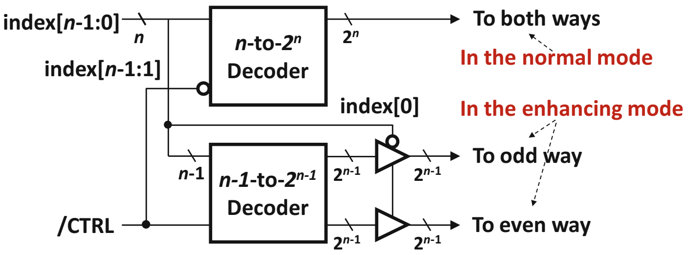


Fig. 6.28 Implementation of cache decoders

odd (even) indexed cache lines in the odd (even) way are allocated to the odd (even) indexes of the enhancing way. The even (odd)-indexed cache lines in the odd (even) way are inactivated. The enhancing way has complete indexes with this allocation.

Decoders of the associativity-reconfigurable cache are extended to realize interleaving allocation in an enhancing way. The extended decoder comprises an n-to-2^n decoder and an $(n-1)$-to-2^{n-1} decoder (n is a bit width of the cache index) is shown in Fig. 6.28. In the normal mode, the n-to-2^n decoder is activated and drives each cache way independently. In the enhancing mode, the $(n-1)$-to-2^{n-1} decoder is activated. The decoder of the enhanced way drives the even indexed cache lines in the even way and the odd indexed cache lines in the odd way.

In the associativity-reconfigurable cache, the tag array is also implemented with 7T/14T SRAM. The same organization explained above is applied to the tag array.

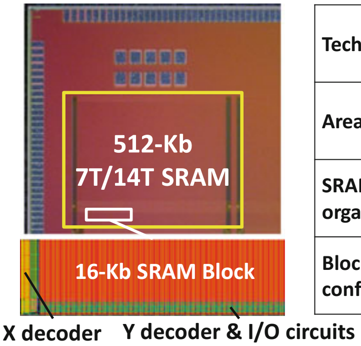
6.4.4 Experimental Result

We describe our experimental evaluations of the associativity-reconfigurable cache. The cache system configuration is presented in Table 6.3.

The minimum operating voltage (V_{min}) improvement is evaluated based on measurement of a 512-Kb 7T/14T SRAM macro manufactured 65-nm CMOS technology (Fig. 6.29). We also analyze impacts on the processor's overall performance enabled by the reconfiguration of associativity.

Table 6.3 Cache system configuration

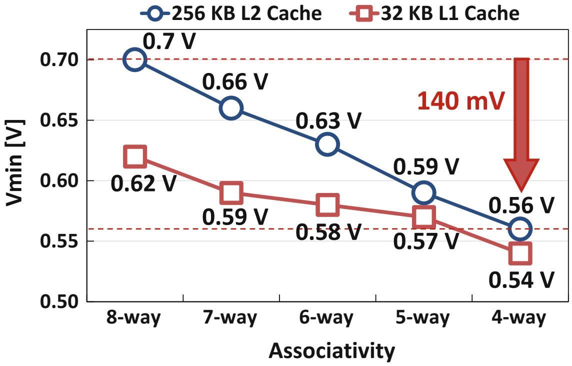
Level 1 cache	32-KB 8-way set-associative cache (with 2.75 KB tag array)
Level 2 cache	256-KB 8-way set-associative cache (with 19 KB tag array)



Technology	65-nm CMOS 12 metal layers
Area	2.04 mm^2 (1260 um × 1620 um)
SRAM organization	16-Kb block × 32 (= 512 Kb)
Block configuration	128 rows × 8 columns × 16 bits/word

Fig. 6.29 512-KB 7T/14T SRAM die photograph and 16-KB block layout

Fig. 6.30 Measured $V_{\min}$ s of the associativity-reconfigurable caches in 256 KB and 32 KB cache with respect to each operating associativity



6.4.4.1 Minimum Operating Voltage ($V_{\min}$) Evaluation

Figure 6.30 presents the $V_{\min}$ of the associativity-reconfigurable cache with respect to each operating associativity. The $V_{\min}$ can be scaled by trading off the associativity. If all 4-way pairs enter the enhancing mode, then the associativity-reconfigurable cache can operate as a 4-way 128-KB cache at 0.56 V, achieving a 140 mV lower $V_{\min}$ than the 8-way 256-KB in the normal mode. Applying the enhancing mode in one way pair reduces $V_{\min}$ by 30–40 mV. Similarly, 32-KB L1 cache is scaled by trading off the associativity.

6.4.4.2 Processor Performance Evaluation

Decreasing associativity affects a cache hit rate and, therefore, the processor performance. To evaluate the impacts on the processor's overall performance, we conducted processor simulations using the associativity-reconfigurable cache architecture with respect to various L2 cache configurations. Gem5 simulator [100]

Table 6.4 Baseline processor configuration

Parameter	Value
Processor frequency	1 GHz
L1 instruction/data cache	32 KB, 8-way, 32-byte line, 3-cycle access time
Unified L2 Cache	256 KB, 8-way, 32-byte lines, 10-cycle access time
Cache Replacement Policy	LRU
External DRAM latency	100 cycles

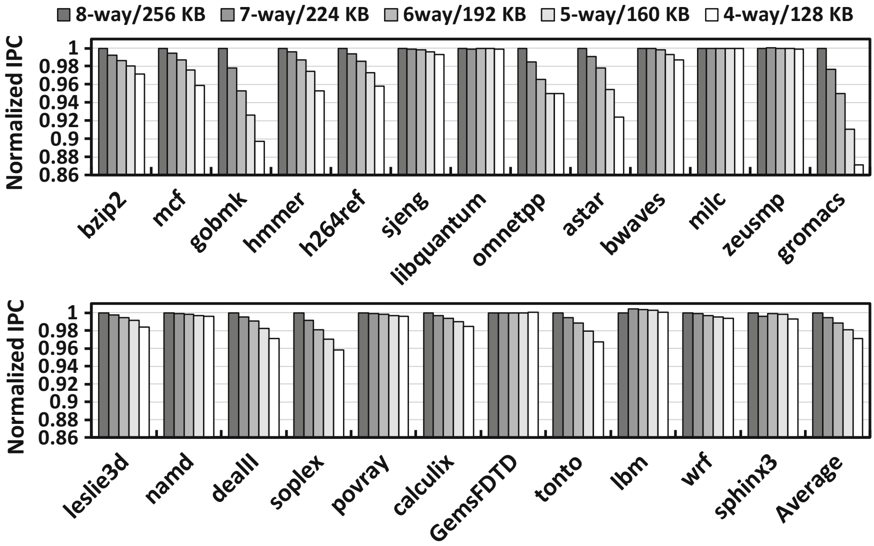


Fig. 6.31 Normalized IPCs of SPEC2006 benchmarks with respect to each associativity

was utilized and benchmarks from SPEC 2006 [101] were chosen. Table 6.4 shows baseline processor configuration assumed in the simulation. We chose instructions per cycle (IPC) as the index of the processor performance.

Figure 6.31 shows normalized instructions per cycle (IPCs) for each benchmark. The IPC degradation is 0.72% on average when the enhancing mode is applied to a single way pair and the cache associativity decreases by one. The average IPC degradation is 2.95% in the 128-KB 4-way L2 cache (in the case in which all the pairs operate in the enhancing mode).

6.4.5 Conclusions

We describe an adaptive cache design for wide-range reliable low-voltage operation as the associativity-reconfigurable cache. The associativity-reconfigurable cache possesses the scalable characteristic of operating margin and it can decrease the $V_{\min}$ by 140 mV. The processor simulation shows that applying the associativity-reconfigurable architecture results in 2.95% maximum IPC loss but it can choose various performance levels. The associativity-reconfigurable cache can be reconfigured depending on the required degree of reliability and processor performance and is useful to mitigate possible effects of device degradation.

6.5 Runtime Self-reconstruction for Tolerating Software/ Hardware Faults Increment from Aging

Hajime Shimada, Nagoya University

Jun Yao, Nara Institute of Science and Technology

6.5.1 Background

In this section, we introduce runtime self-reconstruction idea to tolerate multiple soft/hard fault in single processor. This idea is effective to tolerate soft/hard fault comes from aging, because the processor can decouple damaged units and incorporate healthy unit to keep modular status to tolerate next faults.

As an adverse side effects of semiconductor process technology advancement, threats to the system's dependability from soft errors due to noises and radiations, and hard errors due to NBTI and electromigration have increased dramatically. Past dependable processor utilizes DMR and TMR organization to tolerate single-event soft errors as well as hard errors. But in the future process technology, cumulative multiple soft and hard errors may occur in a single processor. Traditional DMR and TMR would not be able to accommodate errors of such nature. To mitigate this problem, an architecture that we call runtime self-reconstruction has been proposed [102]. The idea utilizes modular- and quick recover-aimed processor cores. It tolerates multiple soft errors by a quick recovery, and multiple hard errors by decoupling a faulty processor core and incorporating a healthy core, respectively. The rest of this section will be used to describe the details of the architecture and operation of runtime self-reconstruction.

6.5.2 Tolerating Soft/Hard Faults with Runtime Self-reconstruction

6.5.2.1 Concept

Most of the conventional methods mentioned in the last section only tolerate a few kinds of single-event soft errors and one type of permanent error, so we thought that they cannot sustain enough reliability under future ultimately scaled semiconductor process technology. To alleviate this problem, DARA (Dynamic Adaptive redundant Architecture), a processor architecture we propose, utilizes quick error detection and runtime self-reconstruction. DARA can apply recover operation before the processor fails by cumulating multiple soft errors. Also, DARA can alleviate multiple hard errors by cutting off a failed core after a permanent error has been detected and adding a healthy core. Furthermore, by utilizing runtime self-reconstruction effectively, DARA can self-reconfigure from TMR into DMR execution keeping precise processor status after a permanent error has been detected. This feature gives average power consumption reduction, restraining degradation of spare resources by hot standby (e.g., NBTI), and reducing resources for dependability by sharing spare resources under multicore organization.

Figure 6.32 shows the concept of DARA and Fig. 6.33 shows the outline of the pipeline-stage-level modular execution by carving out a part of the pipeline stage. DARA employs multicore organization designed with multiple modular redundancy configurations in mind. Each core is equipped with the following functions:

- Comparator for error detection
- Inter-core communication path connected to the comparator for modular execution
- Error recovery administrator which summarizes discord result from the comparator
- Partial register value protection by parity for precise processor status under dynamic DMR to TMR expansion.

In the current implementation, we utilized 6-stage pipeline stage organization which consists of instruction fetch (IF), instruction decode (ID), register read (RR),

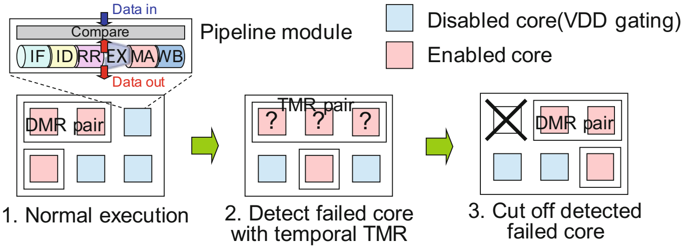


Fig. 6.32 DARA processor core and self-reconstruction

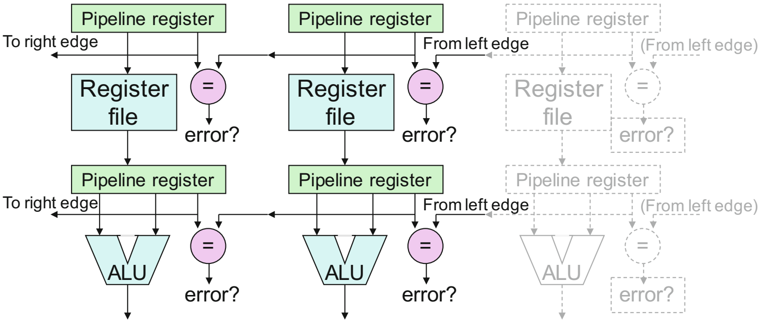


Fig. 6.33 Modular status and error detection in each stage

execution (EX), memory access (MA), and write back (WB). By parallelizing this processor core, we can organize DMR/TMR organization. The processor core can operate alone if we do not require high reliability. We have to accord some area overhead coming from the additional circuit for comparing the processor core without reliability. Note that parities which are added to some registers improve reliability even if the processor core operates alone.

6.5.2.2 DMR Operation

By combining two processor cores described in the previous section, we can achieve DMR organization. Blocks and buses delineated in solid lines in Fig. 6.33 show active part in DMR organization. Outputs of each stage are once stored in pipeline register, and compared to the next clock cycle. The comparator and re-execution controller are built-in individual cores, being duplicated as well. So, DARA can continue correct operation even if error (especially permanent error like stack-at-0 fault) has occurred in those parts.

Recovery from a detected error is done like recovery from branch misprediction. The processor sends Program Counter value which is existing beside the instruction in error-detected stage to the Program Counter register of IF stage. After that, the processor restarts with instruction fetch from failed instruction. Under this procedure, there is a possibility that another error takes place. To treat this problem, we keep precise status before re-execution has started in the pipeline and realize “re-execution of re-execution procedure” in DARA. In case of re-execution of the instruction which updates multiple register value, we cannot achieve precise re-execution with above simple re-execution if the instruction updates a part of register values. Let us consider the instruction which increments base register value after memory read as an example. Generally, memory read requires a longer time than a register value increment so that the order of the register value update becomes “base register update” and “store memory read result” order. In this case, if an error occurs under memory read, the base register value has already updated so that the processor status becomes wrong if the processor updates the base register value again. To resolve this problem, we introduced instruction decomposition and sub Program Counter value to achieve individual recover operation. Above instruction is decomposed into memory read sub instruction and base register value increment sub-instruction by this scheme and achieve recover operation from individual sub Program Counter value allocated to individual sub instructions.

6.5.2.3 DTMR Operation

DARA allows dynamic DMR to TMR expansion so that DARA can migrate into TMR mode to alleviate permanent error by adding one processor core after an error has been detected under DMR mode. We call counter permanent error organization based on above idea as DARA-DTMR organization.

When a permanent error has occurred in DMR mode shown in the previous section, the permanent error has been observed as a series of soft errors that occur too frequently. In this case, first, DARA attaches one processor core which has a copy of the correct processor status and configures a TMR organization (add dotted line part in Fig. 6.33). Then, DARA starts re-execution and identifies healthy cores that output the same result. The left one core is treated as a broken core and is detached as broken so that the system migrates into DMR mode again (Fig. 6.32). This TMR mode migration requires several hundreds of cycles because it requires healthy register value transmission to the attached core. On the other hand, detaching a broken core only requires several cycles including one instruction re-execution for the broken core detection because it does not require data transmission. It only requires identification of the DMR pair which DARA still utilize.

In DTMR organization, DARA does not supply power to the third core until a permanent error has been detected. By this characteristic, DARA can reduce average power consumption, subdue degradation (due, e.g., to NBTI) of spare resources by shutting down the power supply, and sharing the spare resources in multicore operation. Note that if we cannot tolerate overhead under DMR to TMR expansion (e.g., real-time applications), we can choose full-time TMR operation in DARA. DARA does not require OS support under re-execution and reconstruction procedure. So, we (or OS) only indicate required dependability (e.g., DMR, DTMR, full-time TMR, etc.) by the configuration of the special register value.

6.5.3 Evaluation and Discussion

6.5.3.1 Circuit Area

DARA contains a comparator and an additional data path in each processor core module so that it gives additional area overhead. To evaluate this overhead, we implemented DARA with Hitachi/Renesas SH-2 instruction set. The design is synthesized by Synopsis Design Compiler and Rohm 180 nm logic cell library to evaluate the area. In this implementation, we implement low-capacity L1 cache to the module itself and implement ECC to register file and caches to keep precise value.

If we assume the area of a no-counter error processor core to be 100%, the area of a core in DARA is 135%, DMR organization 217%, and TMR organization 298%, respectively. The reason that that DMR/TMR organization does not become an integral multiple of the one core of DARA comes from the area of L1 cache which is not modular because it is covered with ECC and multi-porting. Because of ECC-covered cache and registers, 61% of the circuit is covered from errors. We cannot achieve 100% cover rate because we could not eliminate stack-at-0 fault to the circuits which indicate re-execution. The DARA-DTMR organization uses TMR upon permanent error detection. So, if we assume that the power consumption increases in proportion to the area, DARA-DTMR can tolerate permanent error with 72% power consumption of the traditional TMR organization.

6.5.3.2 Error Tolerance Under Alpha Particle Irradiation

To evaluate high-frequency soft error, we executed each benchmark of Stanford Benchmark Suite for 1000 times under 1.25 V supply voltage and alpha particle irradiation from Am241/3Mq alpha particle source (Fig. 6.34). Figure 6.35 shows the number of execution cycles including re-execution operation. The horizontal axis shows benchmarks, the line chart (with right axis) shows average and distribution of execution cycles, and the bar chart shows the average and distribution of number of re-execution operation. The re-execution operation occurs 0.34 per second in average. Due to architectural vulnerability factor (AVF) difference

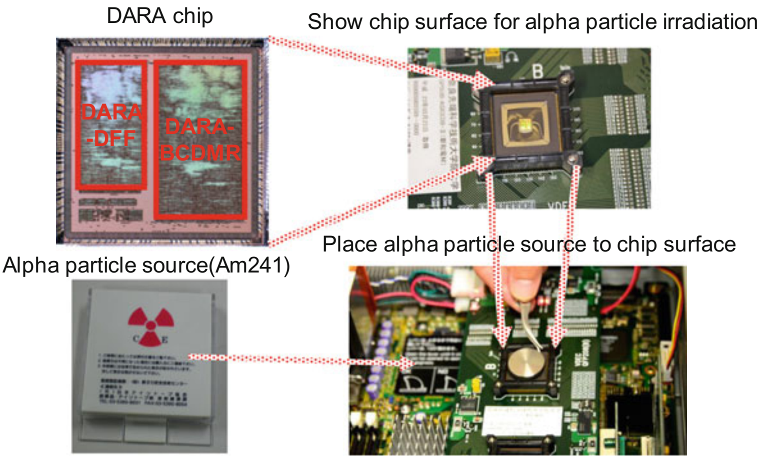

DARA chip
Show chip surface for alpha particle irradiation
DARA -DFF
DARA-BCDMR
Alpha particle source(Am241)
Place alpha particle source to chip surface

Fig. 6.34 Manufactured DARA chip and alpha particle irradiation environment

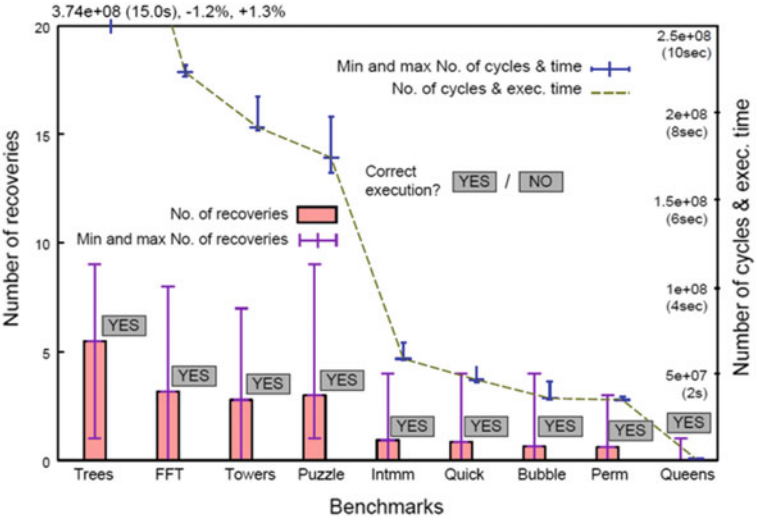


Fig. 6.35 Execution cycles and number of re-execution under alpha particle irradiation

between benchmark programs, the frequencies of errors differ between benchmark programs. Typically, AVF comes from instruction mix of the benchmark program and we found that the Puzzle benchmark contains comparatively many vulnerable instructions. AVF also affects re-execution operation so that the distribution of the execution cycle differs between benchmark programs that have similar error rates and average execution cycles.

6.5.4 Conclusion

Under the concept that utilizes self-reconstruction to tolerate soft error and permanent error, we have proposed DARA architecture and evaluated it with trial manufacturing and alpha particle irradiation. The results show that DARA-DMR organization works correctly under high soft error rate environment. There are several processor levels or ALU level DMR or TMR implementation. But DARA gives further cost-effectiveness and dependability by dynamically reconstructing its organization under required dependability and given resources.

References

1. R. Degraeve, G. Groeseneken, R. Bellens, J.L. Ogier, M. Depas, P.J. Roussel, H.E. Maes, New insights in the relation between electron trap generation and the statistical properties of oxide breakdown. IEEE Trans. Electron Devices **45**(4), 904–911 (1998)
2. B. Kaczer, R. Degraeve, M. Rasras, K.V. de Mieroop, P.J. Roussel, G. Groeseneken, Impact of MOSFET gate oxide breakdown on digital circuit operation and reliability. IEEE Trans. Electron Devices **49**(3), 500–506 (2002)
3. M. Depas, T. Nigam, M.M Heyns, Soft breakdown of ultra-thin gate oxide layers. IEEE Trans. Electron Devices **43**(9), 1499–1504 (1996)
4. K. Okada, Extended time dependent dielectric breakdown model based on anomalous gate area dependence of lifetime in ultra think silicon dioxides. Japan. J. Appl. Phys. **36**(3B), 1443–1447 (1997)
5. A. Popa, An injection level dependent theory of the MOS transistor in saturation. IEEE Trans. Electron Devices **19**(6), 774–781 (1972)
6. P.E. Cottrell, R.R. Troutman, T.H. Ning, Hot-electron emission in n-channel IGFET's. IEEE Trans. Electron Devices **26**(4), 520–533 (1979)
7. C. Hu, Lucky-electron model of channel hot electron emission. IEDM Tech. Dig. **25**, 22–25 (1979)
8. S. Mahapatra, C. Parikh, V. Rao, C.R. Viswanathan, J. Vasi, Device scaling effects on hot-carrier induced interface and oxide-trapped charge distributions in MOSFET's. IEEE Trans. Electron Device **47**(4), 789–796 (2000)
9. J.H. Stathis, S. Zafar, The negative bias temperature instability in MOS devices. Rev. Microelectron. Reliab. **46**(2–4), 270–286 (2006)
10. S.E. Rauch, Review and reexamination of reliability effects related to NBTI-induced statistical variations. IEEE Trans. Device Mater. Reliab. **7**(4), 524–529 (2007)
11. T. Grasser, B. Kaczer, W. Goes, An energy-level perspective of bias temperature instability, in *Proceedings of International Reliability Physics Symposium* (*IRPS*) (April 2008), pp. 28–38
12. P.B. Ghate, Electromigration-induced failures in VLSI interconnects, in *Annual Reliability Physics Symposium* (IEEE, 1982), pp. 292–299
13. D. Pierce, P. Brusius, Reliability physics of advanced electron devices electromigration. Rev. Microelectron. Reliab. **37**(7), 1053–1072 (1997)
14. J.R. Black, Electromigration failure modes in aluminum metallization for semiconductor devices. Proc. IEEE **57**(9), 1587–1594 (1969)
15. J. Yue, W. Funsten, R. Taylor, Stress induced voids in aluminum interconnects during IC processing, in *Annual Reliability Physics Symposium* (IEEE, 1985), pp. 126–137
16. T.H. Kim, R. Persaud, C.H. Kim, Silicon odometer: an on-chip reliability monitor for measuring frequency degradation of digital circuits. IEEE J. Solid-State Circ. **43**(4), 874–880 (2008)
17. T. Sato, T. Kozaki, T. Uezono, H. Tsutsui, H. Ochi, A device array for efficient bias-temperature instability measurements, in *Proceedings of European Solid-State Device Research Conference* (*ESSDERC*) (2011), pp. 143–146
18. H. Awano, M. Hiromoto, T. Sato, BTIarray: a time-overlapping transistor array for efficient statistical characterization of bias temperature instability. IEEE Trans. Device Mater. Reliab. **14**(3), 833–843 (2014)
19. J.B. Velamala, K.B. Sutaria, T. Sato, Y. Cao, Physics matters: statistical aging prediction under trapping/detrapping, in *Proceedings of ACM/IEEE Design Automation Conference* (*DAC*) (June 2012), pp. 139–144
20. P. Singh, E. Karl, D. Sylvester, D. Blaauw, Dynamic NBTI management using a 45 nm multi-degradation sensor, in *IEEE Custom Integrated Circuits Conference* (Sept 2010), pp. 1–4

21. P.F. Lu, K.A. Jenkins, A built-in BTI monitor for long-term data collection in IBM microprocessors, in *Proceedings of International Reliability Physics Symposium* (*IRPS*) (Apr 2013), pp. 4A.1.1–4A.1.6
22. H. Fuketa, M. Hashimoto, Y. Mitsuyama, T. Onoye, Adaptive performance compensation with in-situ timing error predictive sensors for subthreshold circuits. IEEE Trans. Very Large Scale Integr. VLSI Syst. **20**(2), 333–343 (2012)
23. S. Iizuka, M. Mizuno, D. Kuroda, M. Hashimoto, T. Onoye, Stochastic error rate estimation for adaptive speed control with field delay testing, in *IEEE International Conference on Computer Aided Design* (Nov 2013), pp. 107–114
24. F. Masuoka et al., A new flash E^2PROM cell using triple polysilicon technology, in *IEEE International Electron Devices Meeting* (*IEDM*) (1984), pp. 465–467
25. F. Masuoka et al., New ultra high density EPROM and flash EEPROM with NAND structure cell, in *IEEE International Electron Devices Meeting* (*IEDM*) (1987), pp. 552–555
26. F. Masuoka, Great encounters leading me to the inventions of flash memories and surrounding gate transistor technology. IEEE Solid-State Circ. Mag. 10–20 (2013)
27. S. Aritome, NAND flash innovations. IEEE Solid-State Circ. Mag. 21–29 (2013)
28. M. Bauer et al., A multilevel-cell 32 Mb flash memory, in *IEEE International Solid-State Circuits Conference* (*ISSCC*) (1995), 132–133
29. K. Takeuchi et al., A 56 nm CMOS 99 mm^2 8 Gb Multi-level NAND flash memory with 10 MB/s program throughput, in *IEEE International Solid-State Circuits Conference* (*ISSCC*) (2006), pp. 144–145
30. R. Cernea et al., A 34 MB/s-program-throughput 16 Gb MLC NAND with all-bitline architecture in 56 nm, in *IEEE International Solid-State Circuits Conference* (*ISSCC*) (2008), pp. 420–421
31. R. Zeng et al., A 172 mm^2 32 Gb MLC NAND flash memory in 34 nm CMOS, in *IEEE International Solid-State Circuits Conference* (*ISSCC*) (2009), pp. 236–237
32. H. Kim et al., A 159 mm^2 32 nm 32 Gb MLC NAND-flash memory with 200 MB/s asynchronous DDR interface, in *IEEE International Solid-State Circuits Conference* (*ISSCC*) (2010), pp. 442–443
33. C. Lee et al., A 32 Gb MLC NAND-flash memory with Vth-endurance-enhancing schemes in 32 nm CMOS, in *IEEE International Solid-State Circuits Conference* (*ISSCC*) (2010), pp. 446–447
34. K. Fukuda et al., A 151 mm^2 64 Gb MLC NAND flash memory in 24 nm CMOS technology, in *IEEE International Solid-State Circuits Conference* (*ISSCC*) (2011), pp. 198–199
35. T.-Y. Kim et al., A 32 Gb MLC NAND flash memory with Vth margin-expanding schemes in 26 nm CMOS, in *IEEE International Solid-State Circuits Conference* (*ISSCC*) (2011), pp. 202–203
36. N. Shibata et al., A 19 nm 112.8 mm^2 64 Gb multi-level flash memory with 400 Mb/s/pin 1.8 V toggle mode interface, in *IEEE International Solid-State Circuits Conference* (*ISSCC)* (2012), pp. 422–423
37. M. Helm et al., A 128 Gb MLC NAND-flash device using 16 nm planar cell, in *IEEE International Solid-State Circuits Conference* (*ISSCC*) (2014), pp. 326–327
38. S. Choi et al., A 93.4 mm^2 64 Gb MLC NAND-flash memory with 16 nm CMOS technology, in *IEEE International Solid-State Circuits Conference* (*ISSCC*) (2014), pp. 328–329
39. Y. Li et al., A 16 Gb 3b/cell NAND flash memory in 56 nm with 8 MB/s write rate, in *IEEE International Solid-State Circuits Conference* (*ISSCC*) (2008), pp. 506–507
40. S.-H. Chang et al., A 48 nm 32 Gb 8-Level NAND flash memory with 5.5 MB/s program throughput, in *IEEE International Solid-State Circuits Conference* (*ISSCC*) (2009), pp. 240–241
41. G.G. Marotta et al., A 3 bit/cell 322 Gb NAND flash memory at 34 nm with 6 MB/s program throughput and with dynamic 2 bit/cell blocks configuration mode for a program

throughput increase up to 13 MB/s, in *IEEE International Solid-State Circuits Conference* (*ISSCC*) (2010), pp. 444–445

42. Y. Li et al., 128 Gb 3 bit/cell NAND flash memory in 19 nm technology with 18 MB/s write rate and 400 Mb/s toggle mode, in *IEEE International Solid-State Circuits Conference* (*ISSCC*) (2012), pp. 436–437
43. G. Naso et al., A 128 Gb 3b/cell NAND flash design using 20 nm planar-cell technology, in *IEEE International Solid-State Circuits Conference* (*ISSCC*) (2013), pp. 218–219
44. K. Kanda et al., A 120 mm^2 16 Gb 4-MLC NAND flash memory with 43 nm CMOS technology, in *IEEE International Solid-State Circuits Conference* (*ISSCC*) (2008), pp. 430–431
45. C. Trinh et al., A 5.6 MB/s 64 Gb 4b/cell NAND flash memory in 43 nm CMOS, in *IEEE International Solid-State Circuits Conference* (*ISSCC*) (2009), pp. 246–247
46. D. Nobunaga et al., A 50 nm 8 Gb NAND flash memory with 100 MB/s program throughput and 200 MB/s DDR interface, in *IEEE International Solid-State Circuits Conference* (*ISSCC*) (2008), pp. 426–427
47. http://www.itrs.net/home.html
48. K.-T. Park et al., Three-dimensional 128 Gb MLC vertical NAND flash-memory with 24-WL stacked layers and 50 MB/s high-speed programming, in *IEEE International Solid-State Circuits Conference* (*ISSCC*) (2014), pp. 334–335
49. K. Takeuchi et al., A multipage cell architecture for high-speed programming multilevel NAND flash memories. IEEE J. Solid-State Circ. **33**(8), 85–96 (2012)
50. K.-D. Suh et al., A 3.3 V 32 Mb NAND flash memory with incremental step pulse programming scheme, in *IEEE International Solid-State Circuits Conference* (*ISSCC*) (1995), pp. 128–129
51. J.-D. Lee et al., Degradation of tunnel oxide by FN current stress and its effects on data retention characteristics of 90-nm NAND flash memory cells, in *IEEE International Reliability Physics Symposium* (*IRPS*) (2003), pp. 497–501
52. K. Prall, Scaling non-volatile memory below 30 nm, in *IEEE Non-Volatile Semiconductor Memory Workshop* (*NVSMW*) (2007), pp. 5–10
53. S.W. Park, Prospect for new memory technology. Flash Mem. Summit (2012)
54. J.-D. Lee et al., Effects of floating-gate interference on nand flash memory cell operation. IEEE Electron Device Lett. **23**(5), 264–266 (2002)
55. M. Park et al., Direct field effect of neighboring cell transistor on cell-to-cell interference of NAND flash cell arrays. IEEE Electron Device Lett. **30**(2), 174–177 (2009)
56. J.-D. Lee et al., A new programming disturbance phenomenon in NAND flash memory by source/drain hot-electrons generated by GIDL current, in *IEEE Non-Volatile Semiconductor Memory Workshop* (*NVSMW*) (2006), pp. 31–33
57. S. Aritome et al., Novel negative Vt shift phenomenon of program-inhibit cell in 2X-3X-nm self-aligned STI NAND flash memory. IEEE Trans. Electron Devices **59**(11), 2950–2955 (2012)
58. Y.S. Kim et al., New scaling limitation of the floating gate cell in NAND flash memory, in *IEEE International Reliability Physics Symposium* (*IRPS*) (2010), pp. 599–603
59. K. Prall, K. Parat, 25 nm 64 Gb MLC NAND technology and scaling challenges, in *IEEE International Electron Devices Meeting* (*IEDM*) (2010), pp. 102–105
60. K.-T. Park et al., A zeroing cell-to-cell interference page architecture with temporary LSB storing and parallel MSB program scheme for MLC NAND flash memories. IEEE J. Solid-State Circ. **43**(4), 919–928 (2008)
61. N. Mielke et al., Bit error rate in NAND flash memories, in *IEEE International Reliability Physics Symposium* (*IRPS*) (2008), pp. 9–19
62. E. Yaakobi et al., Error characterization and coding schemes for flash memories, in *IEEE Global Communications Conference, Exhibition & Industry Forum* (*GLOBECOM*) (2010), pp. 1856–1860
63. R. Motwani et al., Low density parity check (LDPC) codes and the need for stronger ECC. Flash Mem. Summit (2011)

64. H. Parizi, Flash reliablity, beyond data management and ECC. Flash Mem. Summit (2013)
65. S. Tanakamaru et al., Error-prediction LDPC and error-recovery schemes for highly reliable solid-state drives (SSDs). IEEE J. Solid-State Circ. **48**(11), 2920–2933 (2013)
66. G. Dong et al., On the Use of soft-decision error-correction codes in NAND flash memory. IEEE Trans. Circ. Syst. I **58**(2), 429–439 (2011)
67. D.A. Patterson et al., A case for redundant arrays of inexpensive disks (RAID), in *ACM Special Interest Group on Management of Data* (*SIGMOD*) (1988), pp. 108–116
68. M. Blaum et al., EVENODD: an efficient scheme for tolerating double disk failures in RAID architectures. IEEE Trans. Comput. **44**(2), 192–202 (1995)
69. M. Balakrishnan et al., Differential RAID: rethinking RAID for SSD reliability, in *European Conference on Computer Systems* (2010)
70. D.-H. Lee, W. Sung, Least squares based cell-to-cell interference cancelation technique for multi-level cell NAND flash memory, in *IEEE International Conference on Acoustics, Speech, and Signal Processing* (*ICASSP*) (2012), pp. 1601–1604
71. R. Motwani, Architecture customized constrained coding for mitigating FGFG coupling in flash. Flash Mem. Summit (2011)
72. S. Tanakamaru et al., Highly reliable and low power SSD using asymmetric coding and stripe bitline-pattern elimination programming. IEEE J. Solid-State Circ. **47**(1), 85–96 (2012)
73. International Technology Roadmap for Semiconductors (2013), http://www.itrs.net/
74. W. Wang et al., Compact modeling and simulation of circuit reliability for 65-nm CMOS technology. IEEE Trans. Device Mater. Reliab. **7**(4), 509–517 (2007)
75. International Electrotechnical Commission, IEC61508, Functional safety of electrical/ electronic/ programmable electronic safety-related systems, Ed.2.0 (2010-4), http://www.iec.ch/functionalsafety/
76. ISO26262 Road vehicles -Functional safety-, First Edition, 2011-11
77. N. Kanekawa et al., *Dependability in Electronic Systems* (Springer, 2010). ISBN 978-1-4419-6714-5
78. Y. Sato et al., DART: dependable VLSI test architecture and its implementation. in *Proceedings International Test Conference*, paper 15.2 (2012)
79. Y. Miura et al., On-chip temperature and voltage measurement for field testing, in *Proceedings of European Test Symposium* (2012), p. 204
80. R. Franch, P. Restle, N. James, W. Huott, J. Friedrich, R. Dixon, S. Weitzel, K.V. Goor, G. Salem, On-chip timing uncertainty measurement on IBM microprocessors, in *Proceedings of International Test Conference* (2007), pp. 1.1.1–1.1.7
81. M.-C. Tsai, C.-H. Cheng, C.-M. Yang, An all-digital high-precision built-in delay time measurement circuit, in *Proceedings of IEEE VLSI Test Symposium* (2008), pp. 249–254
82. R. Tayade, J.A. Abraham, On-chip programmable capture for accurate path delay test and characterization, in *Proceedings of International Test Conference* (2008), pp. 6.2.1–6.2.10
83. X. Wang, M. Techranipoor, R. Datta, A novel architecture for on-chip path delay measurement, in *Proceedings of International Test Conference* (2009), pp. 12.1.1–12.1.10
84. X. Wang, M. Tehranipoor, R. Datta, Path-RO: a novel on-chip critical path delay measurement under process variations, in *Proceedings of International Conference on Computer-Aided Design* (Nov 2008), pp. 640–646
85. M. Nicolaidis, Y. Zorian, On-line testing for VLSI-A compendium of approaches. J. Electron. Test. Theory and Applications **12**(1–2), 7–20 (1998)
86. H. Al-Asaad et al., Online BIST for Embedded Systems. IEEE Des. Test Comput. **15**(4), 17–24 (1998)
87. J. Qian et al., Logic BIST architecture for system-level test and diagnosis, in *Proceedings of Asian Test Symposium* (2009), pp. 21–28
88. Y. Li, S. Makar, S. Mitra, CASP: concurrent autonomous chip self-test using stored test patterns, in *Proceedings of Design Automation and Test in Europe* (2008), pp. 885–89
89. H. Inoue et al., VAST: virtualization-assisted concurrent autonomous self-test, in *Proceedings of International Test Conference*, paper 12.3 (2008)

90. Y. Sato et al., A stochastic model for NBTI-induced LSI degradation in field, in *IEEE Asian Test Symposium* (2013), pp. 183–188
91. D. Ernst, N.S. Kim, S. Das, S. Pant, T. Pham, R. Rao, C. Ziesler, D. Blaauw, T. Austin, T. Mudge, K. Flautner, Razor: a low-power pipeline based on circuit-level timing speculation, in *Proceedings of International Symposium on Microarchitecture* (Dec 2003), pp. 7–18
92. T. Sato, Y. Kunitake, A simple flip-flop circuit for typical-case designs for DFM, in *Proceedings of International Symposium on Quality Electronic Design* (Mar 2007), pp. 539–544
93. Y. Sato et al., Reduction of NBTI-induced degradation on ring oscillators in FPGA, in *Proceedings of 20th Pacific Rim International Symposium on Dependable Computing* (2014), pp. 59–67
94. K. Itoh, Adaptive circuits for the 0.5-V nanoscale CMOS era, in IEEE *International Solid-State Circuits Conference* (Feb 2009), pp. 14–20
95. S. Borkar, T. Karnik, V. De, Design and reliability, in *Proceedings of Design Automation Conference* (June 2004), p. 75
96. C. Wilkerson, H. Gao, A.R. Alameldeen, Z. Chishti, M. Khellah, S.-L. Lu, Trading off cache capacity for reliability to enable low voltage operation, in *Proceedings of International Symposium on Computer Architecture* (June 2008), pp. 203–214
97. H. Fujiwara, S. Okumura, Y. Iguchi, H. Noguchi, H. Kawaguchi, M. Yoshimoto, A 7T/14T dependable SRAM and its array structure to avoid half selection, in *Proceedings of International Conference on VLSI Design* (Jan 2009), pp. 295–300
98. E. Seevinick, F.J. List, J. Lohstroh, Static-noise margin analysis of MOS SRAM cells. IEEE J. Solid-State Circ. **22**(5), 748–754 (1987)
99. E. Grossar, M. Stucchi, K. Maex, W. Dehaene, Statically aware SRAM memory array design, in *Proceedings of International Symposium on Quality Electronic Design* (Mar 2006), pp. 6–30
100. N. Binkert, S. Sardashti, R. Sen, K. Sewell, M. Shoaib, N. Vaish, M.D. Hill, D.A. Wood, B. Beckmann, G. Black, S.K. Reinhardt, A. Saidi, A. Basu, J. Hestness, D.R. Hower, T. Krishna, The gem5 simulator. ACM SIGARCH Comput. Archit. News **39**(2), 1–7 (2011)
101. Standard Performance Evaluation Corporation, The SPEC CPU 2006 Benchmark Suite. http://www.specbench.org
102. J. Yao, S. Okada, H. Shimada, K. Kobayashi, Y. Nakashima, DARA: a low-cost reliable architecture based on unhardened devices and its case study of radiation stress test, in *NSREC'12* (July 2012)

Chapter 7
Connectivity in Wireless Telecommunications

Kazuo Tsubouchi, Fumiyuki Adachi, Suguru Kameda, Mizuki Motoyoshi, Akinori Taira, Noriharu Suematsu, Tadashi Takagi, Hiroshi Oguma, Minoru Fujishima, Ryuji Inagaki, Masaomi Tsuru, Eiji Taniguchi, Hiroshi Fukumoto, Akira Matsuzawa, Masaya Miyahara, Makoto Iwata, Fumihiro Yamagata and Noboru Izuka

Abstract Good connection quality is a most important requirement in telecommunication systems. For the public wireless network, however, primary attention has so far been paid to providing broader bandwidth for rapidly expanding subscriber base. In this chapter, the connectivity of wireless telecommunication is undertaken as a central issue, while keeping in mind that the next-generation wireless will take on broader and ubiquitous machine-to-machine (M2M)

K. Tsubouchi (✉) · F. Adachi · S. Kameda · M. Motoyoshi · A. Taira
N. Suematsu · T. Takagi
Tohoku University, Sendai, Japan
e-mail: tsubo@riec.tohoku.ac.jp

F. Adachi
e-mail: adachi@ecei.tohoku.ac.jp

S. Kameda
e-mail: kameda@riec.tohoku.ac.jp

M. Motoyoshi
e-mail: mizuki@riec.tohoku.ac.jp

N. Suematsu
e-mail: suematsu@riec.tohoku.ac.jp

T. Takagi
e-mail: t-takagi@riec.tohoku.ac.jp

H. Oguma
National Institute of Technology, Toyama College, Toyama, Japan
e-mail: oguma@nc-toyama.ac.jp

M. Fujishima
Hiroshima University, Higashihiroshima, Japan
e-mail: fuji@hiroshima-u.ac.jp

R. Inagaki · M. Tsuru · E. Taniguchi · H. Fukumoto
Mitsubishi Electric Corporation, Kamakura, Japan

S. Asai (ed.), *VLSI Design and Test for Systems Dependability*,
https://doi.org/10.1007/978-4-431-56594-9_7

applications, and that the communication traffic will be 1000 times heavier in 10 years. The reliability and dependability will be a must in future wireless communications. The devastation caused by the East Japan Earthquake in March 2011, when few people in the area could use mobile phones satisfactorily because of the significant damages in infrastructure, taught a lesson that the wireless connection has to be maintained even in time of emergency. In this chapter, we will discuss heterogeneous wireless network that is combination of multiple wireless systems, e.g., cellular phone system, Wi-Fi, and wireless personal area network (WPAN) for realizing high-connectivity wireless network. The technology base that we have developed to enables the dependable heterogeneous network will be discussed in detail. All Silicon complementary metal oxide semiconductor (CMOS) technology will be used for analog/radio frequency (RF) circuits and baseband technologies for carrier frequencies from 700 to 60 GHz. A novel frequency domain equalizer (FDE) implemented in an application-specific integrated circuit (ASIC) will be a key component for smooth system handover. A scalable, low-voltage, and adaptive analog-to-digital (A/D) converter will be discussed as well.

Keywords Dependable Air • Wireless dependability • Wireless local area network (WLAN) • Mobile broadband wireless access (MBWA)
Quasi-Zenith Satellites (QZS)

A. Matsuzawa
Tokyo Institute of Technology, Tokyo, Japan
e-mail: matsu@ssc.pe.titech.ac.jp

M. Miyahara
High Energy Accelerator Research Organization, Tsukuba, Japan
e-mail: masaya@post.kek.jp

M. Iwata
Kochi University of Technology, Kami, Japan
e-mail: iwata.makoto@kochi-tech.ac.jp

F. Yamagata
National Institute of Technology, Kushiro College, Kushiro, Japan
e-mail: bun@kushiro-ct.ac.jp

N. Izuka
National Institute of Technology, Suzuka College, Suzuka, Japan
e-mail: izuka@info.suzuka-ct.ac.jp

7.1 Evolution of Public Wireless Networks and Future Challenges

Fumiyuki Adachi, Tohoku University

7.1.1 Wireless Network Evolution

The representative public wireless network is the cellular network. Recently, most of people always carry one or more wireless terminals to talk with each other and also to access/collect the information scattered all over the world and/or disseminate information through the Internet.

Figure 7.1 shows the schematic structure of the wireless cellular network. A number of base stations (BSs) are deployed in the service area. Users roam from one place to the other. One important function different from fixed telephone network is the database, called home location register (HLR) of the user equipment (UE) information including the UE location. The UE location is essential to forward the incoming call to each UE's nearest BS. Each UE communicates with its nearest BS and continuous communication is made by selecting another BS while moving across the network. More than one UEs can access the same BS using the multiple access technique [1], e.g., frequency-division multi-access (FDMA), time-division

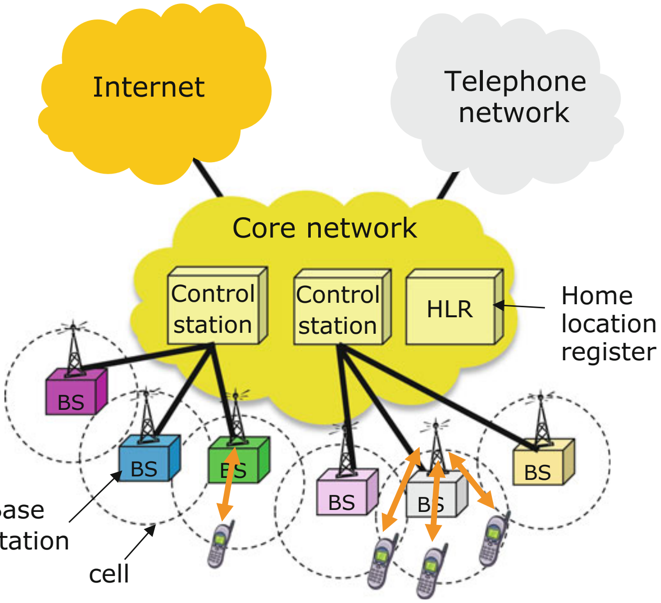


Fig. 7.1 Cellular network structure

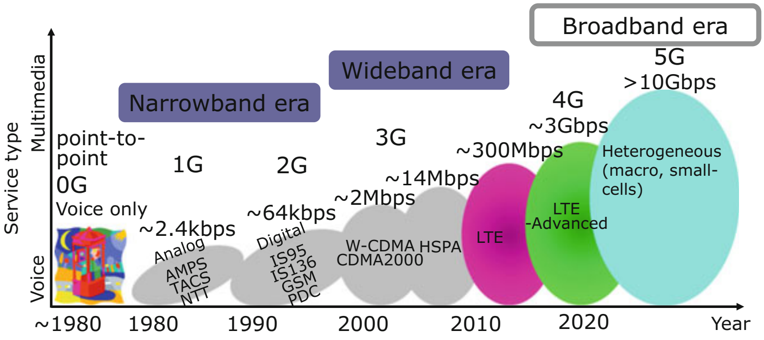


Fig. 7.2 Evolution of cellular networks

multi-access (TDMA), code-division multi-access (CDMA) or orthogonal frequency-division multi-access (OFDMA).

Every 10 years, a new technology has been introduced to evolve the wireless cellular network. In Japan, the first-generation public cellular networks (1G networks) with fully automated exchange, nationwide location registration and handover was put into service first in the world in December 1979 (at that time, it was called car telephone network [2]). 1G networks were based on analog wireless technology and had a very limited data transmission capability of around few kbps. Nonetheless, 1G brought about a change from the fixed "point-to-point" communication a wireless "anytime and anywhere" communication. Cellular networks have evolved from narrowband networks of around a few 10 kbps (2G networks) to wideband networks (3G networks) of around a few Mbps, and now on the way to broadband Long Term Evolution (LTE) [3] networks of 300 Mbps (3.9G networks) and LTE-Advanced networks (4G networks) (Fig. 7.2).

There was a big technical leap from 2G networks to 3G networks in terms of data rate capability (Fig. 7.3). 2G networks were designed to provide voice communication services while 3G networks were designed to provide broadband data services. In 1G and 2G networks, narrowband FDMA and narrowband TDMA were respectively adopted to efficiently share the limited bandwidth among many UEs. In 3G networks, wideband CDMA was adopted to increase the peak data rate [4]. In 4G, OFDMA and single-carrier FDMA (SC-FDMA) [5] are used.

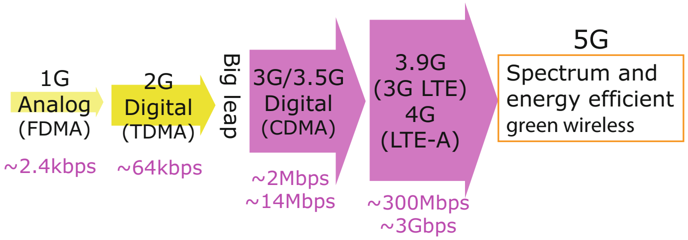
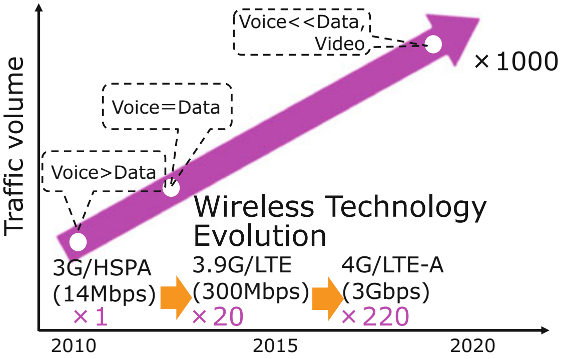


Fig. 7.3 Technology innovation towards broadband wireless

Fig. 7.4 Mobile communications traffic prediction (1,000 times increase in 10 years)



The penetration rate of cellular phones has reached 100% of Japanese population in around 2012. The wireless networks have become an important and essential infrastructure to our society. Recently, information to be exchanged over wireless networks is rapidly shifting from voice/low-speed data to high-speed data, e.g., high fidelity images, video, etc. Moreover, machine-to-machine (M2M) and device-to-device (D2D) communication traffic are expected to increase rapidly [6]. A huge number of machines/devices with relatively low data rate traffic are distributed widely. Therefore, the volume of wireless data traffic is predicted to increase exponentially about two times per year; it will increase about 1,000 times in 10 years (Fig. 7.4).

However, the available radio bandwidth and energy are limited. Therefore, the important technical issues for the forthcoming 5G wireless networks are to significantly improve the spectrum-efficiency and the energy-efficiency.

Small-cell networks are expected to simultaneously improve the spectrum-efficiency and energy-efficiency. The communication range between a UE and a BS of present cellular networks is around a few kilo meters, whereas it may be reduced to a few 100 m or less for a small-cell network. The short distance communication allows utilizing new frequency bands, e.g., millimeter-wave bands, where broad bandwidths are available.

7.1.2 Technical Issues

The prolonged communication failures over the wide area due to the Great East Japan Earthquake which attacked East Japan on March 11, 2011 reminded us that broadband data services is not a sole goal of wireless networks [7]. People take it for granted that they are connecting with communication networks at any time. However, once this routine is lost, our society may be brought into a tremendous chaos. The wireless networks will continuously evolve to provide more and more broader band data services without any doubt. However, in order to make wireless networks to be a dependable infrastructure of our modern society, future wireless networks should be resilient against disasters.

Currently the different networks such as cellular network, satellite communication network, Wi-Fi network, etc., are independently deployed and operated. If they are designed to cooperate in case of disaster, the dependability of communications networks can significantly improve. A huge volume of emergency traffic, such as safety confirmation, disaster information, etc., can be carried by any of surviving networks. This is the concept of the multilayered communications network [8].

In the multilayered communications network, different networks cooperate only in case of disaster. More attractive network architecture is a heterogeneous architecture consisting of macro-cell base station (MBS) and a number of small-cell base stations (SBSs) deployed inside MBS area (Fig. 7.5), where SBS can be a Wi-Fi access point. MBS takes a role of connection control for all UEs within its coverage area and SBS is dedicated to provide high-speed data transmission using high frequency band such as Millimeter wave [9]. The stationary and low-mobility UEs connect to SBS for high-speed data communication. However, if high mobility UEs connect to SBS, the handoff among SBSs occurs quite frequently and hence, increasing signaling overhead for connection control becomes a serious problem. Thus, high-mobility UEs are connected to MBSs for voice and data communication. Such a heterogeneous wireless network can simultaneously improve spectrum-efficiency and energy-efficiency while improving the resiliency against disasters.

Also device technology needs to be continuously evolved along with network evolution. Although 4G bandwidth will broaden to about 100 MHz, it does not necessarily mean the use of consecutive 100 MHz bands. Therefore, linear power amplifiers with low power consumption and low distortion having more than 100 MHz bandwidth need to be developed. Until the 3G networks, time domain wireless signal processing has been used. Beyond the 4G wireless networks, the

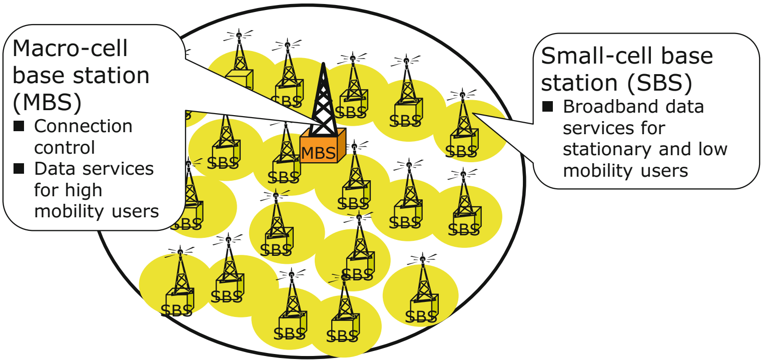

Macro-cell base station (MBS)
■ Connection control
■ Data services for high mobility users
MBS
SBS
Small-cell base station (SBS)
■ Broadband data services for stationary and low mobility users

Fig. 7.5 Heterogeneous wireless network (coexistence of MBS and SBSs deployed inside MBS area)

frequency domain wireless signal processing will be used. Low-power, high-speed devices will be required, such as digital/analog converters and discrete Fourier transform/inverse discrete Fourier transform (DFT/IDFT) devices with a sampling frequency of higher than 400 MHz and error correction coder/decoder of peak throughput of above 1 Gbps.

In the following subsection, an example of the heterogeneous wireless network will be introduced and its dependability will be discussed.

7.2 Challenges for Dependable Wireless System

Kazuo Tsubouchi, Tohoku University
Suguru Kameda, Tohoku University
Mizuki Motoyoshi, Tohoku University
Akinori Taira, Tohoku University
Noriharu Suematsu, Tohoku University
Tadashi Takagi, Tohoku University
Hiroshi Oguma, National Institute of Technology, Toyama College

7.2.1 History and Technical Trend of Hardware Technologies for Wireless Network

In Sect. 7.1, the evolution of wireless network technologies has been discussed. In this section, we will begin by reviewing the hardware based technologies and then discuss systems aspects in wireless telecommunications with particular emphasis on dependable connection.

The history and technical trend of cellular phone, personal computer (PC), network, and semiconductor are shown in Fig. 7.6. From Fig. 7.6, we can see that growth of cellular phone and PC technologies has been based on the semiconductor and network technologies. Scaling of complementary metal oxide semiconductor (CMOS) has developed according to Moore’s Law. Evolutions of network physics (PHY) technology, transmission control protocol & internet protocol (TCP/IP), and world wide web (WWW) have led the spread of the Internet. “Wintel” led the PC technologies and opened the door to the “Internet to the home” in the 1990s. For the evolution of wireless telecommunications in future, the hardware technologies based on Silicon technologies will be continue to be indispensable.

As described in Sect. 7.1, in recent years, communication traffic of mobile wireless terminals have been increasing, which demands higher throughput and larger capacity characteristics on mobile wireless systems. Moreover, it was a

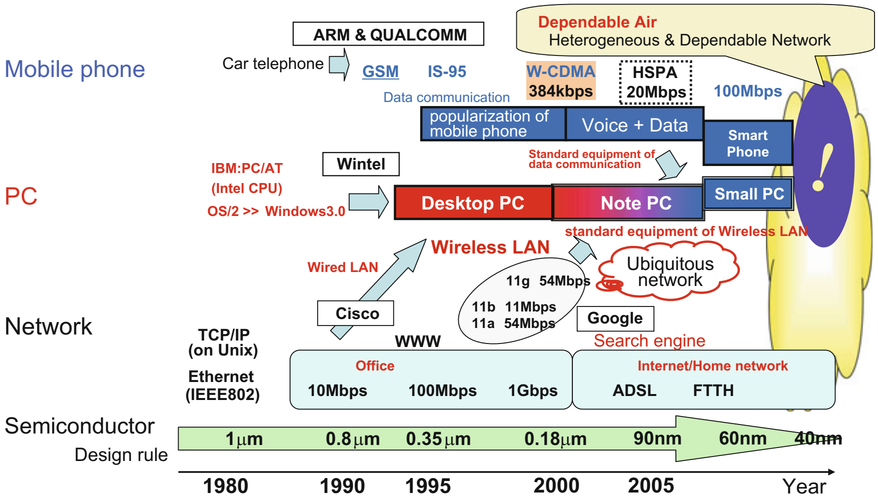


Fig. 7.6 History and technical trend of mobile phone, PC, Network, and Semiconductor. Growth of cellular phone and PC technologies has been based on the semiconductor and network technologies

painful lesson that most people in the most devastated areas in the great disaster of the East Japan Earthquake in 2011 were not able to use mobile phones because of the severe damage in infrastructures. It is desirable to construct a dependable wireless network which can achieve a high throughput during normal operation and still provide a communication link in the event of an emergency such as a great disaster. For such a wireless network, we have proposed “Dependable Air [10–15].” The Dependable Air is a new concept of wireless network that consists of various heterogeneous wireless systems adequately and seamlessly connected according to link conditions to realize larger communication capacity, higher throughput, and better link connectivity. As an estimation criterion for conventional wireless systems, frequency usage efficiency has been used. To make more adequate estimation for recent variety of wireless systems, we have proposed a new figure-of-merit called “Wireless Dependability [13, 14]” (see Sect. 7.2.3).

The concept of the Dependable Air is shown in Fig. 7.7, where the horizontal axis is throughput (bit/s) and vertical axis is distance (network cell size) (m), various wireless systems now in existence and/or being discussed for standardization are plotted. It is desirable to make a wireless network having a higher throughput with lower cost as well as a larger cell size, simultaneously. There is, however, a restriction (a solid line), which is plotted by assuming output power of 1 W at 2 GHz from mobile terminals. Here, output power of 1 W is reasonably determined by considering the effect on human body of electromagnetic radiation. From Fig. 7.7, we can see that there exists a tradeoff relationship between throughput and cell size and that performance of various wireless systems now

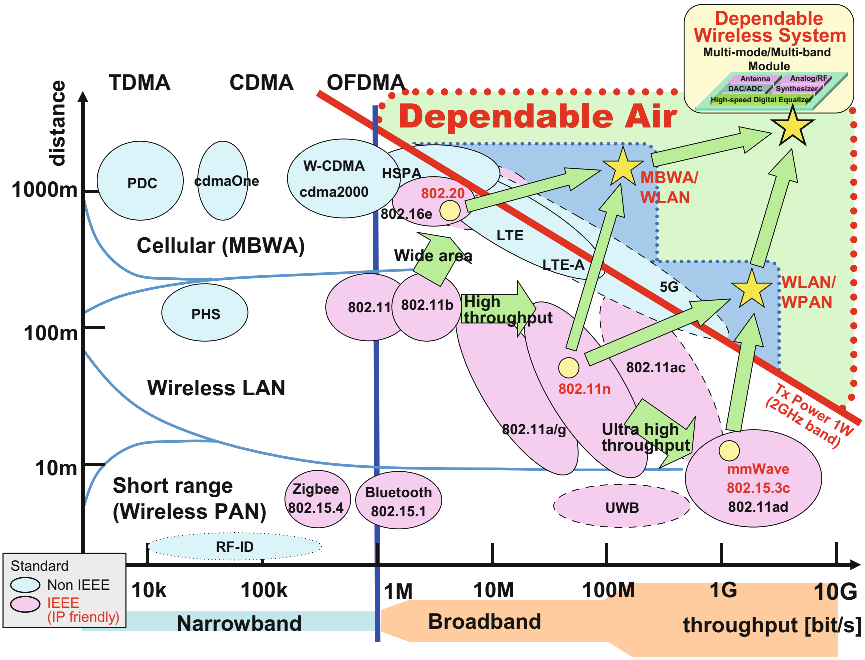


Fig. 7.7 Concept of Dependable Air. A solid line is plotted by assuming output power of 1 W at 2 GHz from mobile terminals. There exists a tradeoff relationship between throughput and cell size and that performance of various wireless systems now existing and/or under standardizing are approaching this restriction (solid) line. To overcome this restriction, the Dependable Air which consists of a number of cooperating heterogeneous wireless systems has been proposed

existing and/or under standardizing are approaching this restriction line. To overcome this restriction and to realize both higher throughput and larger cell size simultaneously, we have proposed Dependable Air which consists of a number of cooperating heterogeneous wireless systems.

7.2.2 Dependable Air

The Dependable Air is wireless networks with various heterogeneous wireless systems which are adequately and seamlessly connected according to link conditions to realize larger communication capacity, higher throughput, and better link connectivity. Figure 7.8 shows an example of the network configuration of Dependable Air. A number of heterogeneous wireless systems with higher throughput but small-cell size such as wireless local area network (WLAN) or wireless personal area network (WPAN) are installed in a wireless system with larger cell size but lower throughput such as mobile broadband wireless access (MBWA). The base station of MBWA controls other base stations of heterogeneous

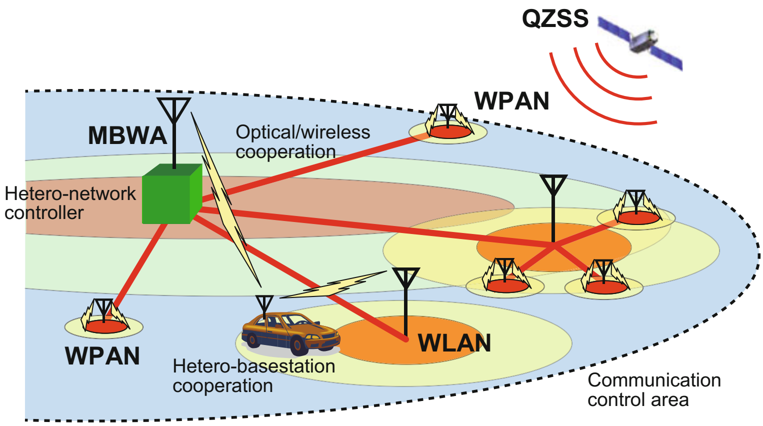

QZSS
WPAN
MBWA
Optical/wireless cooperation
Hetero-network controller
WPAN
Hetero-basestation cooperation
WLAN
Communication control area

Fig. 7.8 Coordinated heterogeneous base station of Dependable Air. A number of heterogeneous wireless systems such as WLAN and WPAN are installed in MBWA. The base station of MBWA controls other base stations of heterogeneous wireless systems, in this case WLAN or WPAN through light or wireless network links

wireless systems, in this case WLAN or WPAN through light or wireless network links. With a cooperation of these heterogeneous base stations, Dependable Air wireless network can realize (1) large mobility capability due to wide cell control and (2) user high throughput due to adequate access. Furthermore by selecting the optimum access network according to link condition and by adding satellite communication systems such as a location short message communication via Quasi-Zenith Satellites (QZS), written in Chap. 23, in the event of an emergency, (3) robust, safe and secure wireless system can be realized.

In the following sections in Chaps. 7, 9 and 23, the hardware and network technologies for the Dependable Air will be explained;

- Hardware technologies for the Dependable Wireless System (DWS) as multiband and multimode mobile terminals for Dependable Air
  - RF/antenna system by using all Silicon metal oxide semiconductor (Si-CMOS) technologies (in Sects. 7.3, 7.4 and 7.5)
  - Adaptive and scalable analog-to-digital converter (ADC) (in Sect. 7.6)
  - Adaptive digital processing for multiband and multimode broadband wireless systems (in Sect. 7.7).
- Network technologies for Dependable Air
  - Heterogeneous wireless network technologies (in Sect. 7.8)
  - Synchronized wireless system technologies (in Sect. 9.4)
  - Extended Dependable Air: Use of satellites in boosting dependability in wireless communications (in Chap. 23).

7.2.3 Wireless Dependability

We have proposed Wireless Dependability as a new estimation criterion of wireless network [13, 14]. It consists of two estimation factors which are gross throughput (F-value) and a number of simultaneously available users.

7.2.3.1 Gross Throughput (F-Value)

Figure 7.9a shows communication control area which has radius L_0 and area $S = \pi L_0^2$. Figure 7.9b shows an example of its throughput profile $R(\mathbf{r})$. Here, $R(\mathbf{r})$ is the throughput at an arbitrary position r and its value changes due to distance from the base station and link condition, etc. Then, gross throughput F is given as follows:

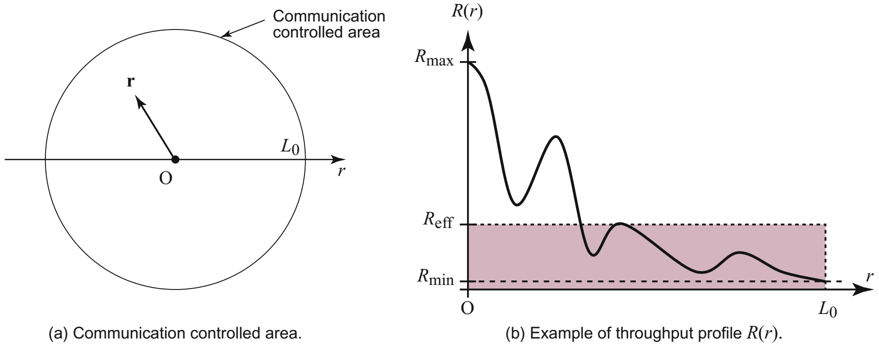
$$F = \int_S R(\mathbf{r}) d\mathbf{r} \tag{7.1}$$

When we introduce the average throughput in the cell area, Eq. 7.1 become Eq. 7.2.

$$F = S \cdot R_{\text{eff}} \tag{7.2}$$

For simplicity of calculation of R_{eff}, if we can suppose that R_{eff} is given by a geometric mean of maximum throughput $R_{\max}$ and minimum throughput $R_{\min}$, Eq. 7.2 becomes as follows

$$F = S\sqrt{R_{\max} \cdot R_{\min}} \tag{7.3}$$



(a) Communication controlled area.

(b) Example of throughput profile $R(r)$.

Fig. 7.9 **a** Communication cell area of wireless system, **b** example of throughput profile $R(r)$

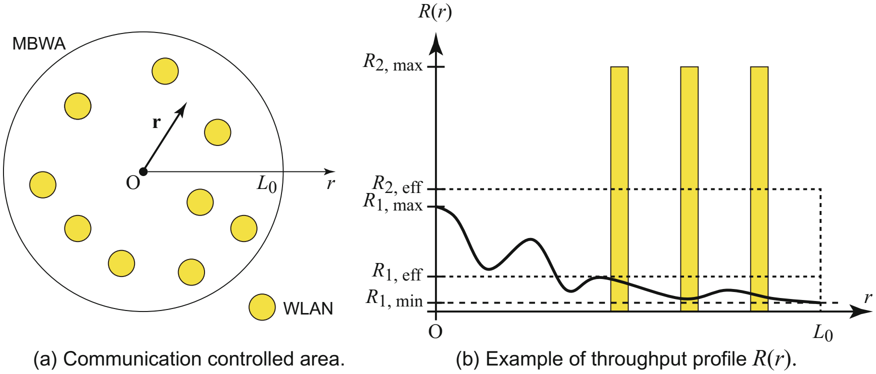


Fig. 7.10 **a** Heterogeneous network consisting of a MBWA as a control area and a number of WLAN cells, **b** example of throughput profile $R(r)$ of heterogeneous network consisting of a MBWA as a control area and a number of WLAN cells

Here, we consider that Eq. 7.3 is a new definition for a gross throughput and we call it "F-value."

Next, we expand this definition to a network composed of two types of heterogeneous systems. Figure 7.10a, b show the case where a number of WLAN cells with higher throughput but smaller cell size are installed in a MBWA cell with larger cell area but lower throughput. Here, the MBWA base station controls the other WLAN cells. Then the F-value (F_{h2}) of the heterogeneous network which consists of two types of wireless systems is defined as follows:

$$F_{\text{h2}} = S\sqrt{R_{2,\max}\sqrt{R_{1,\max}\cdot R_{1,\min}}} \tag{7.4}$$

Here, $R_{2,\max}$ is maximum throughput of the WLAN system, and $R_{1,\max}$ and $R_{1,\min}$ are maximum and minimum throughputs of the MBWA system, respectively. Equation 7.4 corresponds to the case where $R_{2,\max}$ is substituted for $R_{\max}$ and

$$R_{1,\text{eff}} = \sqrt{R_{1,\max}\cdot R_{1,\min}} \tag{7.5}$$

is substituted for $R_{\min}$ in Eq. 7.3.

From the analogy, we can expand the definition to a network composed of three types of heterogeneous systems. Figure 7.11a, b show the case where a number of WLAN and WPAN cells are installed in a MBWA cell. The F-value (F_{h3}) of the heterogeneous network which consists of three types of wireless systems is given by

$$F_{\text{h3}} = S\sqrt{R_{3,\max}\sqrt{R_{2,\max}\sqrt{R_{1,\max}\cdot R_{1,\min}}}} \tag{7.6}$$

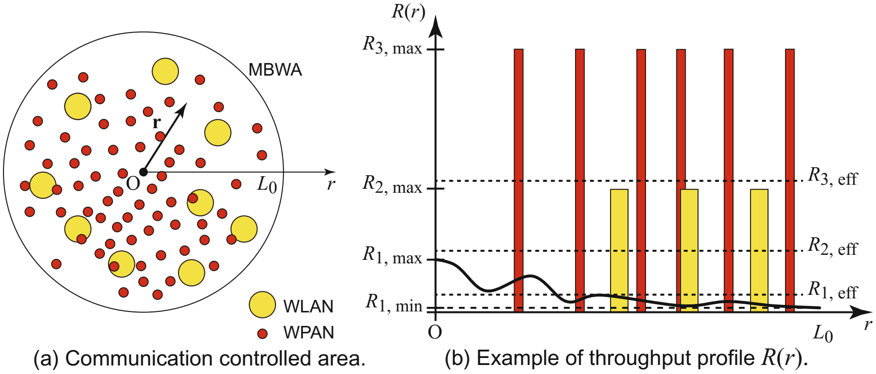


Fig. 7.11 **a** Heterogeneous network consisting of a MBWA as a control area and a number of WLAN and WPAN cells, **b** example of throughput profile $R(r)$ of heterogeneous network consisting of a MBWA as a control area and a number of WLAN and WPAN cells

Here, $R_{3,\max}$ is maximum throughput of the WPAN system.

In order to realize reasonable approximation for the Eqs. 7.4 and 7.6, WLAN and WPAN cells have to cover some part of the MBWA cell area. When the gross area of WLAN cells is A where the maximum throughput of $R_{2,\max}$ is achieved and that of WPAN cells is B where the maximum throughput of $R_{3,\max}$ is achieved, A and B are given as follows:

$$\frac{A}{S} = \frac{\sqrt{R_{2,\max}\sqrt{R_{1,\max}\cdot R_{1,\min}}} - \sqrt{R_{1,\max}\cdot R_{1,\min}}}{R_{2,\max}} \tag{7.7}$$

$$\frac{B}{S} = \frac{\sqrt{R_{3,\max}\sqrt{R_{2,\max}\sqrt{R_{1,\max}\cdot R_{1,\min}}}} - \sqrt{R_{2,\max}\sqrt{R_{1,\max}\cdot R_{1,\min}}}}{R_{3,\max}} \tag{7.8}$$

Table 7.1 shows the F-values of the individual systems of MBWA, WLAN, and WPAN and Dependable Air consisting of heterogeneous wireless systems. Here, each cell area S (km^2) of MBWA, WLAN and WPAN is assumed to be 2^2, 0.2^2, and 0.02^2, respectively. Each maximum throughput (Mbit/s) of MBWA, WLAN and WPAN are assumed to be 100, 1000, and 10,000, respectively. The minimum throughput is assumed to be 1/100 of the maximum throughput of each systems. Moreover, A/S and B/S, which correspond to gross areas of WLAN and WPAN in Dependable Air, are assumed to be 0.09 from Eqs. 7.7 and 7.8.

From Table 7.1, we can see that the F-value of homogeneous systems is 40 (km^2 Mbit/s) at the highest which is obtained in the system of MBWA and that those of WLAN and WPAN whose cell areas are smaller than MBWA are decreased in spite of their higher maximum throughputs. On the other hand, F-value (F_{h2}) of

Table 7.1 Example of F. In the table, the maximum throughput $R_{\max}$ (Mbit/s) of MBWA, WLAN and WPAN are assumed to be 100, 1000 and 10,000, respectively. The minimum throughput $R_{\min}$ (Mbit/s) is assumed to be 1/100 of the maximum throughput of each system

System	L^2 (km^2)	$R_{\max}$ (Mbit/s)	$R_{\min}$ (Mbit/s)	F (km^2 Mbit/s)
MBWA	2^2	$R_{1,\max} = 100$	$R_{1,\text{mix}} = 1$	40
WLAN	0.2^2	$R_{2,\max} = 1000$	$R_{1,\text{mix}} = 10$	4
WPAN	0.02^2	$R_{3,\max} = 10{,}000$	$R_{1,\text{mix}} = 100$	0.4
Dependable Air (MBWA + WLAN)	2^2	$R_{1,\max} = 100$ $R_{2,\max} = 1000$	$R_{1,\min} = 1$	400 (F_{h2})
Dependable Air (MBWA + WLAN + WPAN)	2^2	$R_{1,\max} = 100$ $R_{2,\max} = 1000$ $R_{3,\max} = 10,000$	$R_{1,\min} = 1$	4000 (F_{h3})

Dependable Air consisting of MBWA and WLAN is 400 (km^2 Mbit/s) and F-value (F_{h3}) of Dependable Air consisting of MBWA, WLAN and WPAN becomes as high as 4000 (km^2 Mbit/s).

Figure 7.12 shows the plots of F-value on the Fig. 7.7. The calculated F-values in Table 7.1 were fitted on Fig. 7.7.

7.2.3.2 Number of Simultaneously Available Users

The traffic congestion at emergency time such as the east Japan earthquake in 2011 is a serious problem. In such a case, it is important to evaluate wireless systems by the number of users who can communicate at the same time. Here, we discuss about the parameter N_{user} which is the number of users simultaneously communicating in a control area of wireless network. The user's throughput R_{user} is defined as follow by using parameters of a total throughput R_{all} and N_{user} of a control area.

$$R_{\text{user}} = \frac{\varepsilon R_{\text{all}}}{N_{\text{user}}} - R_{\text{oh}} \tag{7.9}$$

Here, ε is efficiency by multiple accesses and R_{oh} corresponds to a throughput which is converted from user's overhead. Next, Eq. 7.10 is derived from Eq. 7.9.

$$N_{\text{user}} = \frac{\varepsilon R_{\text{all}}}{R_{\text{user}} + R_{\text{oh}}} \leq \frac{\varepsilon R_{\text{all}}}{R_{\text{user, min}} + R_{\text{oh}}} \leq \frac{\varepsilon R_{\text{all}}}{R_{\text{oh}}} = N_{\text{user, max}} \tag{7.10}$$

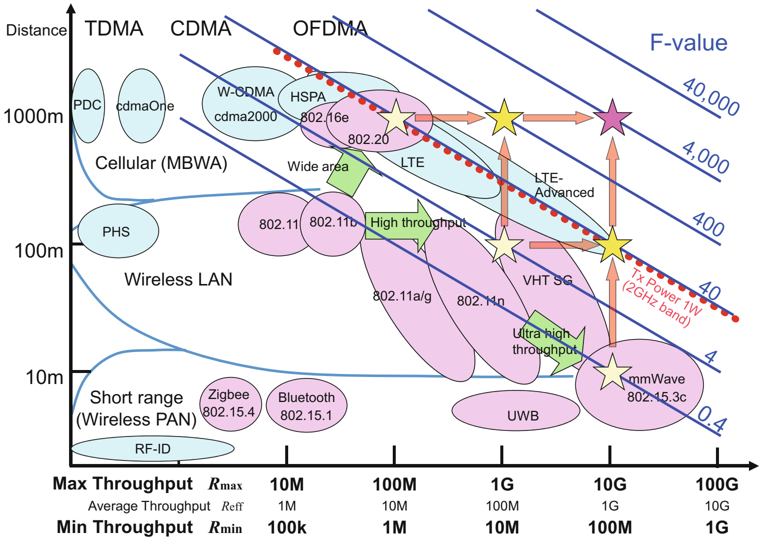


Fig. 7.12 Plots of F-value on the Fig. 7.7. The calculated F-values in Table 7.1 were overlaid on Fig. 7.7

Here, the $R_{\text{user, min}}$ is user's minimum throughput. From Eq. 7.10, it is said that there exists the maximum number of users $N_{\text{user, max}}$.

To increase $N_{\text{user, max}}$, maximizing of $\varepsilon\,(\varepsilon \to 1)$ or minimizing of $R_{\text{oh}}\,(R_{\text{oh}} \to 0)$ may be acceptable, however for an actual system, there is a limit for these values. By contrast, it is important to increase R_{all} for increasing $N_{\text{user, max}}$. Dependable Air network constructed by cooperation of a number of heterogeneous wireless systems can increase R_{all}.

Figure 7.13 shows relationship between N_{user} versus R_{user} for the homogeneous wireless systems and Dependable Air networks. In the figure, the data of now existing Long Term Evolution (LTE), IEEE 802.11n and under standardizing IEEE 802.11ad as MBWA, WLAN, and WPAN systems are shown with black lines, respectively. In the figure, those of Dependable Air networks consisted of a number of these heterogeneous systems are shown with red lines. From the figure, we can see that employment of Dependable Air networks makes not only much larger R_{user} but also N_{user}. Moreover, by the adding of location short message communication via QZS in the event of emergency, N_{user} will be further increased.

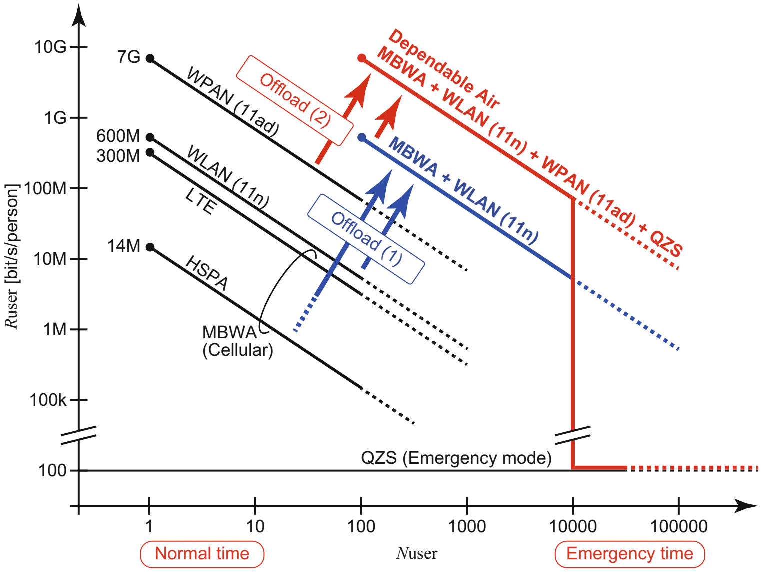


Fig. 7.13 Number of users in existing wireless systems and Dependable Air. Dependable Air networks enable not only much larger R_{user} but also N_{user}. By the adding of location short message communication via QZS in the event of emergency, N_{user} will be further increased

7.3 Transceiver Technologies for Dependable Wireless System

Tadashi Takagi, Tohoku University
Suguru Kameda, Tohoku University
Noriharu Suematsu, Tohoku University
Kazuo Tsubouchi, Tohoku University

7.3.1 Wireless Signal Processing

We have proposed the Dependable Wireless System (DWS) [10–12] as multiband and multimode mobile terminals for Dependable Air. Since the DWS transmits and receives wireless signals in the frequency range from 700 MHz to over 60 GHz band, the DWS requires multiple-carrier-frequency radio frequency (RF) circuits. Moreover, since the target system uses multiple bandwidths, the DWS has multiple sampling frequencies for digital processing.

Figure 7.14 shows the structure of the DWS. The key technologies for the transceiver are as follows:

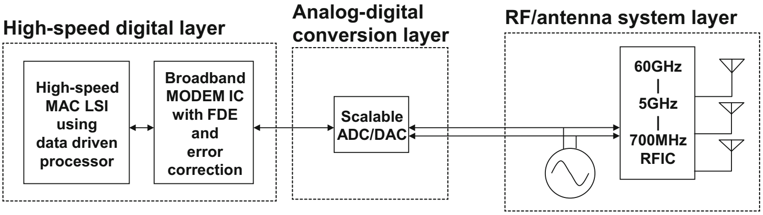

High-speed digital layer
High-speed MAC LSI using data driven processor
Broadband MODEM IC with FDE and error correction
Analog-digital conversion layer
Scalable ADC/DAC
RF/antenna system layer
60GHz
5GHz
700MHz
RFIC

Fig. 7.14 Structure of the dependable wireless system

1. An RF/antenna system using all silicon complementary metal oxide semiconductor (Si-CMOS) technology: to realize the DWS, we have developed 5- and 60-GHz-band RF circuits using 90 nm Si-CMOS technology.
2. High-speed digital processing: we have developed a novel frequency domain equalizer (FDE) technology, which is implemented in an application-specific integrated circuit (ASIC).
3. An adaptive and scalable analog-to-digital converter (ADC) and digital-to-analog converter (DAC): we have devised a current-mode pipeline ADC, which is suitable for process miniaturization and a low supply voltage.

In this section, the RF/antenna system technologies are discussed. Baseband technologies are explained in Sect. 7.7, and ADC technologies are explained in Sect. 7.6.

7.3.2 Si-CMOS 60-GHz-Band Receiver for Phased Array Antenna with Seven-Stage Low-Noise Amplifier, Wideband Mixer, and Five-Bit Baseband Phase Shifter

By using a millimeter-wave band, we can realize Gbit/s wireless connection because of the broad bandwidth. However, since the propagation loss of millimeter waves is high, an antenna with high-directional gain is required. Normally, high-directional-gain antennas have a narrow beam width, making it difficult to align the direction of a mobile terminal, especially for handheld devices. A phased array antenna system is one way for achieving high-directional gain and a wide beam-scanning area.

In this section, we propose a receiver for 60 GHz broadband communication [16, 17]. The receiver is designed and fabricated using 90 nm Si-CMOS technology. A superheterodyne structure with a baseband phase shifter is employed. A low-noise amplifier (LNA) in the receiver has seven stages whose peak gain frequencies are equally allocated in the desired bandwidth to achieve a flat gain characteristic. The 60 GHz downconversion mixer has an inductor-capacitor-resistor (LCR) load to achieve flatness over a 2 GHz bandwidth. The five-bit baseband phase shifter [18, 19]

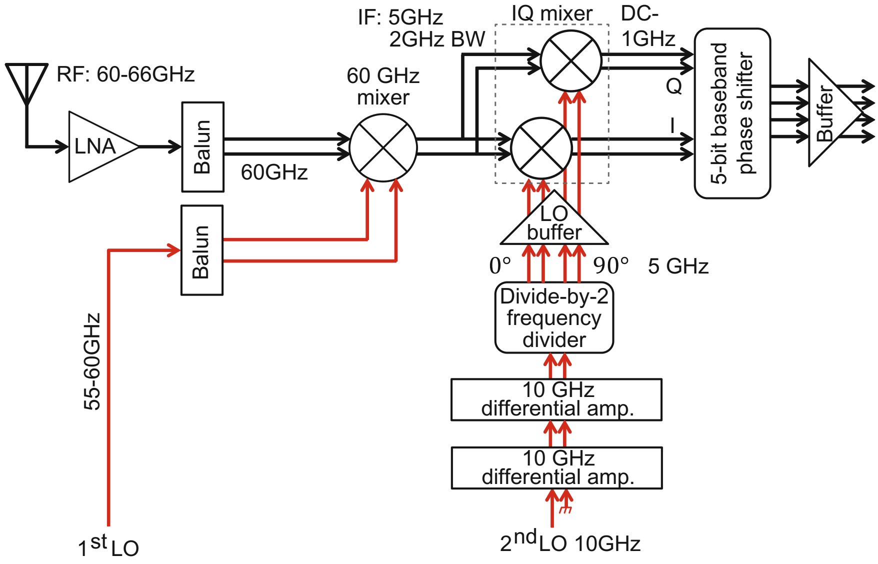


Fig. 7.15 Structure of the receiver

consists of a fixed amplifier matrix with five stages. Each stage has a phase shift with two fixed states. The proposed baseband phase shifter theoretically has no gain variation or phase error.

7.3.2.1 Design of the Receiver

The structure of the receiver is shown in Fig. 7.15. To connect the single-end output of the LNA to the differential input of the 60 GHz downconversion mixer, a passive balun [20] is used. A balun with the same structure is also used for the local oscillator (LO) input of the mixer. The intermediate frequency (IF) is selected to be 5 GHz. A double-balanced Gilbert cell mixer is used to implement the IQ mixer. The frequency of the second LO is 10 GHz. The second LO signal is converted to a 5 GHz IQ LO signal by a divide-by-2 frequency divider. The IQ mixer output is directly connected to the input of a baseband phase shifter with DC coupling. The phase shifter shifts the phase of the IQ signal. Moreover, it also suppress the 10 GHz image and leakages of the IQ mixer from LO and IF to baseband (BB). Therefore, no low-pass filter is necessary.

The details of the LNA, the 60 GHz downconversion mixer, and the five-bit baseband phase shifter are described in the following subsections.

Low-noise amplifier

The structure of the proposed LNA is shown in Fig. 7.16. A seven-stage structure is employed to achieve a power gain of over 20 dB. Coplanar lines with the ground are

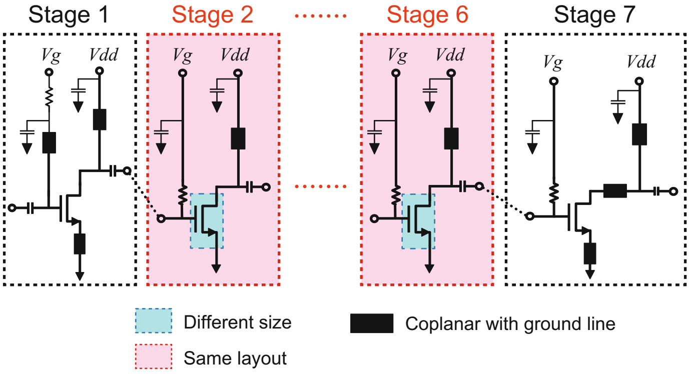
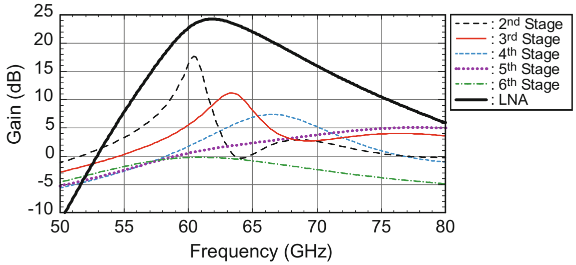


Fig. 7.16 Proposed LNA structure

Fig. 7.17 Simulated voltage gain peak of second to sixth stages and power gain of LNA



used for matching. The input of the first stage and the output of the seventh stage are designed for 50 Ω matching. To reduce the size of the matching circuit, a conjugate matching technique is used for interstage matching. From the second stage to the sixth stage, the matching center frequencies are adjusted as shown in Fig. 7.17 to achieve flatness over a wide bandwidth. Horizontal axis shows the frequency in GHz. Vertical axis shows the voltage gain of each stage. The solid line shows the power gain of the seven-stage LNA. When using a channel satisfying the IEEE 802.15.3c standard, the gain variations of channels 2–4 are lower than 2 dB. The simulated noise figure for the LNA is smaller than 6.5 dB in these three channels.

60 GHz downconversion mixer

A double-balanced Gilbert cell was used to design the downconversion mixer. The RF and LO signals are matched to 50 Ω. To realize a wide bandwidth, an LCR load is used as the output load of the mixer. Figure 7.18 shows the simulation results of the conversion gain for three cases using an R load, an LC resonance load, and an LCR load. Here, the LO frequency is 58 GHz, and the RF frequency is changed from 60 to 66 GHz. The LCR load achieves 1.2 dB gain variation over a 2 GHz bandwidth.

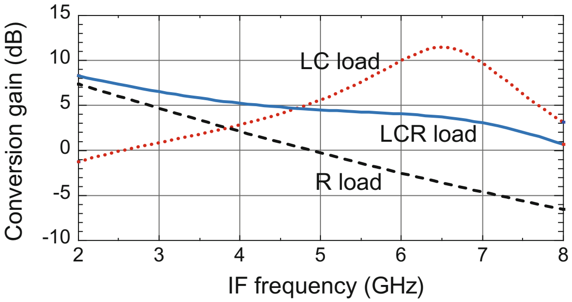


Fig. 7.18 Simulated conversion gain of mixer with different loads

Five-bit baseband phase shifter

We proposed a five-bit baseband phase shifter using a fixed-gain-amplifier matrix [18, 19]. The five-bit baseband phase shifter is divided into five stages. In theory, the gain variation and phase error are 0 for all states of the phase shifter. The baseband phase shifter has an rms phase shift error of less than 2.2° and an rms gain variation of less than 0.42 dB. The 3 dB bandwidth is 1.05 GHz.

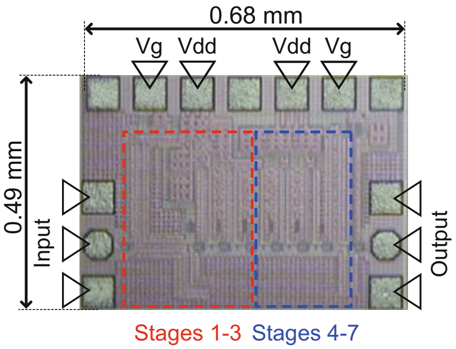
7.3.2.2 Evaluation Results

The LNA, 60 GHz mixer, and receiver were fabricated using 90 nm mixed-signal Si-CMOS technology. Figures 7.19, 7.20 and 7.21 shows photographs of the LNA, the 60 GHz mixer, and the receiver, whose die sizes were 0.49 × 0.68, 0.86 × 0.65, and 1.0 × 2.9 mm^2, respectively. The receiver was evaluated using continuous wave (CW) and quadrature phase shift keying (QPSK) signals. The CW was used for conversion gain and noise figure evaluation. The QPSK signal was used for error vector magnitude (EVM) measurement.

Evaluation using CW

The receiver was evaluated for channels 2, 3, and 4 of the IEEE 802.15.3c standard, whose frequencies of the first LO are 55.68, 57.64, and 59.8 GHz, respectively. The frequency of the second LO was fixed to 5 GHz. For each channel, the RF signal

Fig. 7.19 Photograph of fabricated LNA



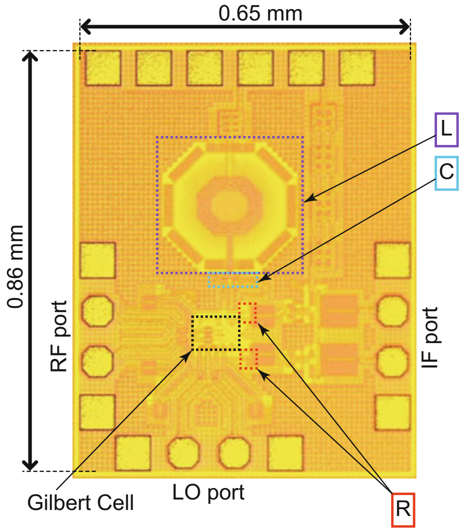


Fig. 7.20 Photograph of fabricated 60 GHz mixer

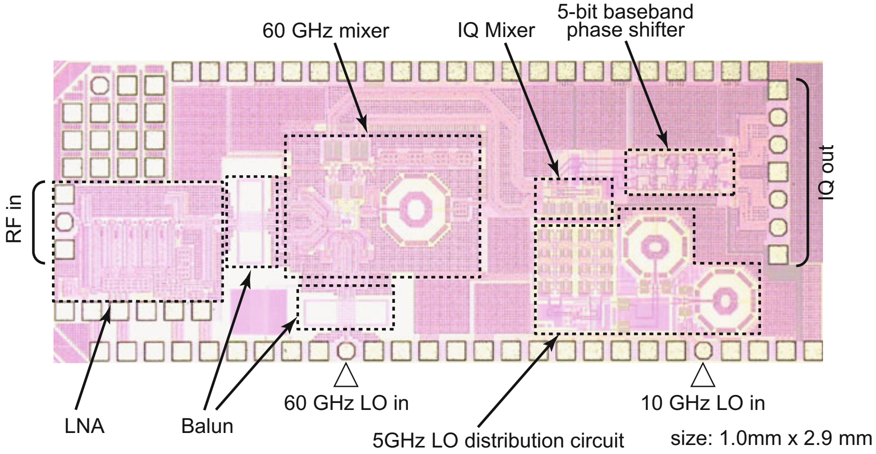


Fig. 7.21 Photograph of fabricated receiver

was swept in the range of ±1.2 GHz from the channel center. The outputs of the receiver are baseband differential I and Q signals. With the RF CW input, these IQ signals were CWs with theoretically the same amplitude and a 90° difference in the phase. The IQ differential signals comprise four single-end signals of $I+$, $I-$, $Q+$, and $Q-$. The conversion gain G is calculated as the power difference between the $Q-$ signal and the input CW signal. The noise figure F_N of the receiver is

Table 7.2 Power consumption of subcircuits of receiver

Subcircuit	Power consumption (mW)
LNA	31.8
60 GHz mixer core	8.3
60 GHz mixer buffer	6.8
IQ mixer	11.8
Second LO distribution circuit	48.4
Five-bit baseband phase shifter	4.9
Baseband output buffer	14.3

calculated from output noise power density N_{out} at $Q-$, the conversion gain G, and the input thermal noise density of −173.8 dBm/Hz (temperature 300 K) as

$$F_N = N_{out} - G - (-173.8)\ (\text{dB}). \tag{7.11}$$

The receiver consumed a power of 124 mW from a 1.2 V power supply. The power consumption of the subcircuits is shown in Table 7.2.

Figure 7.22 shows the conversion gain of the receiver. The horizontal axis shows the frequency in GHz. The vertical axis shows the conversion gain in dB. The solid lines show the measured results. The dotted lines show the calculated results. The calculated results were obtained from the measurement results for individual chips of the LNA, the balun, the 60 GHz mixer, and the baseband phase shifter and from the simulation results for the IQ mixer. These measurement and simulation results for the subcircuits are also plotted in the bottom half of Fig. 7.22. The variation of the gain of the LNA is lower than 1.5 dB for channels 2 and 3. The variation of the conversion gain of the 60 GHz mixer is 1.9 GHz.

The calculated and measured results were in agreement within 2 dB. Channel 2 had a 3 dB bandwidth of 1.9 GHz. Channel 3 had a 3 dB bandwidth of 1.6 GHz

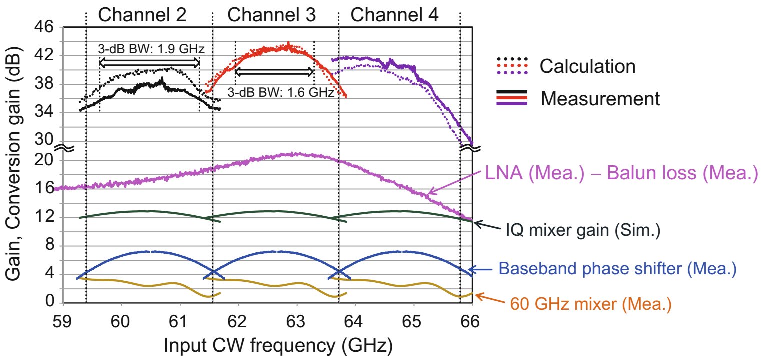


Fig. 7.22 Measured conversion gains of receiver and its component circuits. Calculated gains for receivers are plotted as well

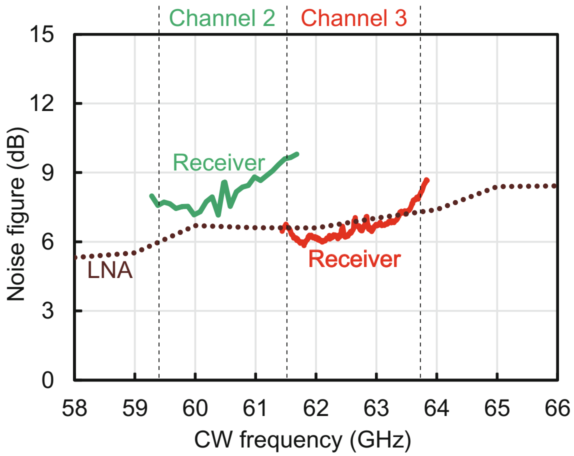


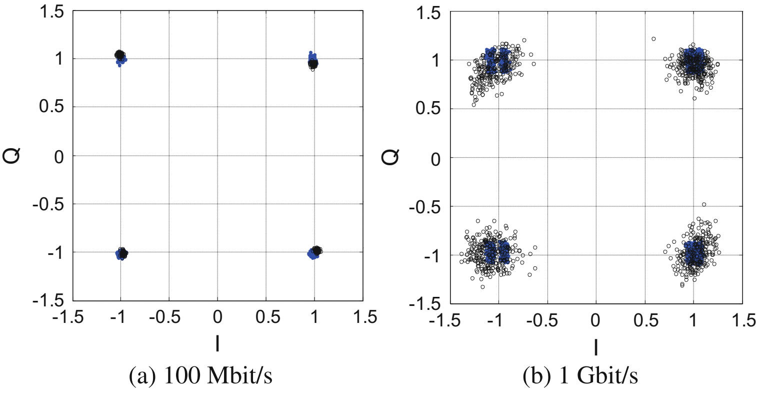
Fig. 7.23 Measured noise figures of LNA and the receiver

These 3 dB bandwidths are narrower than the channel bandwidth of 2.16 GHz. From the gain characteristics of the subcircuits, these 3 dB bandwidths are mostly affected by the baseband phase shifter. Therefore, to expand the 3 dB bandwidths of channels 2 and 3, it is necessary to expand the bandwidth of the baseband phase shifter. Channel 4 has a steep gain characteristic, which is due to the steep gain characteristic of the LNA.

Figure 7.23 shows the noise figures of the receiver and the LNA. Where the former is obtained using Eq. 7.11 and the latter is measured by a noise meter using the Y-factor method. The noise figure of the receiver was almost the same as that of the LNA. For channel 2, with an average gain of the LNA of 17 dB, the noise figure of the receiver was degraded in comparison with that of the LNA. For channel 3, with an average gain of the LNA of 20 dB, the degradation was lower. Moreover, due to the uncertainly of the gain measurement, there were frequency ranges where the measured noise figure of the receiver was lower than that of the LNA. The average noise figures of channels 2 and 3 were 8.6 and 6.9 dB, respectively.

Evaluation using QPSK signal

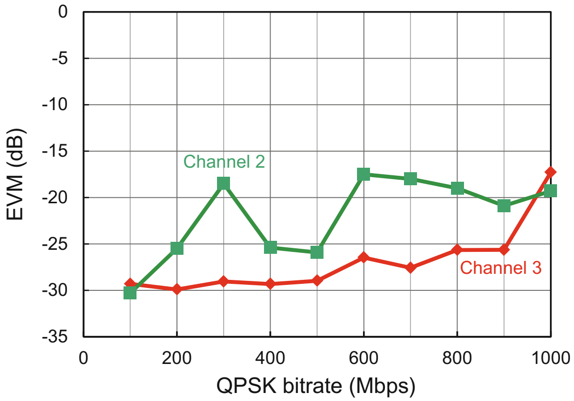
QPSK signals with a bit rate from 100 Mbit/s to 1 Gbit/s were used to measure the EVM. The QPSK signals were generated by an arbitrary wave generator (AWG) then modulated to the RF frequencies of channels 2 and 3. The AWG limited the maximum bit rate to 1 Gbit/s. Figure 7.24 shows the constellation of the normalized IQ signal with QPSK bit rates of 100 Mbit/s and 1 Gbit/s. The hollow points are IQ outputs of the receiver and the filled points are those of the original signal of the AWG. From Fig. 7.24a, the IQ signal had very good orthogonality. For a narrow bandwidth, the EVM of the output of the receiver was −30.3 dB, 2 dB worse than that of the original signal of −32.4 dB. For 1 Gbit/s QPSK, the original signal had an EVM of −23.7 dB, while the output signal of the receiver had an EVM of −17.3 dB. The degradation of the EVM is due to the high bandwidth of the signal.



(a) 100 Mbit/s (b) 1 Gbit/s

Fig. 7.24 Constellation of normalized IQ outputs of receiver (open circles) and arbitrary wave generator (blue closed circles)

Fig. 7.25 Measured EVMs of the receiver at channel 2 and 3



However, for the EVM of −17.3 dB, QPSK signal can be demodulated without error.

Figure 7.25 shows the EVM of the output of the receiver at channels 2 and 3 with bit rates from 100 Mbit/s to 1 Gbit/s. The horizontal axis shows the bit rate of the QPSK signal in Mbit/s. The vertical axis shows the EVM in dB. The EVM for channel 3 was roughly proportional to the bit rate, i.e., the higher the bit rate, the larger the EVM. The EVM for channel 2 was not proportional to the bit rate. This is due to the nonsmooth gain characteristic of channel 2 as shown in Fig. 7.22. From Fig. 7.25, the EVMs were smaller than −17 dB for channels 2 and 3. Therefore, the receiver can demodulate signals with bit rates of up to 1 Gbit/s.

7.3.3 60-GHz-Band Planar Dipole Array Antenna Using 3-D SiP Structure

Wireless systems using the unlicensed 60 GHz band are indispensable for ultrahigh-data-rate communication at bit rates of over 1 Gbit/s. IEEE 802.15.3c was published in 2009 for 60 GHz wireless personal area network (WPAN) systems.

Millimeter-wave-band wavelengths are shorter than those in the microwave band, making the transmission loss relatively large. Antennas should therefore be integrated with front-end parts. We have previously proposed a 3-D system-in-package (SiP) front-end module [21–23] and evaluated the antenna characteristics of a 60-GHz band 3-D SiP front-end module [24–27]. The radiation pattern of the antenna is static because a single-element antenna is used. However, the beam direction of the terminal should be oriented toward the access point. To solve problems of placement and poor portability, beamforming technologies are attractive solutions for small wireless terminals.

In this section, we propose a novel 60-GHz-band planar dipole array antenna structure using 3-D SiP technology [26, 27]. Its 2-D array structure is easily integrated with conventional small wireless terminals and it has a beam parallel to the substrates.

7.3.3.1 Design of the 60-GHz Band Beamforming Array Antenna Using the 3-D System-in-Package Structure

Figure 7.26 shows a conceptual illustration of a 60-GHz-band planar dipole array antenna using a 3-D SiP structure. A planar dipole antenna is selected as an element antenna since the planar dipole antenna has a beam parallel to the substrates. Several substrates are stacked vertically using 3-D SiP technology [22, 23]. Soldered copper balls support the substrates and are used to transmit the 60 GHz signal [22, 23]. The planar dipole antenna is located on top of the substrates in the 3-D SiP

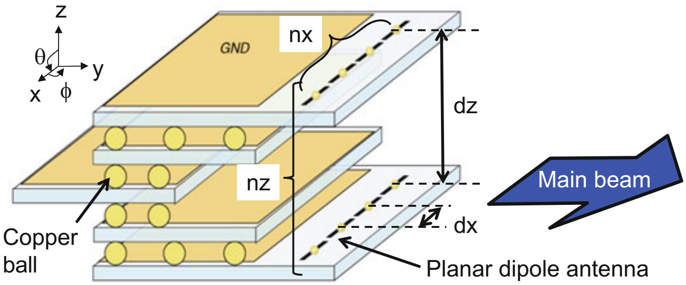


Fig. 7.26 A 60-GHz band planar dipole array antenna using 3-D SiP structure with a beam parallel to the substrates

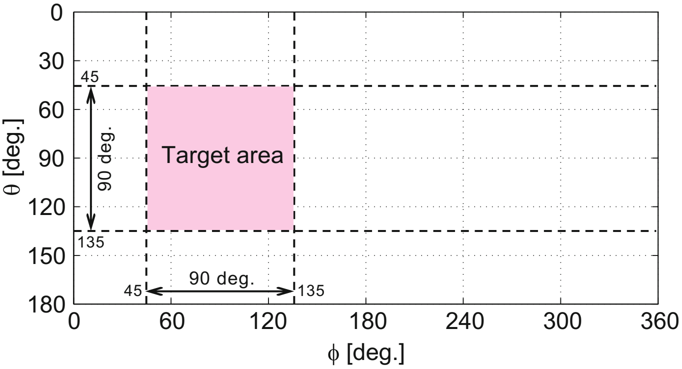


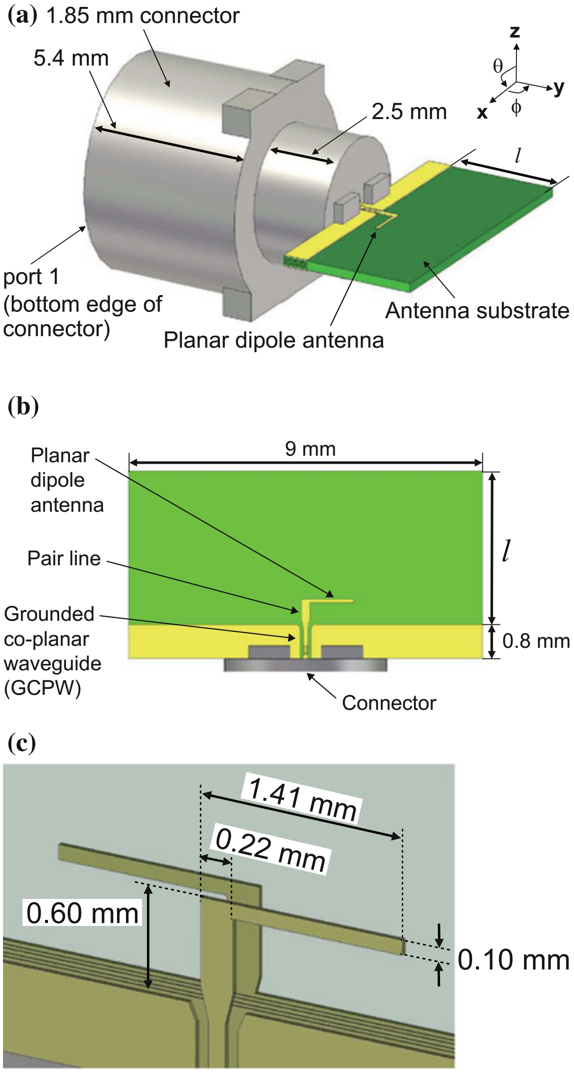
Fig. 7.27 Target area of the 60-GHz-band planar dipole array antenna for beamforming applications

structure. Four parameters, *nx*, *nz*, *dx*, and *dz*, are used in our numerical and 3-D electromagnetic field simulations, where *nx* and *nz* are the numbers of element antennas in the *x*- and *z*-directions and *dx* and *dz* are the distances between the element antennas in the *x*- and *z*-directions, respectively. We use five vertically stacked substrates with the planar dipole antennas placed on the top and bottom substrates as shown in Fig. 7.26. The number of stacked substrates is determined by *nz* or *dz*.

Figure 7.27 shows the target area of the 60-GHz-band planar dipole array antenna for beamforming applications. The target area is 90° in both the phi and theta directions. The objective of the design is full coverage of the target area with an antenna gain of 10 dBi.

Figure 7.28 shows a simulation model of a single-element planar dipole antenna with a 1.85 mm connector used for numerical analysis of the array antenna. Figure 7.28a shows an overview of the model, which consists of two parts: the antenna substrate and a connector. The main beam direction is the +*y* direction because the connector and the ground in the substrate act as reflectors. The effect of the reflectors in the 3-D SiP structure is large for measurement in the 60 GHz band; thus, the connector is modeled beforehand. We select a planar dipole antenna located at the center of the substrate as an antenna element. A feed port is set at the bottom edge of the connector. A 50 Ω coaxial transmission line is modeled in the connector, which has a length of 7.9 mm. The connector is simplified by assuming it to be a perfect electric conductor (PEC). In the simulation, the substrate length *l* (the length measured from the top edge of the grounded coplanar waveguide (GCPW)) is set as a parameter to analyze the relationship between *l* and the beam width. Figure 7.28b shows a front view of the antenna substrate. The width of the substrate is 9 mm, and a 0.8 mm GCPW is used as a feed line to the antenna. Figure 7.28c shows a transparent view of the antenna portion, in which both the inner and bottom layers can be seen. An antenna element is placed on the top and bottom surface of the substrates. The antenna is fed by a 0.60 mm pair line, which

Fig. 7.28 Simulation model of the 60-GHz-band planar dipole antenna with a 1.85 mm connector: **a** overview of the simulation model, **b** front view of the antenna substrate, and **c** transparent view of the antenna portion



is directly connected to the GCPW. The one-sided antenna length is 1.41 mm. The 3-D electromagnetic field simulation software Microwave Studio (Computer Simulation Technology Co.) was used to perform the simulation. In the simulation, MEGTRON6 substrates (Panasonic Electric Industry Co.) are assumed as the multilayered substrates. Datasheet values of 3.5 for the relative permittivity and 0.002 for the dielectric loss tangent at 2 GHz are used. The dielectric loss tangent at 60 GHz is defined as 0.002 on the basis of the second-order general dispersion model, since higher order models realize broadband constant characteristics.

7.3.3.2 Fabrication of the Proposed Array Antenna Structure

Figure 7.29 shows a block diagram of the 60-GHz-band 4 × 2 planar dipole array antenna for measurement of the beamforming coverage area. The beamforming coverage area where the gain exceeds 10 dBi is measured by operating the fabricated array antenna as a receiving antenna. To calculate 3-D radiation patterns, the amplitude and phase of the received signal in each direction are measured for each element antenna. Since 60 GHz multichannel measurement of the amplitude and phase is difficult, eight passive mixers are used for downconverting the received RF signal to an IF signal at each element antenna. The amplitude and phase of the downconverted IF signals are measured using multichannel oscilloscopes. The frequency of the IF signal is 1 MHz to allow observation of both the amplitude and the phase using a multichannel oscilloscope. Eight passive mixers (HMC-MDB169, Hittite Microwave Corporation) were used. A conventional T-junction was used to split the LO signal.

Figure 7.30 shows the structure of the 60-GHz-band 4 × 2 beamforming array antenna using 3-D SiP technology for measurement of the beamforming coverage area. Five multilayered substrates, named S1, S2, S3, S4, and S5 from the bottom of the 3-D SiP structure, are vertically stacked using 3-D SiP technology. Copper ball interconnections are used in the 3-D SiP structure for 60-GHz-band LO signal transmission [22, 23] and 1 MHz IF signal transmission. The copper balls are soldered and fixed, and serve to bond and support the various substrates. The 60-GHz-band LO signal is equally divided into eight passive mixers using T-junctions in substrates S1, S3, and S5. The antenna spacings dx and dz are $0.50\,\lambda_0$ and $0.65\,\lambda_0$, respectively, where substrates S2 and S4 are used to provide a wide dz spacing. The 1 MHz IF signal is transmitted from a coaxial connector mounted on both sides of substrate S3 to the multichannel oscilloscopes.

Figure 7.31 shows the 60-GHz-band 4 × 2 beamforming array antenna fabricated using 3-D SiP technology for measuring the beamforming coverage area.

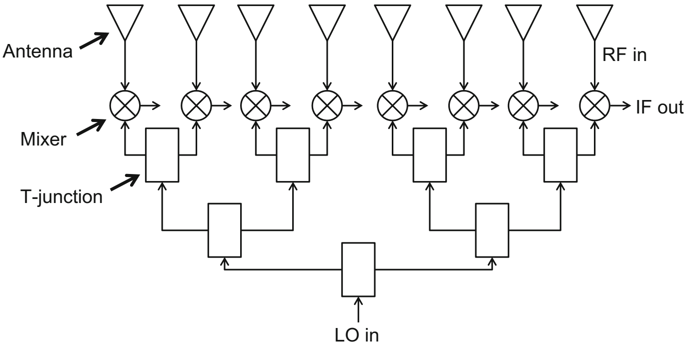


Fig. 7.29 Block diagram of a 60-GHz-band 4 × 2 planar dipole array antenna for measurement of beamforming coverage area

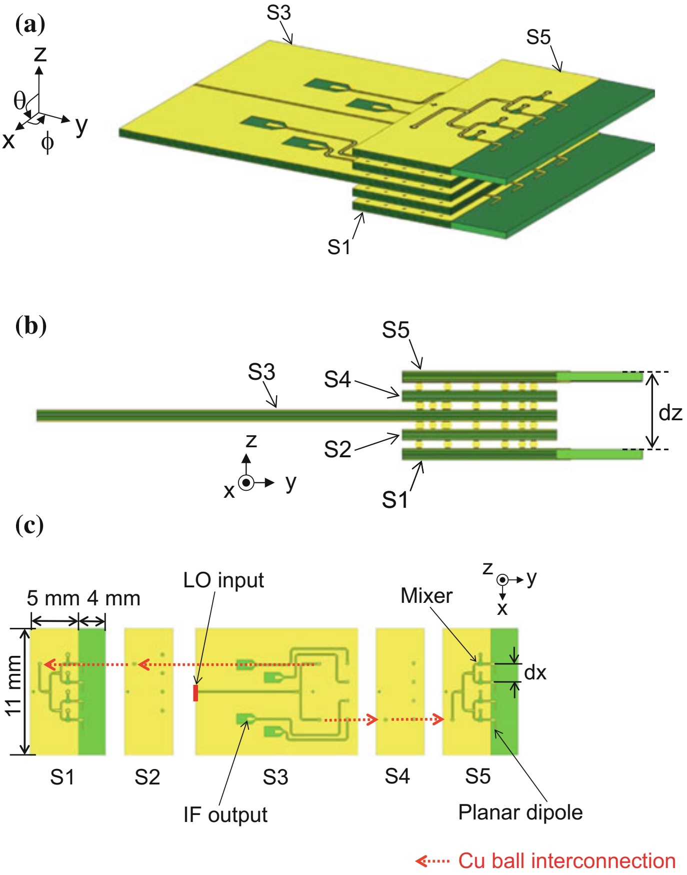


Fig. 7.30 Structure of the 60-GHz-band 4 × 2 beamforming array antenna using 3-D SiP technology for measurement of the beamforming coverage area: **a** overview, **b** side view, and **c** front view of each substrate

The five substrates are vertically stacked using 3-D SiP technology with copper balls. The planar dipole antennas are located on the top and bottom substrates. The passive mixers for downconverting the received signal are mounted by conventional gold wire bonding. The input terminal for the LO signal is located at the left edge of substrate S3, which is the center substrate in the 3-D SiP structure. For the LO input to substrate S3, a 1.85 mm coaxial connector integrated with a GCPW transition is used. The LO signal is equally divided by a T-junction and is transmitted to the LO pad of the mixer. Ultrasmall coaxial connectors (W.FL series, Hirose Electric Co.) are used for IF signal transmission.

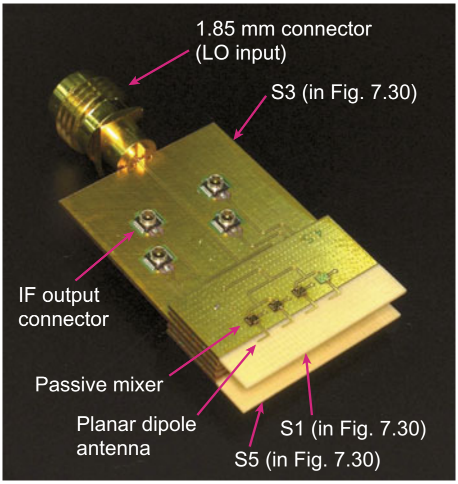


Fig. 7.31 60-GHz-band 4 × 2 beamforming array antenna fabricated using 3-D SiP technology for measurement of the beamforming coverage area

7.4 Broadband RF Circuit for Versatile, Dependable Wireless Communications

Minoru Fujishima, Hiroshima University

7.4.1 Requirements for RF Circuits in Dependable Wireless Communications

Wireless communication system sometimes fails to offer uninterrupted connection due to changes in environment conditions by motion and position of terminals, which is different from the situation of fixed wireline communication system. In the case of low-speed wireless communication, it is relatively easy to maintain connectivity against changes in environment conditions even for communication over a large distance. On the other hand, in high-speed communication it is generally more difficult to maintain connectivity. Therefore, the dependable wireless system, which is the main topic of this chapter, requires the RF circuits which offer high-speed communication in desirable environment conditions and reduced communication speed in undesirable environment conditions to avoid disconnect in communication. To build this kind of adaptive system, wireless integrated circuits supporting multiple communication methods are required. For example, when microwave band (low frequency) for high connectivity and millimeter-wave band (high frequency above 30 GHz) for high-speed application beyond one giga-bits per second are simultaneously available in a wireless communication system, average data rate will be improved while maintaining connectivity. Namely, to realize high-speed communication service without losing connection reliability, wireless circuits for millimeter-wave or even short-millimeter-wave (over 100 GHz) as well as microwave must be integrated. It is noted that low-power operation is always important to improve battery lifetime, which is inevitable for mobile communication system. Thus, in this section, two basic building blocks, a low-phase-noise oscillator and a wideband amplifier, for silicon-integrated circuits applicable to millimeter wave are discussed using CMOS process. Here, key technologies for an oscillator and an amplifier are addressed. With regard to an oscillator, generally, phase noise becomes degraded as frequency is increased. Nevertheless, phase noise below −90 dBc/Hz at 1 MHz offset is required for multi-symbol quadrature modulation. To overcome this issue, we proposed a novel oscillator utilizing p-type MOSFETs, which have not been used due to its performance inferior to n-type MOSFETs. With regard to an amplifier, bandwidth more than 20 GHz is required for over 10 Gbps communication. For this purpose, many-stage amplifiers with properly designed matching networks are proposed. In the following sections, technologies for an oscillator and an amplifier are discussed, which is important to realize high speed and low power simultaneously in wireless integrated circuits.

7.4.2 Millimeter-Wave Oscillator Using P-Type Transistors

Since silicon integrated circuits have been widely used in home electronics such as cellular phone, personal computer, television, etc., and still have a great potential of low cost and low power in home electronics even in millimeter-wave band. Therefore, we are studying millimeter-wave silicon integrated circuits due to their potential nature of low cost and low power even though high frequency characteristics of silicon may generally be slightly inferior to those of compound semiconductor. Here, we have to consider availability of frequency bands for wireless communication since radio wave is principally finite resource shared by many different kinds of applications. To improve communication speed utilizing already allocated frequency bands, multi-symbol quadrature modulation is a good choice since they can offer more number of bits per hertz and thus communication capacity. When multi-symbol quadrature modulation is used even in millimeter-wave band, oscillators generating carrier signals should have low-phase-noise characteristics. It is generally considered that n-type transistors operate at high speed but generate large noise while p-type transistors operate at low speed but generate low noise in silicon integrated circuits. From this reason, n-type transistors were conventionally used for millimeter-wave applications. However, not only n-type transistors but also p-type transistors are improved in frequency characteristics due to reduction of channel length and mobility improvement with strained silicon. Thus, we have studied a millimeter-wave oscillator with p-type transistors in W-band (75–110 GHz) for applications such as radars and high-speed communications, for p-type transistors generate less flicker noise than n-type transistors and are expected to realize low-noise oscillators. We have fabricated an 80 GHz oscillator comprising of p-type transistors with 65 nm

Fig. 7.32 Chip microphotograph of 80 GHz oscillator with p-type transistors

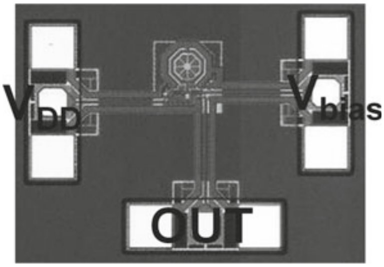


Fig. 7.33 Schematic of 80 GHz p-type transistor oscillator

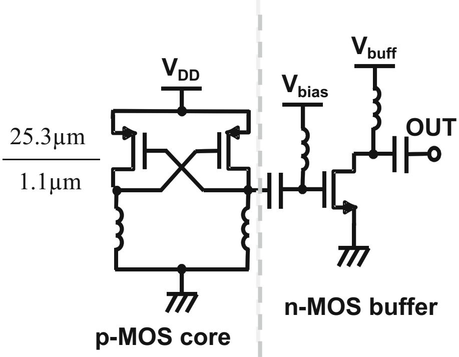


Fig. 7.34 Phase-noise characteristics of 80 GHz p-type transistor oscillator

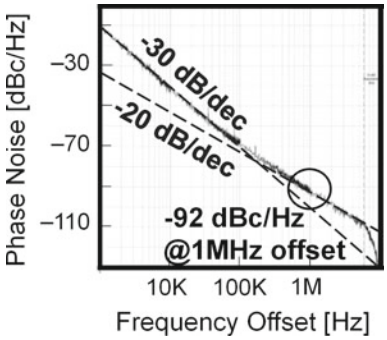
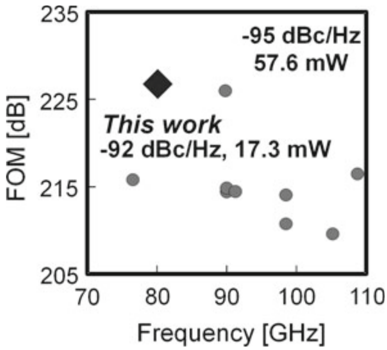


Fig. 7.35 Comparison among 80 GHz p-type transistor oscillator and other oscillators ever published



CMOS process [28]. Chip microphotograph of the fabricated oscillator with p-type transistors is shown in Fig. 7.32 and its schematic is shown in Fig. 7.33. Measured results of phase noise are shown in Fig. 7.34 and comparison of the figures of merits (FOM) is shown in Fig. 7.35. In this study, we have successfully realized an 80 GHz oscillator with p-type transistors, which shows −92 dBc/Hz at 1 MHz offset from carrier frequency. Finally, it is shown that the proposed oscillator demonstrates the best FOM in W-band.

7.4.3 Short-Millimeter-Wave Wideband Silicon Amplifier

Silicon high-speed communication circuits with 60 GHz band becomes promising candidate realizing more than one giga bit per second and will be implemented in mass production in the near future thanks to advancement in manufacturing technology, In fact, as will be shown below, a wide frequency band in excess of 20 GHz will be available in the carrier frequency range above 100 GHz, which would enable a throughput higher than 10 Gbit/s with low power consumption. Key technology for realizing it is wideband silicon amplifiers operating at more than 100 GHz. The amplifiers must have flat frequency response in gain and group delay over 20 GHz frequency band in order to amplify modulated signal without distortion. Therefore, we aim at realizing wideband amplifier with flat gain and group-delay response operating at more than 100 GHz.

We have designed multi-stage amplifier operating in D band (110–170 GHz) which can be allocated for applications for wireless communication [29, 30]. Although frequency response of the MOSFETs has been improved due to miniaturization of transistor size, transistor gain per stage is still less than 5 dB in a typical case which is insufficient for the amplifier gain. Thus, a many-stage amplifier is inevitable for realizing reasonable gain. Here, matching networks connect each gain stage for impedance transformation to transfer input power to output efficiently. Matching network has own frequency characteristics determined by circuit parameters. By allocating frequency response properly in the matching networks inserted between gain stages, wideband amplifier with flat gain and group-delay frequency response can be realized. By applying this design methodology, we have designed two types of amplifiers operating at 120 and 140 GHz bands. The amplifiers have been fabricated with 65 nm CMOS process. Circuit schematic and chip microphotograph are shown in Figs. 7.36 and 7.37, respectively. Measured frequency responses are shown in Fig. 7.38. Both amplifiers for 120 and 140 GHz bands show wideband characteristics more than 20 GHz, and the desired flat frequency responses in gain and group delay have been successfully realized.

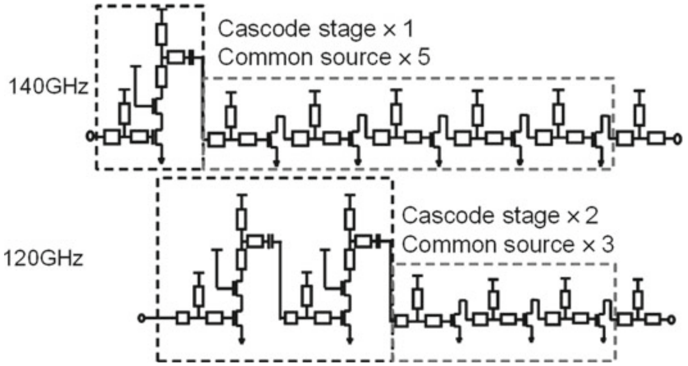


Fig. 7.36 Schematics of short-millimeter-wave amplifiers with silicon integrated circuits

Fig. 7.37 Chip microphotograph of short-millimeter-wave amplifiers

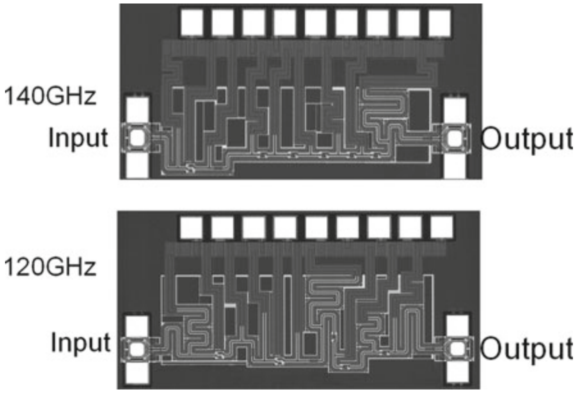
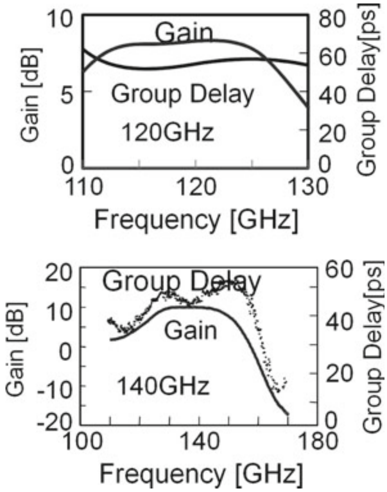


Fig. 7.38 Frequency responses of short-millimeter-wave amplifiers



7.4.4 Discussions and Further Investigations

In this section, two basic building blocks, a p-type oscillator and many-stage amplifiers, on millimeter-wave silicon integrated circuits are introduced for realizing high-speed communication. One is 80-GHz oscillator with p-type transistors, which is firstly applied in millimeter-wave operation. The fabricated p-type 80-GHz oscillator realizes −92 dBc/Hz at 1 MHz offset, which is useful for 16- or 64-quadrature amplitude modulations (QAM) for higher speed communication. The other one is short-millimeter-wave silicon amplifiers with frequency band over 20 GHz. It is shown that silicon integrated circuits, generally inferior to compound semiconductor circuits, can still operate in short-millimeter-wave band beyond 100 GHz. Furthermore, it is shown that flat frequency responses in gain and group delay can be realized by designing matching networks properly. It will be useful for realizing high-speed communication more than 10 Gbit/s using wide frequency band more than 20 GHz. The techniques introduced in this section will contribute to super broadband RF circuits for versatile, dependable wireless communications. Since we opened a door to future super broadband wireless system, the complete wireless hardware and system should be studied in the next step.

7.5 All-Si-CMOS Front-End ICs for Multiband Micro-/Millimeter-Wave Communications

Ryuji Inagaki, Mitsubishi Electric Corporation
Masami Tsuru, Mitsubishi Electric Corporation
Eiji Taniguchi, Mitsubishi Electric Corporation
Hiroshi Fukumoto, Mitsubishi Electric Corporation

7.5.1 Techniques for the Multiband Front-End IC

Recently, various different types of wireless communication systems, such as Mobile Broadband Wireless Access (MBWA), Wireless Local Area Network (WLAN), and Wireless Personal Area Network (WPAN), have been used. If a system is down, a user subscribing only to that specific system is totally cut out of the communication network, but it will be inconvenient to have many mobile devices for each communication system. One of methods to solve this problem is to realize a multiple wireless system, such as described as the Dependable air [12, 13].

Figure 7.39 shows the block diagram of a mobile device for multiple wireless systems. The main circuits constituting the mobile device are Radio Frequency (RF) Transmitter/Receiver Module, Digital–Analog (D/A)/Analog–Digital (A/D) converter [31], Transmitter/Receiver Baseband Module [32], etc. The mobile device

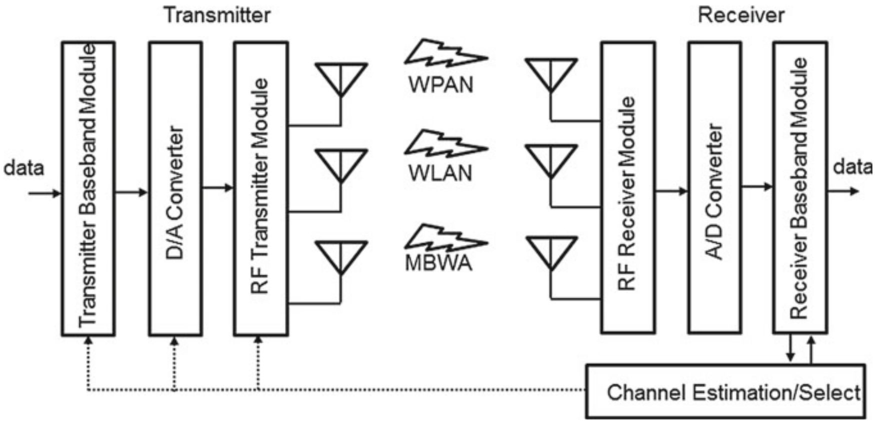


Fig. 7.39 Block diagram of a mobile device for multiple wireless systems

provides dependable connection because it automatically switches to another available system even if one system is down. The RF Transmitter/Receiver Module takes the role of converting a baseband signal to RF signals, and vice versa. A family of multiband transmitter/receiver front-end Integrated Circuits (ICs) that can be used for both microwave- and millimeter-wave communications is necessary for the RF Module.

This section presents the result of the development of the multiband receiver front-end ICs. In order to realize the multiband receiver front-end IC, small size, switching function, and low-noise performance are required. The assembly of the millimeter-wave ICs is also important. For miniaturization, it is effective to use sub-micron process on Si and to share a part of some receiver front-ends. Each received signal is switched in the shared circuit. However, the power level of each received signal differs between the systems. Therefore, it is needed to adjust the power level using a variable gain amplifier (VGA), because the received signal is strained by saturation of a mixer of shared circuit and the signal quality is degraded. In order to achieve a low-noise performance, it is important to develop a high gain low-noise amplifier (LNA) because it reduces influence of the subsequent circuit such as the mixer. The LNA has high output power, requiring high saturation performance for the mixer. The design of the assembly including the flip-bonded millimeter-wave ICs on a substrate requires careful waveguide engineering to avoid spurious propagation modes.

The outline of the section is as follows. Section 7.5.2 describes the configuration of the multiband receiver front-end IC for 5 GHz band and 60 GHz band systems, such as WLAN and WPAN. Section 7.5.3 presents the circuit components for the multi-band receiver front-end IC: a high gain LNA, a high saturation transistor pair type even harmonic mixer (HMIX) for low-noise performance and the 5 GHz band Intermediate Frequency (IF)-VGA to change the gain. Section 7.5.4 presents suppression of spurious modes in flip-chip assembly. Section 7.5.5 shows measurement results of the fabricated multiband (5 GHz/60 GHz) receiver front-end IC.

7.5.2 Configuration of the Multiband Receiver Front-End IC

Figure 7.40 shows a configuration of a 5 GHz/60 GHz receiver front-end IC [33]. The architecture of the receiver front-end IC is a direct conversion configuration at 5 GHz band and a superheterodyne configuration at 60 GHz band. The 5 GHz front-end and the 60 GHz front-end share an IF-VGA and a quadrature mixer for reduction of the area of IC.

The 5 GHz front-end consists of a 5 GHz band LNA and a 5 GHz band common circuit. The 60 GHz front-end consists of the 60 GHz RF front-end and the 5 GHz band common circuit. The 5 GHz band common circuit consists of a switch, the IF-VGA, the quadrature mixer, a baseband amplifier (AMP), and a 10 GHz band frequency divider. The 60 GHz RF front-end consists of a 60 GHz band LNA, a balun, a 60 GHz band HMIX, and a 5 GHz band IF-AMP.

The 60 GHz RF front-end converts 60–5 GHz as IF signal. The IF signal is input into the quadrature mixer through the switch and the IF-VGA. The power level of each IF signal differs between the systems. Is needed to adjust the power level using the VGA because the received signal is strained by saturation of the quadrature mixer and the signal quality has been degraded.

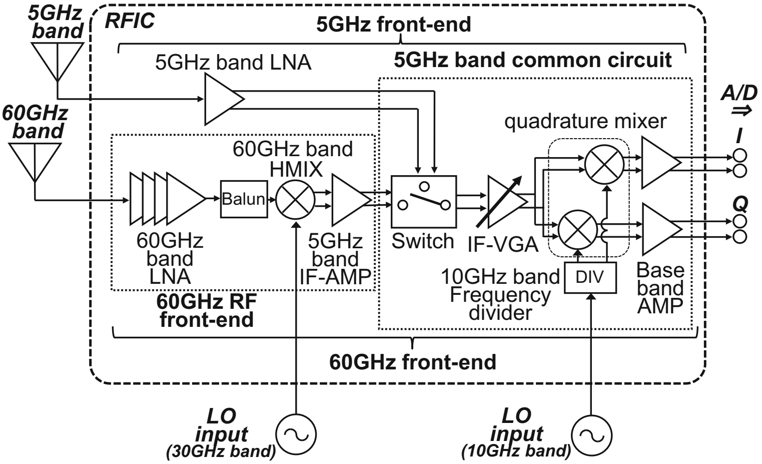


Fig. 7.40 Configuration of the 5 GHz/60 GHz receiver front-end IC

7.5.3 Circuit Components for the Multiband Receiver Front-End IC

60 GHz band LNA

A high gain LNA contributes to achieve a low-noise performance because it reduces influence of the subsequent stage in the circuit, such as the mixer. A cascode configuration [34, 35] is used for the high gain LNA. Figure 7.41 shows the configuration of an inductive matched cascode LNA (four-stage amplifier) [36, 37]. In high frequency band, capacitances of the field-effect transistors (FETs) reduce the gain of a cascode amplifier. To cancel out the capacitances of FETs [38], an inductor formed by the microstrip lines (MSL_{IS}) is connected in parallel to the interstage (node A_{1-4}) of the cascode LNA. The optimum inductance of MSL_{IS} was determined analytically in terms of the interstage matching of the cascode amplifier.

Figure 7.42 shows the simulation results of NF_{min} as a function of the gate width (Wg) of the FET. NF_{min} is the minimum of noise figure (NF) that can be obtained by input matching. The reduction of NF is enabled by reducing the parasitic resistance and capacitance on the gate of the FET. The simulated NF_{min} of the LNA

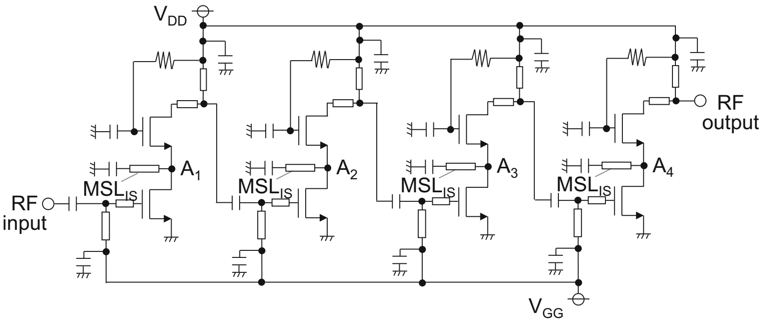
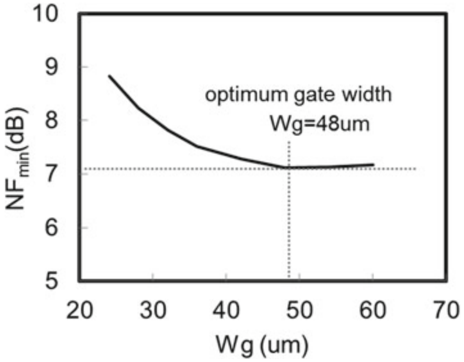


Fig. 7.41 Configuration of an inductive matched cascode LNA (4-stages amplifier)

Fig. 7.42 Simulation results of NF_{min} plotted against the gate width Wg of the FET as the variable



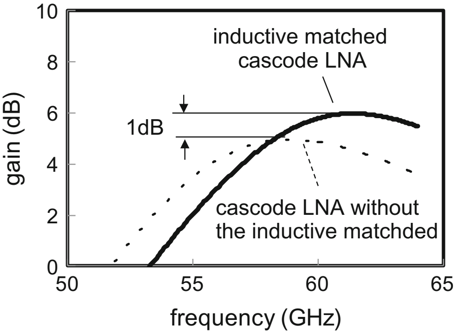


Fig. 7.43 Simulation results of the gain of a cascode LNA (1-stage amplifier) with inductive matching (solid line) and without inductive matching (broken line)

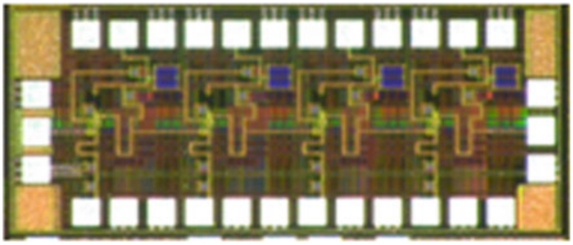


Fig. 7.44 Photograph of the fabricated 60 GHz band LNA (0.6 mm × 1.5 mm)

(1-stage amplifier) has an optimum at the gate width Wg of 48 μm. Figure 7.43 shows the simulation results of gain of the cascode LNA (1-stage amplifier) with and without inductive matching. The Wg of the FET in each LNA is 48 μm. The gain of the inductive matched cascode LNA is 1 dB higher than without inductive matching.

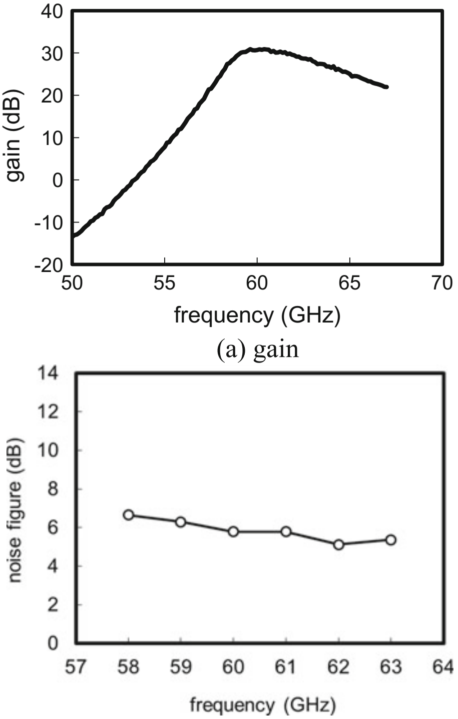
Figure 7.44 shows a photograph of the fabricated 60 GHz band LNA in 90 nm Complementary MOS (CMOS) technology. Figure 7.45 shows the measurement results of the fabricated 60 GHz band LNA. The bias conditions are V_{DD} = 1.2 V and I_{DD} = 5.6 mA at each stage. The fabricated LNA achieved a gain of 30.8 dB with an NF of 5.8 dB at 60 GHz. Output 1 dB Compression Point (OP_{1dB}) was −2.4 dBm.

60 GHz band HMIX

Figure 7.46 shows the configuration of the 60 GHz band HMIX [39]. The HMIX has two transistor pairs. Each transistor pair consists of two FETs which have a common drain and a common source.

The load TL_1 at the common source consists of a transmission line of which the length is a quarter of the RF wavelength. The input RF signal amplitude at the common source is kept large because of the high input impedance. In addition, the HMIX realizes high saturation characteristics for the RF input power because the transistor which is an active device is not used for the input circuits. The output load TL_2 at the common drain consists of a transmission line whose length is a quarter wavelength of the 2nd harmonic (2LO) of the Local Oscillator (LO).

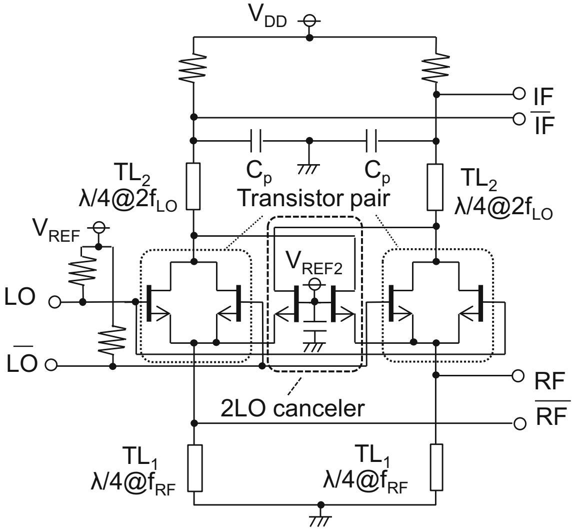
Fig. 7.45 Measurement results of the fabricated 60 GHz band LNA



(a) gain

(b) noise figure

Fig. 7.46 Configuration of the 60 GHz band HMIX



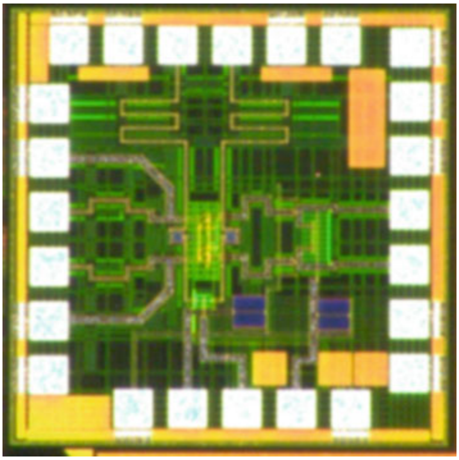


Fig. 7.47 Photograph of the fabricated HMIX (0.8 mm × 0.8 mm)

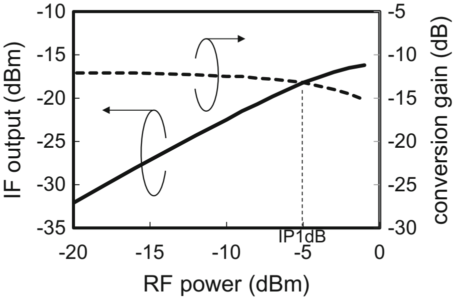


Fig. 7.48 Measurement results of the fabricated HMIX

The capacitance C_p is chosen to become a short circuit in the millimeter-wave band and an open circuit in the IF band. The leakage of the 2LO to IF band output circuit is reduced due to the high output impedance for the 2LO. In addition, the 2LO canceler circuit connected to the common drain suppresses the 2LO that occurs on a grand terminal and a power supply terminal for the influence of wire bonding.

Figure 7.47 shows a photograph of the fabricated HMIX in 90 nm CMOS technology. Figure 7.48 shows the measurement results of the fabricated HMIX. Supply voltage is $V_{DD} = 1.2$ V and the consumption power is 1.2 mW. RF is 60 GHz, IF is 5 GHz, and LO frequency is 27.5 GHz. The fabricated HMIX realized conversion gain of −12.7 dB, NF of 29.6 dB, and Input 1 dB Compression Point (IP_{1dB}) of −5 dBm at the LO power of 2 dBm.

5 GHz band IF-VGA

Figure 7.49 shows a configuration of the 5 GHz band IF-VGA. The IF-VGA comprises two-stage amplifiers [40]. The 1st VGA is a stacked differential circuit with a resistive output load. The 2nd VGA is also a stacked differential circuit with a reactive output load. 5 GHz band frequency characteristics of the IF-VGA are optimized by properly tuning the resistive and reactive loads. The current through

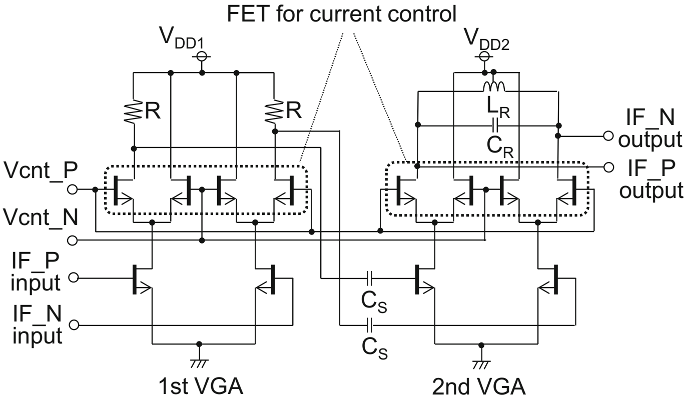


Fig. 7.49 Configuration of the 5 GHz band IF-VGA (bias circuit is not shown)

the load is controlled by the current-controlling FETs, thereby controlling the amplifier gain. The bias of the FETs of the input is approximately constant relatively high linearity.

Figure 7.50 shows a photograph of the fabricated IF-VGA in 90 nm CMOS technology. Figure 7.51 shows the measurement results of gain with respect to Vcnt_P of the IF-VGA. Supply voltage is V_{DD1} and V_{DD2} = 1.2 V and the consumption power is 21.7 mW. The fabricated IF-VGA realized the maximum gain of 10.9 dB and gain control range of 27 dB.

7.5.4 Flip-Chip Assembly

Figure 7.52 shows the upper metal conductor pattern on a substrate for the flip-chip assembled IC. Figure 7.53 shows a cross section view of the flip-chip assembled IC and the substrate. The millimeter-wave Si IC has a ground plane, which isolates the Si substrate from the lower metal layer, because the Si substrate has a large millimeter-wave loss. The ground plane and the lower metal forms a waveguide, which is coupled with the IC via holes and Au bumps. As frequency is increased, various spurious modes arise in the waveguide, degrading the performance of the IC.

Figure 7.54 shows the calculation results of cutoff frequency of the waveguide with respect to relative permittivity. The relative permittivity has to be less than 8 in order that the cutoff frequency of dominant mode is higher than 60 GHz. Figure 7.55 shows the simulation results of electric fields by HFSS (3D RF/Electromagnetic simulator). The substrate used in the simulation is alumina which has a relative permittivity ε_r of 9.9. The height of the substrate is 0.15 mm

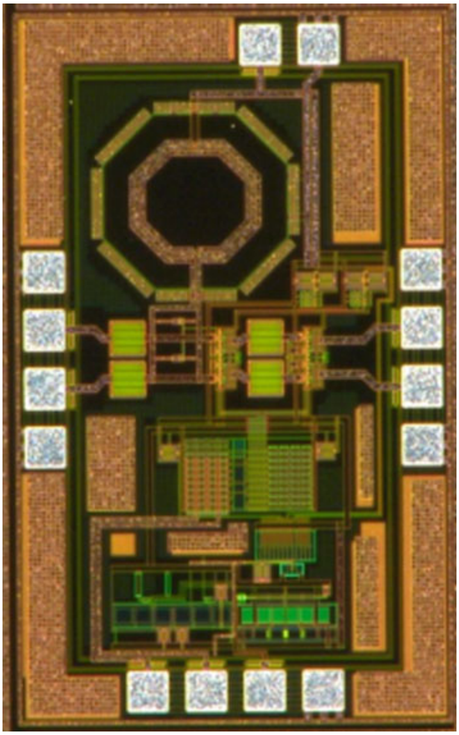


Fig. 7.50 Photograph of the fabricated IF-VGA (0.7 mm × 1.2 mm)

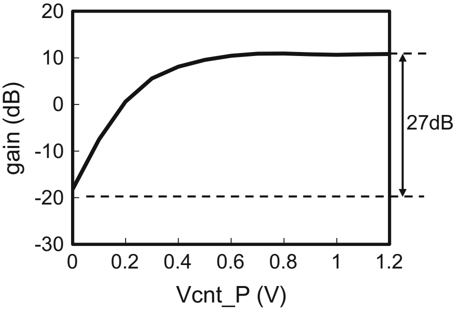


Fig. 7.51 Measurement results of gain with respect to Vcnt_P of the IF-VGA (Vcnt_N = 0 V)

and distance between the holes is 0.87 mm. Figure 7.55a shows the ground plane, but not the pattern of the transmission line on the flip-chip assembled IC. Figure 7.55b shows the simulated propagation of 60 GHz shown in the alumina waveguide.

Figure 7.56 shows a photograph of the flip-chip assembled 60 GHz band LNA. Ultrasonic vibration was used for flip-chip bonding with Au bumps, 30 μm high.

Fig. 7.52 Pattern on a substrate for the flip-chip assembled IC

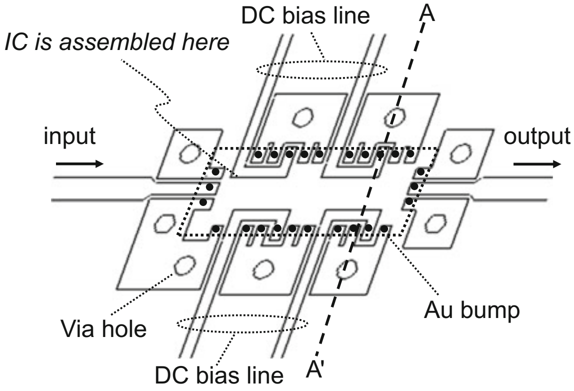


Fig. 7.53 Cross section view (A-A′) of the flip-chip assembled IC and the substrate

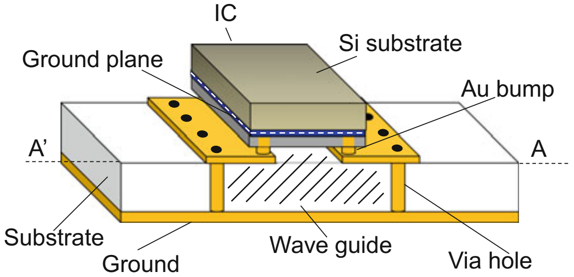


Fig. 7.54 Calculation results of cutoff frequency with respect to relative permittivity

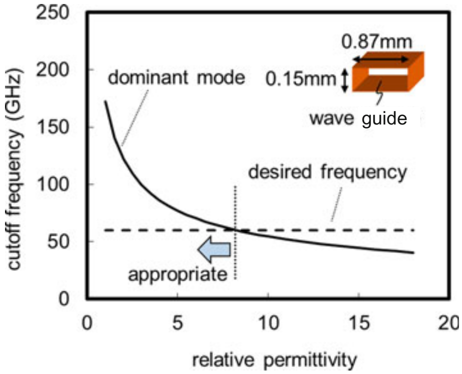
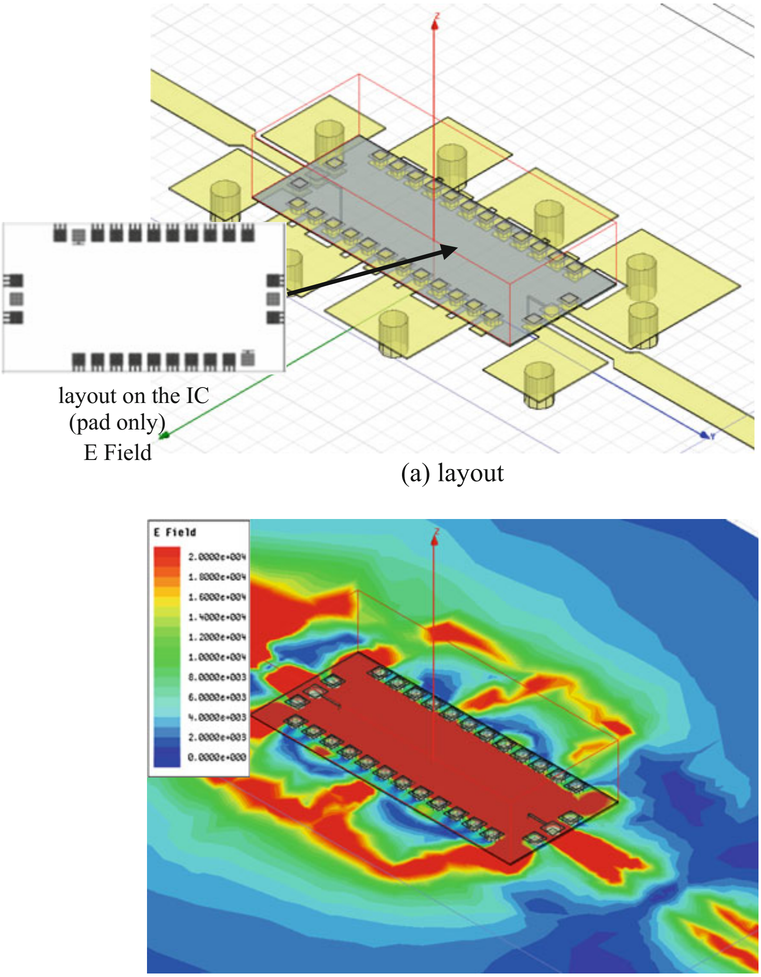


Figure 7.57 shows the measurement results of the flip-chip assembled 60 GHz band LNA. The flip-chip assembled LNA on an alumina substrate has spurious modes. On the other hand, the flip-chip assembled LNA on a resin substrate ($\varepsilon_r = 3.8$ at 1 GHz) has a gain of 31.1 dB without spurious mode. On-wafer probing gave a similar result.



(a) layout

(b) electric field at 60GHz: ε_r=9.9

Fig. 7.55 Simulation results of electric field

7.5.5 5 GHz/60 GHz Receiver Front-End IC

Figure 7.58 shows a photograph of the fabricated 5 GHz/60 GHz receiver front-end IC in 90 nm CMOS technology. Figure 7.59 shows a photograph of the flip-chip assembled 5 GHz/60 GHz receiver front-end IC on the resin substrate.

Figure 7.60 shows the measurement results of conversion gain and NF of the 60 GHz RF front-end including the 60 GHz band LNA, the HMIX, the balun and the 5 GHz band IF-AMP. The 60 GHz RF front-end realized conversion gain of 21.3 dB with NF of 7.2 dB at 60 GHz. A LO frequency and RF power are

Fig. 7.56 Photograph of the flip-chip assembled 60 GHz band LNA

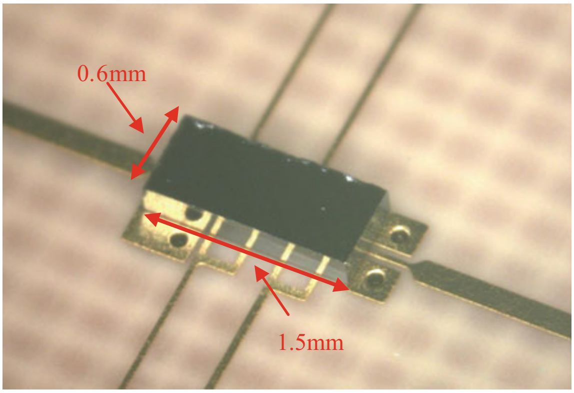


Fig. 7.57 Measurement results of the flip-chip assembled 60 GHz band LNA

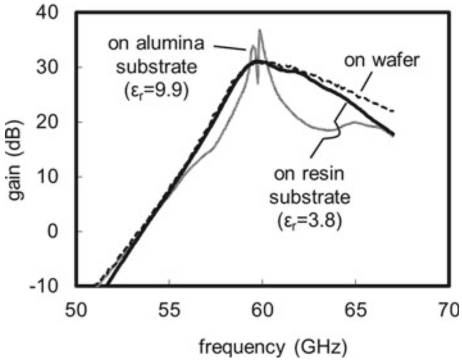


Fig. 7.58 Photograph of the fabricated 5 GHz/60 GHz receiver front-end IC (2.2 mm × 2.9 mm)

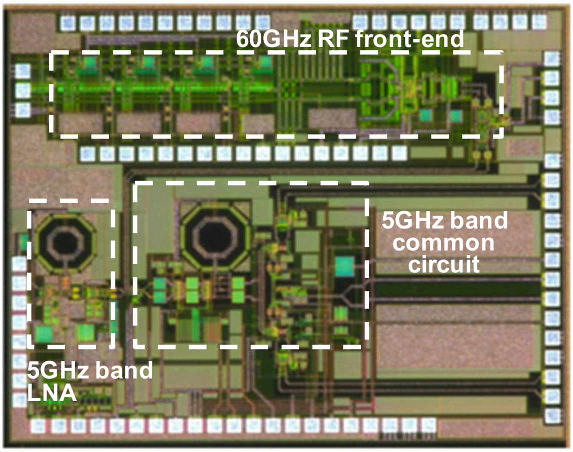


Fig. 7.59 Photograph of the flip-chip assembled 5 GHz/ 60 GHz receiver front-end IC

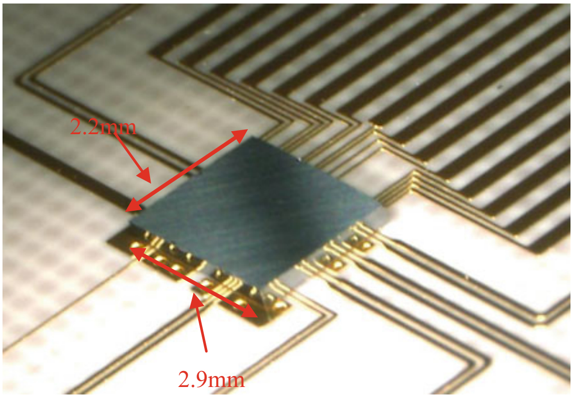


Fig. 7.60 Measurement results of conversion gain of the 60 GHz RF front-end

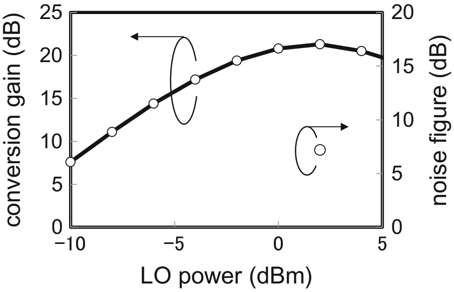
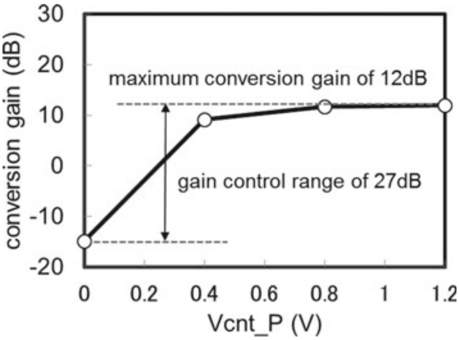


Fig. 7.61 Measurement results of conversion gain with respect to Vcnt_P of the 5 GHz common circuit (Vcnt_N = 0 V)



27.5 GHz and −40 dBm, respectively. Figure 7.61 shows the measurement results of conversion gain with respect to Vcnt_P of the 5 GHz common circuit. An IF frequency is 5.2 GHz, a baseband frequency is 10 MHz, a LO frequency (10 GHz band) is 10.4 GHz. The 5 GHz common circuit realized the maximum conversion gain of 12 dB and gain control range of 27 dB.

Table 7.3 shows the measurement results of the fabricated 5 GHz/60 GHz receiver front-end IC. The input and output port on resin substrate are directly connected with standard coaxial RF connector. The 5 GHz front-end realized conversion gain of

Table 7.3 Measurement results of the fabricated 5 GHz/60 GHz receiver front-end IC

Item	Unit	5 GHz front-end	60 GHz front-end
RE frequency	GHz	5.2	60.5
LO frequency (30 GHz band)	GHz	–	27.6
LO frequency (10 GHz band)	GHz	10.4	10.4
Baseband frequency	MHz	10	10
V_{DD}	V	1.2	1.2
I_{DD}	mA	78.5	105.8
Conversion gain (Vcnt_P = 1.2 V)	dB	32	32
Noise figure	dB	5	8
Output-P1 dB	dBm	−11.2	−12.5

32 dB with NF of 5 dB and the 60 GHz front-end realized conversion gain of 32 dB with NF of 8 dB.

7.5.6 Conclusions and Future Works

In this section, the flip-chip assembled 5 GHz/60 GHz receiver front-end IC in 90 nm CMOS technology was introduced for the multiple wireless system, such as described as the Dependable air.

The receiver front-end IC is switchable between the 5 GHz front-end and the 60 GHz front-end. The architecture of the receiver front-end IC is a direct conversion at 5 GHz band and a superheterodyne at 60 GHz band. The 5 and 60 GHz front-end share the VGA for adjustment of power level and the quadrature mixer.

The fabricated 5 GHz/60 GHz receiver front-end IC achieved conversion gain of 32 dB with NF of 5 dB at 5 GHz band and conversion gain of 32 dB with NF of 8 dB at 60 GHz band.

As the future works, in order to cope with a variety of communications applications, it can be applied to digital-assisted technology that can achieve high performance and high functionality with respect to the front-end IC [41].

7.6 Analog-to-Digital Converters for Versatile and Multiband Wireless Networks

Akira Matsuzawa, Tokyo Institute of Technology
Masaya Miyahara, High Energy Accelerator Research Organization

7.6.1 Analog-to-Digital Converters in Dependable Wireless Network Systems

The Analog-to-Digital Converter (ADC) is the most important analog circuit in many electrical systems. It sometimes determines the system performance and electrical power consumption. ADCs have usually been optimized for specific applications, which have often resulted in limited efficiency and versatility in design. In this Section we will describe the idea of the “dependable ADC” that can realize sufficient Signal to Noise Ratio (SNR) and conversion rate required for versatile wireless applications with lowest power and area. The design is robust against mismatch of components and scalable with advance in technology as well.

Figures 7.62 and 7.63 plot the SNR and the power dissipation, respectively, versus the signal bandwidth (BW) for recently published sigma-delta ADCs for wireless communications [42]. The SNR decreases with increasing BW as follows:

$$SNR\,(\mathrm{dB}) \approx SNR_0 - 10\log BW\,(\mathrm{Hz}), \tag{7.12}$$

where SNR_0 is the SNR at 1 Hz. This equation is very well reflected in the tendency seen in Fig. 7.62, which suggests that an ADC with an SNR of 62 dB at BW of 20 MHz can be built by using the oversampling method and digital filters. The power dissipation of the ADC is below 2.5 mW with a BW of 20 MHz, and is sufficiently low for conventional wireless standards with BW from 1 to 20 MHz.

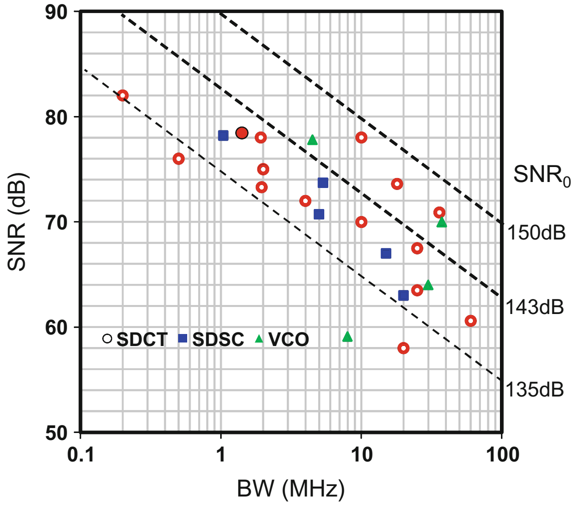


Fig. 7.62 SNR versus BW of ADCs for wireless systems (SDCT: sigma-delta continuous time ADC, SDSC: sigma-delta discrete time ADC, VCO: voltage controlled oscillator ADC)

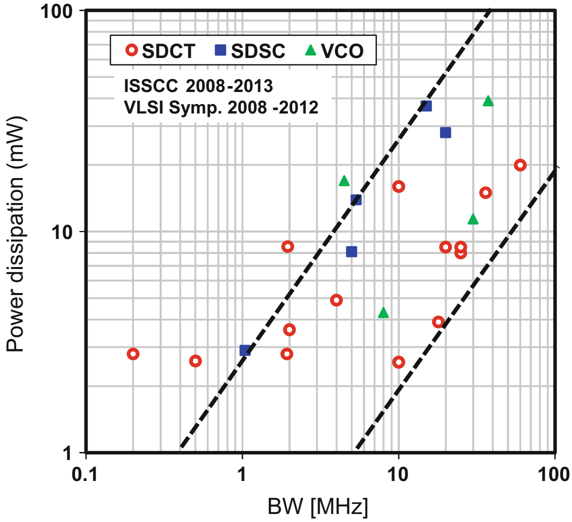


Fig. 7.63 Power dissipation versus BW of ADCs for wireless systems

7.6.2 *Design of Successive Approximation Register ADC*

It will be shown in this subsection that the Successive Approximation Register Analog-to-Digital Converter (SAR ADC) [43] using an internal capacitive Digital-to-Analog Converter (DAC), a dynamic comparator, and Successive Approximation Registers (SARs) is suitable for our current purpose. The two distinguished features of the present SAR ADC is that it has gotten rid of Op-Amps, which is not suitable for scaling, and that it has no static current flow. The ultra-low-power operation at the low conversion rate for ubiquitous sensors and bio-medical applications is becoming very important recently.

However, it has not been easy with the SAR ADC to achieve an SNR above 64 dB at the conversion rate over 50 MS/s with a low-power dissipation of a few mW. Figure 7.64 shows the developed SAR ADC. The Capacitance DAC (CDAC) depicted in Fig. 7.64 is single-ended for simplicity while the actual implementation uses a differential scheme [44]. A Metal Oxide Metal (MOM) capacitor between the interconnections is used to reduce the occupied area and parasitic capacitances and

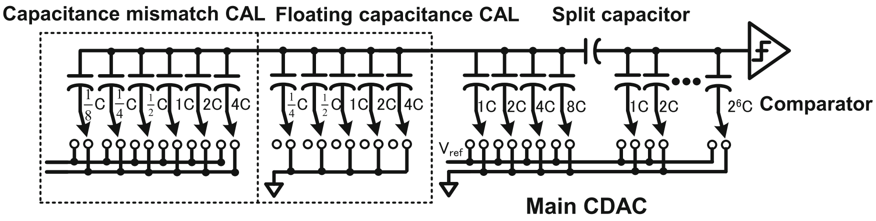


Fig. 7.64 CDAC in SAR ADC

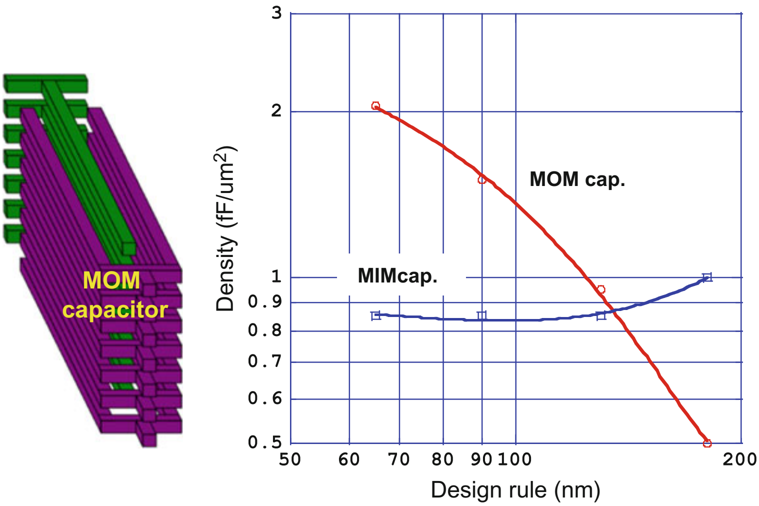
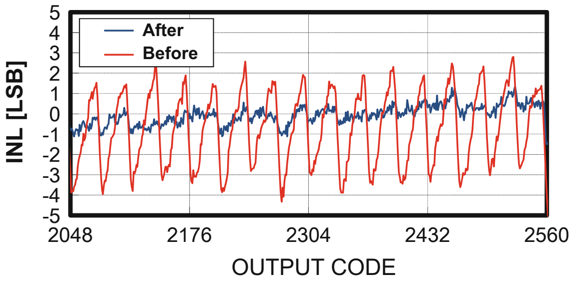


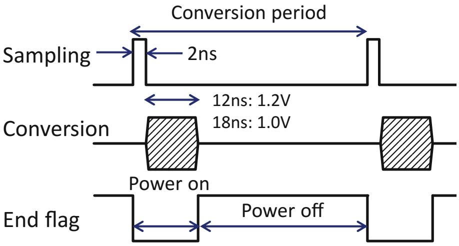
Fig. 7.65 Capacitance density versus design rule for MOM (metal oxide metal) and MIM (metal insulator metal) capacitors

Fig. 7.66 The internal noise level (INL) before and after the calibration correction for capacitances



to avoid the optional Si processes. Figure 7.65 shows the MOM capacitor and capacitance densities of the Metal Insulator Metal (MIM) and the MOM capacitors. The density of the MOM capacitor can be increased with the technology scaling and becomes higher than that of the MIM capacitor when the technology is lower than 0.13 μm. In contrast, the density of the MIM capacitor is almost constant with the technology scaling. A split CDAC is used to reduce the occupied area; however, it may cause nonlinearity error. We addressed this issue by using adjustable floating capacitances. Figure 7.66 shows the effect of the calibration correction for the parasitic capacitance. A large Integral Nonlinearity (INL) error of about 5 LSB before correction has been suppressed to 1 LSB. The thermal noise is another factor that reduces the SNR. The kT/C noise is stored in the sampling phase and 2 pF is selected as the sampling capacitor. Also, a low-noise dynamic comparator, proposed in [45], is used with a relatively large load capacitance of 0.5 pF to suppress the thermal noise. The self-clocking method is implemented to realize a high-speed

Fig. 7.67 Timing chart



and low-power operation, as well as to realize the clock-scalable operation. Figure 7.67 shows the timing chart of the ADC. Only the sampling pulse is required to initiate the analog-to-digital conversion. After the sampling pulse goes down, the bit-cycle action is started by the self-clocking method. The end flag becomes high when the conversion is finished and it can be used for the power off switch to cutoff the leakage current.

7.6.3 Measurement Result

The SAR ADC has been fabricated in 65 nm CMOS process. Figure 7.68 shows the layout of developed ADC. The height of the ADC is suppressed to 70 µm for future development of interleaved ADC to increase the conversion rate. The occupied area is only 0.03 mm^2. Figure 7.69 shows the measured power dissipation versus sampling frequency for several operating voltages. It can be operated with a low V_{DD} of 0.8 V and attains a very high conversion rate of 70 MS/s with a V_{DD} of 1.2 V. Low-power dissipation of 2.2 mW at 50 MS/s with a V_{DD} of 1.0 V is achieved. The consumed power is proportional to the conversion rate perfectly. The Signal-to-Noise and Distortion Ratio (SNDR) of 60 dB is obtained at the input signal frequency of 20 MHz with a V_{DD} of 1.0 V. Table 7.4 summarizes the performance and other 12 bit SAR ADCs [46, 47]. The Figure of Merit (FoM) compares favorably for the present device than others under a V_{DD} of 1.2 V. A very low DC FoM of 28 fJ/conv. has been achieved. The highest conversion rate of 70 MS/s, the lowest power dissipation of 2.2 mW, and the smallest occupied area of 0.03 mm^2 have been achieved.

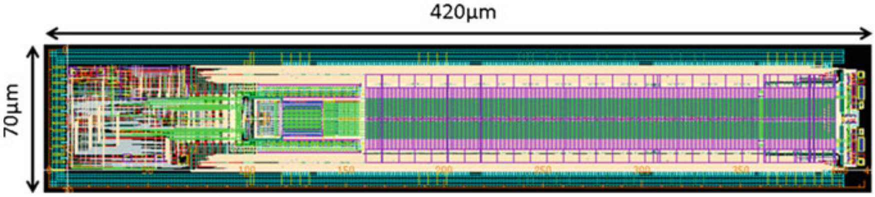


Fig. 7.68 Chip micro-photograph

Fig. 7.69 Power dissipation versus sampling frequency

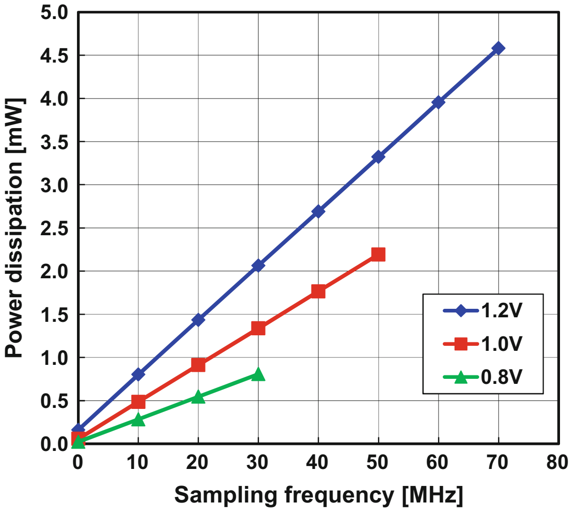


Table 7.4 Performance summary and comparison

	This work			Miyahara et al. [45]	Liu et al. [46]
Resolution (bit)	12			12	12
V_{DD} (V)	0.8	1.0	1.2	1.2	1.2
fsample (MHz)	30.0	50.0	70.0	45.0	50.0
Pdissipation (mW)	0.8	2.2	4.6	3.0	4.2
SNDR (dB)	62.0	64.0	65.0	67.0	71.0
FoM (fJ) Nyq/DC	81/28	62/33	100/45	36/31	36/29
Technology (nm)	65			130	90
Occupied area (mm^2)	0.03			0.06	0.1

$FoM \equiv \frac{Power\ dissipation}{Sampling\ frequency \times 2^{ENOB}}$ (ENOB: effective number of bit)

The ADC can attain the SNR of 62 dB at BW of 20 MHz and 78 dB at BW of 1 MHz, as shown in Fig. 7.70. These SNR values are sufficiently high for the conventional wireless applications. Furthermore, we can increase the SNR up to 84 dB when a higher oversampling rate is used with Dynamic Element Matching (DEM) or dither method [47]. Also we can increase the BW by using the interleaving method. Figure 7.71 shows the measured power dissipation when using the oversampling method. It is seen that this SAR ADC can keep the small power dissipation, lower than other sigma-delta ADCs, in oversampling operation. Also further reduction in power dissipation is possible by using optimizing the V_{DD}.

Fig. 7.70 SNR versus BW of the dependable ADC (solid circles) compared with other ADCs

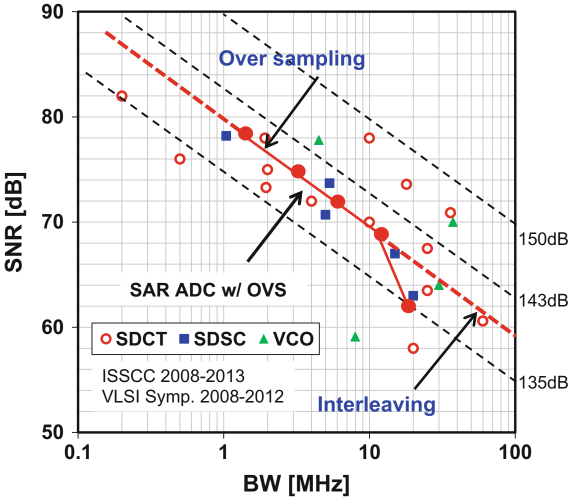
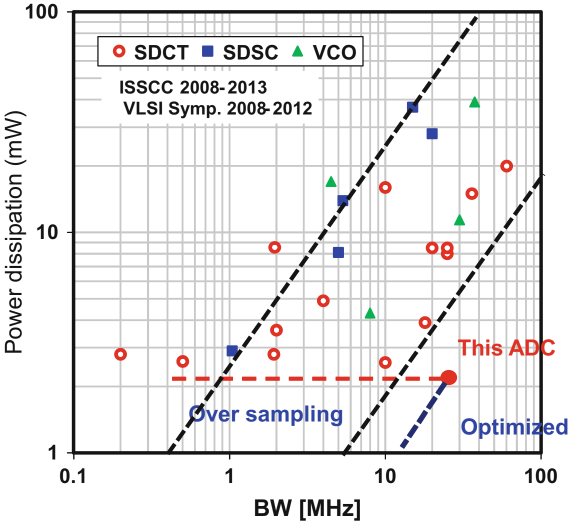


Fig. 7.71 Power dissipation versus BW of the dependable ADC in comparison with other reports



7.6.4 *Discussions and Further Investigations*

A SAR ADC has been developed to realize a dependable ADC that has frequency, performance, and power scalable characteristics with very low-power dissipation and small area in scaled mixed-signal CMOS technology. The fabricated SAR 12 bit ADC in 65 nm CMOS occupies a small area of 0.03 mm^2 and demonstrates low-power dissipations of 2.2/4.6 mW at high conversion rates of 50/70 MS/s.

It also achieves very low DC FoMs of 28/33 fJ/conv with V_{DD} of 0.8/1.0 V. The SNDR is 64 dB and can be increased to 78 dB by the oversampling method.

The measured results support our basic idea of the dependable ADC, as a key element in future wireless interface. It operates with a low voltage of 0.8 V and it is suitable for the scaled CMOS technology. It can cover the wide performance range of SNR and signal bandwidth with the smallest power and occupied area. Therefore, the developed dependable ADC increases the design efficiency and versatility for many applications.

Higher SNDR of over the 78 dB and higher conversion rate of over the 70 MS/s are the next target to cover the higher dynamic range and wider bandwidth for more versatile and multiband wireless systems. The use of DEM or dither method and interleaving technique should be investigated.

7.7 Multimode Frequency Domain Equalizer for Heterogeneous Wireless Systems

Kazuo Tsubouchi, Tohoku University
Suguru Kameda, Tohoku University
Noriharu Suematsu, Tohoku University
Tadashi Takagi, Tohoku University
Makoto Iwata, Kochi University of Technology

7.7.1 Multimode Receiver for Heterogeneous Wireless Systems

Recently, the demand for broadband services involving wireless communication systems has increased tremendously. However, wireless systems have a tradeoff relationship between the bit rate and the coverage area owing to the limited output power of the transmitter. Since the coverage area of a signal with a high throughput is smaller, it is difficult to satisfy the requirement for wide coverage and a high throughput only with one wireless communication system. One of the methods for solving this problem is to use a heterogeneous wireless system, that integrates multiple wireless air interfaces, one of which is adaptively selected according to the propagation environment or the user's needs. Thus, a heterogeneous wireless system can support a high throughput and wide coverage.

One of the key devices used to realize heterogeneous wireless systems is a multimode receiver. In a heterogeneous wireless system, the multimode receiver should be able to demodulate the signals of multiple systems, estimate the propagation environments of each one of the multiple systems, and optimally switch to the best system for communication. In this section, we focus on the frequency domain equalizer (FDE) of a multimode receiver. Frequency domain equalization is required to compensate for the distortion of a signal by a frequency-selective channel. In [48, 49], the effect of a single-carrier (SC) FDE was shown by computer simulation. In our previous studies, an SC-FDE receiver was implemented on a field-programmable gate array (FPGA) [50, 51], and an application-specific integrated circuit (ASIC) chip for a SC-FDE was implemented [12, 32, 52].

In this section, a frequency-selective channel is first described. This channel is one of the main issues in mobile communication systems. To resolve this issue, an FDE technique is used. Next, an ASIC chip for a multimode FDE will be described. To apply a multimode FDE to each system, it is necessary to mount the FDE in a multimode receiver suitable for multiple wireless systems. The multimode FDE is used for the demodulation of both SC and multicarrier (MC) signals and optimally switches the weight calculation according to the system.

7.7.2 Frequency-Selective Channel

As previously stated, a mobile radio channel is composed of many propagation paths with different time delays. As the data transmission rate increases, the duration of each symbol becomes much shorter. This means that the delays of signals arriving via different paths become much larger relative to the symbol length, with the delay sometimes reaching tens of symbols, leading to significant intersymbol interference (ISI), which greatly degrades the system performance. Understanding the mechanism of the mobile radio channel and the degradation of performance is very important for designing systems that can overcome these channel impairments. A mathematical model of a broadband radio channel is given in this section.

A multipath fading channel can be thought of as a time variant filter. Its impulse response $h(\tau, t)$ is described by Eq. 7.13, where L is the number of paths and h_l and τ_l are the complex gain and delay of each path, respectively.

$$h(\tau, t) = \sum_{l=0}^{L-1} h_l(t)\delta(t - \tau_l) \tag{7.13}$$

An equivalent description of a time-dispersive channel is obtained by applying the Fourier transform to the channel impulse response, yielding the channel transfer function given by Eq. 7.14. This equation demonstrates that a time-dispersive channel is also frequency-selective.

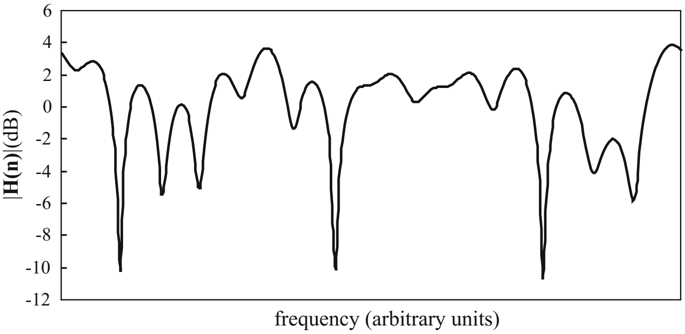


Fig. 7.72 Amplitude of channel transfer function

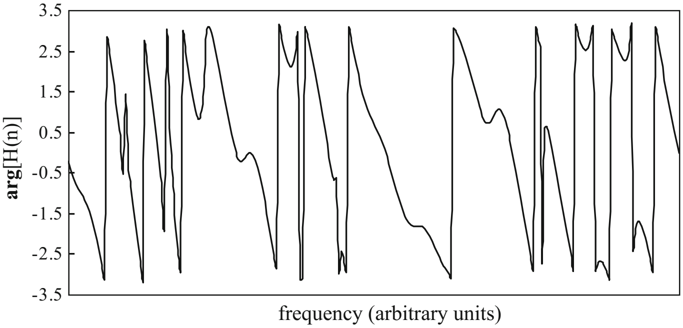


Fig. 7.73 Phase of channel transfer function

$$H(f,t)=\sum_{l=0}^{L-1}h_l(t)\exp(-j2\pi f\tau_l) \tag{7.14}$$

The amplitudes of this function exhibit large variations (fades) with respect to both time and frequency. $H(f,t)$ can be seen as the vector sum of all paths with complex gain $h_l(t)$. As the amplitudes and phases of these paths vary rapidly, this vector sum also changes its value. Because of the large variations in the amplitude of the channel transfer function in the frequency domain, the channel is called a frequency-selective channel. For a more intuitive understanding, the amplitude and phase of a channel transfer function are shown in Figs. 7.72 and 7.73, respectively.

As can be seen in Fig. 7.72, the channel transfer function exhibits some very deep fades, which distort the received signal, inducing difficulties in the recovery of the transmit signal.

Understanding how a signal is distorted when it is transmitted through a frequency-selective channel is important for finding ways to mitigate such distortion. A mathematical expression for a received signal under such conditions is next given. Here a discrete representation is assumed.

As previously stated, the channel can be viewed as a time variant filter; therefore, the received signal $r(t)$ can be described as the convolution of the transmitted signal $s(t)$ and the filter impulse response h_l as

$$r(t) = \sum_{l=0}^{L-1} h_l s(t - \tau_l) + n(t), \tag{7.15}$$

where $n(t)$ is noise. Through the Fourier transform of this equation, the following expression for the received signal in the frequency domain $R(n)$ can be obtained:

$$R(n) = \sum_{t=0}^{N-1} r(t)\exp(-j2\pi n\frac{t}{N_c}) \tag{7.16}$$

$$= S(n)H(n) + N(n), \tag{7.17}$$

where $S(n)$ is the spectrum of $s(t)$ at the n th frequency component and $N(n)$ is the noise spectrum. This equation is very important as it is one of the basic principles for an FDE, which will be introduced in the next section.

7.7.3 Design and Implementation of Multimode FDE

7.7.3.1 Single-Mode FDE

First, for easy understanding, the single-mode FDE block diagram [52] is explained. Figure 7.74 shows the block diagram of a single-mode SC-FDE transmitter. In the transmitter, a pilot $p(t)$ is inserted in the front of the packet as illustrated in Fig. 7.75. For a pilot signal, a Chu sequence [53] is used because it has constant amplitudes in both the time and frequency domains. The data $r(t)$ are divided into N-symbol blocks. A guard interval (GI) is added to each block by copying the last N_g symbols. A root-raised cosine (RRC) filter is used in both the transmitter and receiver to form a raised cosine (RC) filter.

Figure 7.76 shows the block diagram of the SC-FDE receiver. After removing the GI, the received signal $r(t)$ is transformed to the frequency domain signal $R(n)$ through the fast Fourier transform (FFT). A single-tap data equalizer is applied to the signal $R(n)$ as an equalized signal,

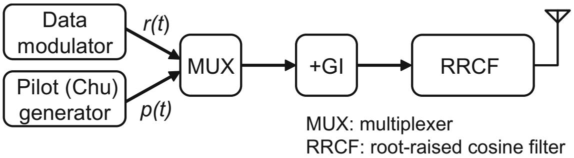


Fig. 7.74 Block diagram of SC-FDE transmitter

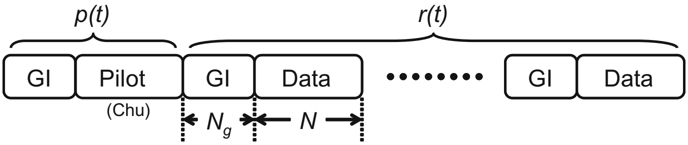


Fig. 7.75 Packet structure

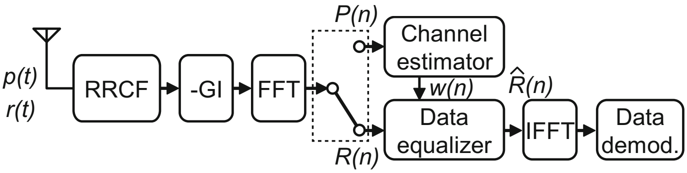


Fig. 7.76 Block diagram of SC-FDE receiver

$$\hat{R}(n) = w(n)R(n), \tag{7.18}$$

where

$$w(n) = \frac{\hat{H}^*(n)}{|\hat{H}(n)|^2 + \sigma^2} \tag{7.19}$$

is the minimum mean square error (MMSE) equalization weight [54], $\hat{H}(n)$ is the nth frequency component of the estimated channel transfer function, and $(\cdot)^*$ and σ^2 denote the complex conjugate and noise power, respectively.

$\hat{H}(n)$ and σ^2 are estimated using the received pilot $p(t)$. The adopted channel estimation technique is given in [55]. The block diagram of the channel estimator is shown in Fig. 7.77. When the pilot signal $p(t)$ is received, after applying the FFT

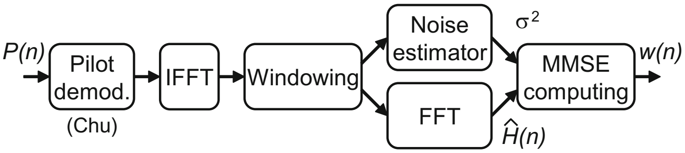
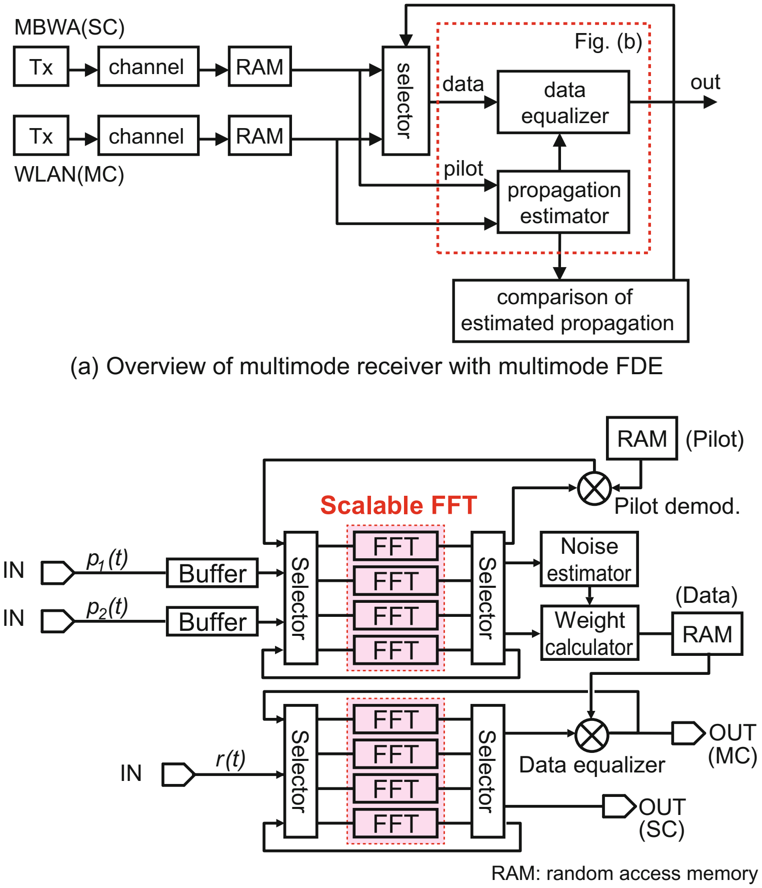


Fig. 7.77 Block diagram of channel estimator

operator, the pilot $P(n)$ is demodulated to obtain an estimate of the channel transfer function. To reduce the influence of noise, a delay-time domain windowing function is used [56]. The inverse FFT (IFFT) is applied to the channel transfer function to obtain the channel impulse response and the outside part of the GI is replaced with zeros. By applying another FFT, an improved estimate of the channel transfer function $\hat{H}(n)$ is obtained. The noise power σ^2 is estimated as in [57] by using the outside part of the GI from the channel impulse response. Finally, the estimated $\hat{H}(n)$ and σ^2 are used to compute $w(n)$.



(a) Overview of multimode receiver with multimode FDE

(b) Block diagram of multimode FDE

Fig. 7.78 Multimode receiver with multimode FDE

7.7.3.2 Multimode FDE

Next we give an overview of adaptive switching between two wireless systems using a multimode FDE. Figure 7.78a shows an overview of the multimode receiver with a multimode FDE. The multimode receiver has two input ports. The two input ports receive the pilot signal which was transmitted to each receiver through a propagation channel. First, the two pilot signals are inputted into the propagation estimator in the multimode FDE. The propagation environments estimated from the pilot signals of each wireless system are compared. In this section, the channel transfer function in the frequency domain was used as the propagation environment. The multimode FDE performs equalization and demodulation on the data transmitted from the system with the superior propagation environment. The optimal wireless system for communication is chosen by the above flow. Since the propagation environment changes, it is necessary to periodically estimate and compare the propagation environments using the pilot signal.

Figure 7.78b shows the block diagram of the multimode FDE. The multimode FDE is able to receive SC and MC signals because there is a feedback path after the data equalizer. The multimode FDE has two input ports for pilot signals and one input port for data signals. To enable parallel signal processing for channel estimation and data compensation, there are two scalable FFT blocks. The FFT block with a reorder function is able to operate as an IFFT block. Each FFT/IFFT block has four 64-point FFTs. The FFT/IFFT blocks are also able to operate either as two 128-point FFTs or one 256-point FFT. The weight calculator has MMSE and zero-forcing (ZF) functions.

Figure 7.79 shows the chip layout of a multimode FDE ASIC. For the ASIC implementation of the multimode FDE, a 180 nm complementary metal oxide

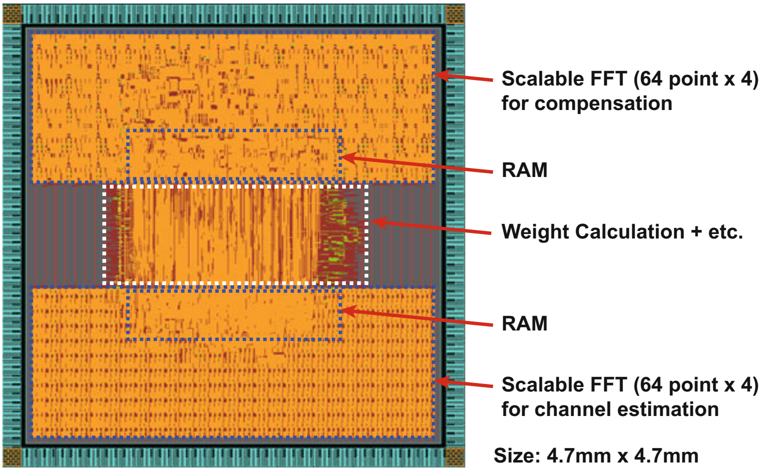

Scalable FFT (64 point x 4)
for compensation
RAM
Weight Calculation + etc.
RAM
Scalable FFT (64 point x 4)
for channel estimation
Size: 4.7mm x 4.7mm

Fig. 7.79 Chip layout of multimode FDE ASIC

semiconductor (CMOS) process was used. The die and core sizes of the multimode FDE chip are 22.1 and 17.6 mm^2, respectively. The implemented multimode FDE ASIC operates 48.1 Mbit/s at 100 Msample/s with 660 mW power consumption.

7.7.4 Evaluation of Multimode FDE ASIC

The implemented multimode FDE ASIC is equipped with channel estimation and data equalization functions only as shown in Fig. 7.78b. In this evaluation, insufficient functions for the evaluation are substituted with a MATLAB simulator and an FPGA chip. Figure 7.80 shows an evaluation block of the multimode FDE ASIC. Figure 7.81 shows a photograph of the evaluation board for the multimode FDE ASIC. The MATLAB simulator simulates a transmitter, a radio propagation channel with additive white Gaussian noise (AWGN), and an analog-to-digital converter (A/D). The MATLAB simulation result is stored on the FPGA chip. The stored data are sent to the ASIC and equalized in the ASIC. The equalized data are then stored in a personal computer (PC) to compute the bit error rate (BER).

The chip was evaluated in a wide-area cellular environment with multipath fading. Table 7.5 shows the specifications of the measurement system. A four-path uniform-power Rayleigh fading channel model was used. All the paths arrive within the GI.

Figure 7.82 shows the BER performance in the SC-FDE mode with the MMSE method. In the RRC filter, the roll-off factor α is 0.2. In this case, the implemented multimode FDE ASIC operates 12.5 Mbit/s at 100 Msample/s because of the large FFT/IFFT size. At a BER of 10^{-3}, the degradation of E_b/N_0 from the simulation was 1 dB. The degradation of E_b/N_0 mainly originated from the quantization error in ASIC implementation.

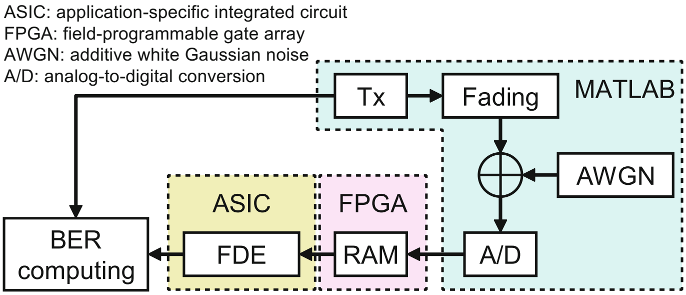

ASIC: application-specific integrated circuit
FPGA: field-programmable gate array
AWGN: additive white Gaussian noise
A/D: analog-to-digital conversion
Tx
Fading
MATLAB
AWGN
ASIC
FPGA
BER computing
FDE
RAM
A/D

Fig. 7.80 Evaluation block of multimode FDE ASIC

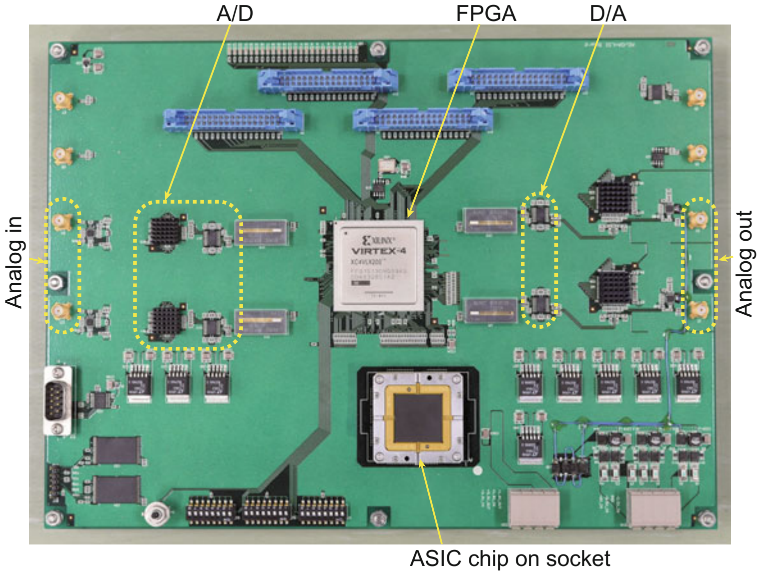


Fig. 7.81 Evaluation board for multimode FDE ASIC

Table 7.5 Specifications of measurement system

Transmission scheme	SC-FDE, OFDM (MC)
Equalization criteria	MMSE, ZF
Modulation	Quadrature phase shift keying (QPSK)
Bit number of A/D	10 bit
Frame composition	Pilot 1 block + data 7 blocks
# of FFT points	256
GI length	32 symbols
Channel model	Uniform 4-path quasi-static Rayleigh fading
Frame and symbol synchronicity	Ideal
Automatic gain control (AGC)	Ideal
Evaluation item	BER

Figure 7.83 shows the BER performance in the orthogonal frequency-division multiplexing (OFDM) mode with the ZF method. The implemented multimode FDE ASIC operates 12.5 Mbit/s at 100 Msample/s in this case. At a BER of 10^{-3}, the degradation of E_b/N_0 from the simulation was less than 1 dB. As a result, the multimode FDE can be implemented on the ASIC with 1 dB performance degradation.

Fig. 7.82 BER performance in SC-FDE mode with MMSE

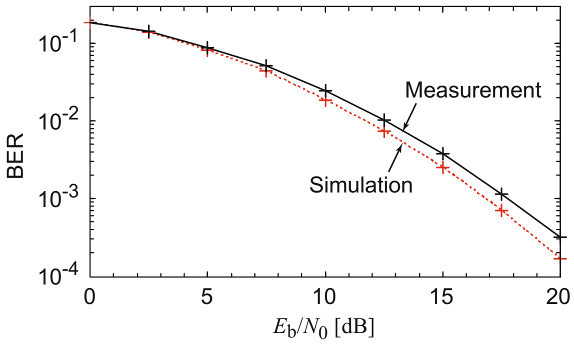
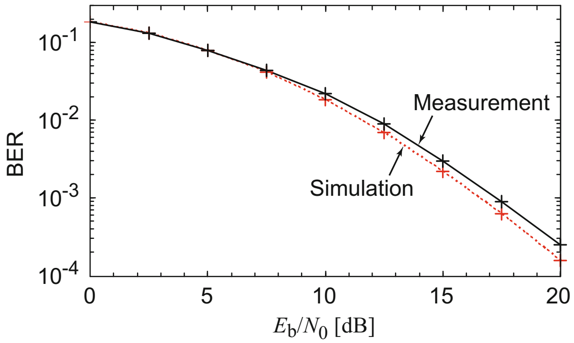


Fig. 7.83 BER performance in OFDM mode with ZF



7.7.5 Conclusions and Future Works

In this section, a multimode FDE was discussed as one of the key solutions of the Dependable Wireless System. A multimode FDE ASIC was designed and implemented using a 180 nm CMOS process and the performance of the multimode FDE ASIC was evaluated. The die and core sizes of the multimode FDE chip were 22.1 and 17.6 mm^2, respectively. The implemented multimode FDE ASIC operated 48.1 Mbit/s at 100 Msample/s with 660 mW power consumption. Under a four-path uniform-power Rayleigh fading channel condition, the multimode FDE can be implemented on the ASIC with 1 dB performance degradation at a BER of 10^{-3}. The proposed multimode FDE ASIC design has the potential for use in the Dependable Wireless System.

Future works are as follows: (1) ASIC implementation by using more fine CMOS processes to realize low power consumption, a small size, and high frequency, (2) transceiver implementation with RF/analog circuits using the developed ASIC, and (3) algorithm implementation for a wireless system selector by using the estimated propagation.

7.8 Network Technology for Heterogeneous Wireless Systems

Suguru Kameda, Tohoku University
Fumihiro Yamagata, National Institute of Technology, Kushiro College
Noboru Izuka, National Institute of Technology, Suzuka College
Hiroshi Oguma National Institute of Technology, Toyama College
Noriharu Suematsu, Tohoku University
Tadashi Takagi, Tohoku University
Kazuo Tsubouchi, Tohoku University

7.8.1 Coverage Problem of Mobile Networks

First, a coverage problem in present homogeneous mobile broadband wireless access (MBWA) networks is discussed. To clarify the problem, coverage estimates for an uplink 64 quadrature amplitude modulation (QAM) signal based on the received signal level measured in a field trial [58–63] are shown under different bandwidth conditions. We have reported on a MBWA system field trial with Fast Low-latency Access with Seamless Handoff Orthogonal Frequency-Division Multiplexing (FLASH-OFDM), which was carried out at Sendai city in Japan [58–63]. The following figures are based on the field trial.

Figure 7.84 shows the estimated coverage area of an uplink 64 QAM signal with an output power of 23 dBm when the signal bandwidth is 1.28 MHz. This figure shows that the estimated coverage is approximately 300 m. Figure 7.85 shows the estimated coverage area when the signal bandwidth is 5.12 MHz under the same terminal output power as in Fig. 7.84. These figures show that the quad bandwidth condition yields a narrower coverage area. The 64 QAM coverage area is almost disappears when the signal bandwidth is 5.12 MHz, and 64 QAM has no coverage area when the signal bandwidths are 10.24 and 20.48 MHz. The above results show that high-level modulation, which yields high throughput, can only be used in the area close to the base station (BS). The results are generalized as follows. The maximum throughput is increased with increasing signal bandwidth; however, the coverage area of the signal with maximum throughput is narrowed. We consider that all homogeneous wireless data communication networks with the traditional cellular configuration have this problem since the signal bandwidth, coverage, and throughput are common basic parameters in the networks.

Next, we discuss a proposed heterogeneous wireless communication network using multiple air interfaces that solves the coverage problem. Figure 7.86 shows the simplified service areas of a conventional homogeneous MBWA network and the proposed heterogeneous network with MBWA and wireless local area network (WLAN) air interfaces. The high-throughput area is limited to the cell center in the homogeneous network. In contrast, high-throughput areas away from the cell center

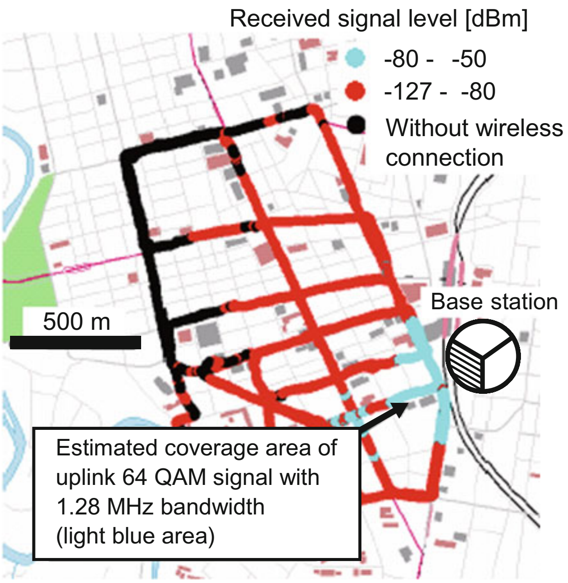

Received signal level [dBm]
● -80 - -50
● -127 - -80
● Without wireless connection
Base station
500 m
Estimated coverage area of uplink 64 QAM signal with 1.28 MHz bandwidth (light blue area)

Fig. 7.84 Estimated coverage area of uplink 64 QAM signal with 1.28 MHz bandwidth. This figure is based on the received signal level measured in a field trial [58–63]. The light blue area (received signal level of over −80 dBm) is the estimated coverage area

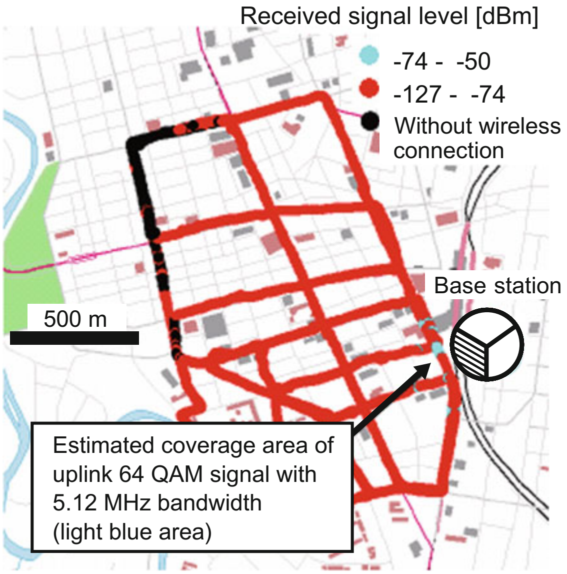
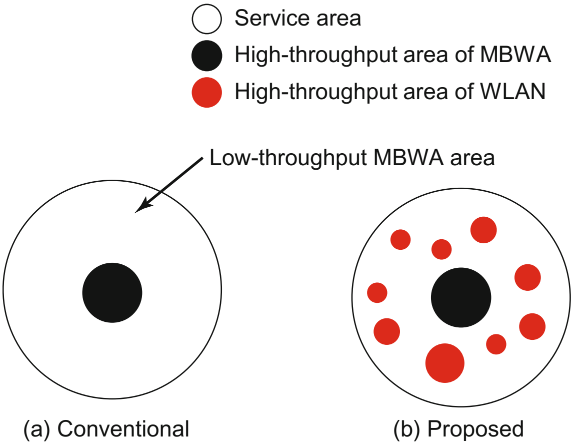

Received signal level [dBm]
● -74 - -50
● -127 - -74
● Without wireless connection
Base station
500 m
Estimated coverage area of uplink 64 QAM signal with 5.12 MHz bandwidth (light blue area)

Fig. 7.85 Estimated coverage area of uplink 64 QAM signal with 5.12 MHz bandwidth. This figure is based on the received signal level measured in a field trial [58–63]. The light blue area (received signal level of over −74 dBm) is the estimated coverage area

are provided by the WLAN air interface in the proposed network. This means that the proposed heterogeneous network attains a wider service area with high throughput than that in the conventional homogeneous network. The other service areas are provided by the MBWA air interface with relatively low throughput.

Fig. 7.86 Simplified service areas of conventional homogeneous network (**a**) and proposed heterogeneous network (**b**)



To provide a wireless data communication service with higher throughput and a wide coverage area to users of the proposed network, we have proposed two schemes: (1) a seamless system handover scheme for a heterogeneous wireless network [64, 65] and (2) a hybrid single-carrier and multicarrier technology [66–68].

7.8.2 Seamless System Handover for Heterogeneous Wireless Network

This section describes the proposed system handover scheme in a heterogeneous wireless network [64, 65]. Seamless handover is required between wireless networks with different air interfaces. An application-layer soft handover scheme, which is an essential part of the proposed network, is described in this section.

7.8.2.1 Overview of Proposed Handover Scheme

In the proposed scheme, the mobile terminal (MT) has a wide coverage air interface such as an MBWA and a high-throughput air interface such as a WLAN. Each air interface has a different physical layer, data link layer, and internet protocol (IP) layer. All handover functions are implemented in the application layer.

Figure 7.87 illustrates the proposed handover scheme. The MT has multiple wireless communication cards. Each communication card independently establishes wireless links with the BS and the access point (AP). The M T selects an appropriate air interface from the two interfaces. In the field trial, the simple selection rule that the MT preferentially selects the WLAN was adopted. The content server selects the transmission route requested by the MT and transmits data packets along the route.

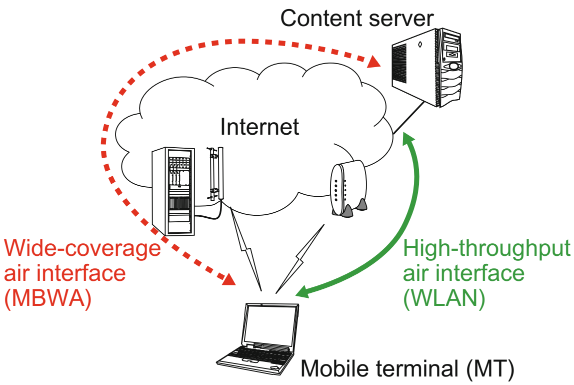


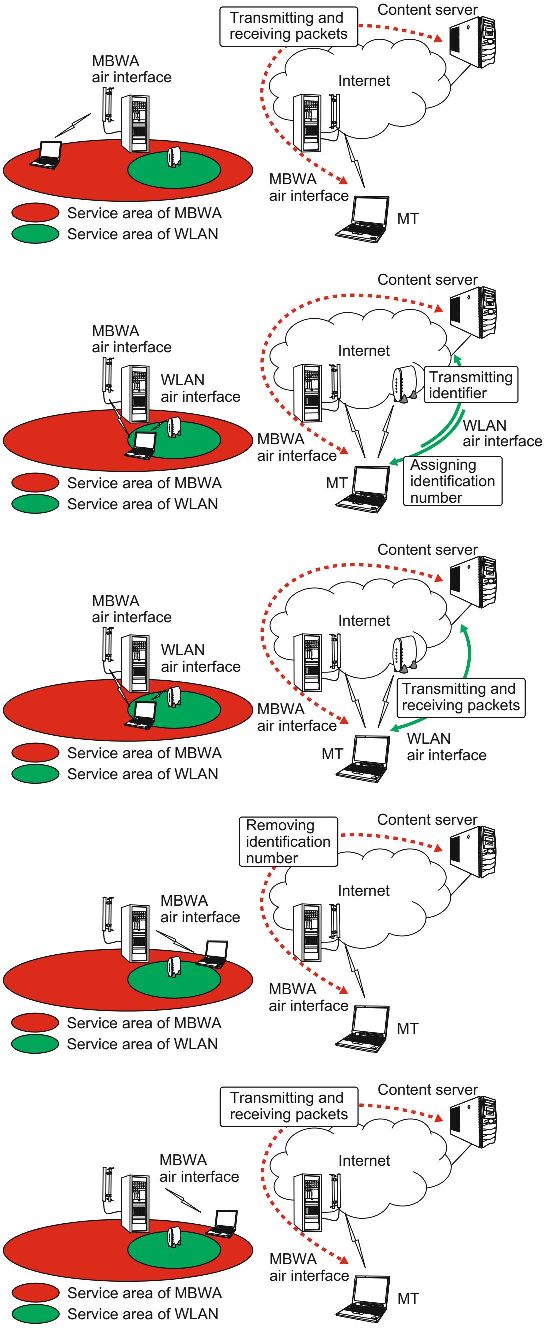
Fig. 7.87 Proposed handover scheme. In the conventional scheme, a user of a mobile terminal (MT) select connection system by manual operation for optimal system selection. In the proposed scheme, a MT evaluates channel conditions of MBWA and WLAN, and chooses connection system automatically

7.8.2.2 Handover Procedure

The proposed handover procedure is as follows. As an example, the handover procedure is discussed for the case that an MT moving in the service area of a wide coverage air interface, such as that used in an MBWA network, moves across the service area of a high-throughput air interface such as that of a WLAN. Figure 7.88a shows the MT outside the WLAN service area. The MT establishes a communication link with the content server using the MBWA air interface. When the communication link is established, the content server assigns a unique identifier and identification number to the MT, which are used by the server to identify the terminal. After the identification is completed, the server communicates with the terminal using the MBWA air interface. Note that the identification number is not the IP address. When the IP address is used as an identification number in the presence of network address translation, the proposed handover scheme cannot be carried out.

Figure 7.88b shows the MT immediately after it has moved into the WLAN service area. The MT establishes a communication link with the content server using the WLAN air interface. By receiving the identifier of the terminal through the WLAN air interface, the content server understands that the MT using the MBWA air interface is the same as that using the WLAN air interface. If required, the server assigns an identifier and an identification number after confirming the presence of one of them.

Figure 7.88c shows the MT after identification. Since the content server understands that the terminal using the MBWA air interface is the same as that using the WLAN air interface, the terminal can use both the communication links. In our field trial, the terminal selects the WLAN air interface on the basis of the rule that the MT preferentially selects the WLAN air interface.



(a) Mobile terminal (MT) outside WLAN service area. The MT establishes a communication link with the content server using the MBWA air interface.

(b) MT immediately after moving into WLAN service area. The MT establishes a communication link with the content server using the WLAN air interface.

(c) MT after identification. Since the content server understands that the terminal using the MBWA air interface is the same as that using the WLAN air interface, the terminal can use both the communication links.

(d) MT immediately after moving out of WLAN service area. The terminal requests the removal of the WLAN identification number via MBWA air interface after disconnecting the WLAN link.

(e) MT after moving across WLAN service area. The MT communicates with the content server using the MBWA air interface in the same way as shown in (a).

Fig. 7.88 The proposed handover procedure. As an example, the handover procedure is discussed for the case that an MT moving in the service area of a wide coverage air interface, such as that used in an MBWA network, moves across the service area of a high-throughput air interface such as that of a WLAN

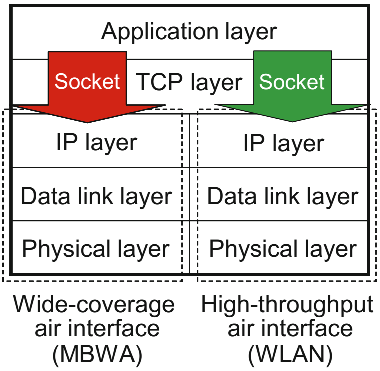


Fig. 7.89 Protocol stack of multiple sockets

Figure 7.88d shows the MT immediately after it has moved out of the WLAN service area. The terminal requests the removal of the WLAN identification number via MBWA air interface after disconnecting the WLAN link. The content server removes the WLAN identification number when the server receives the request for removal from the terminal or after time-out.

Figure 7.88e shows the MT after moving across the WLAN service area. The MT communicates with the content server using the MBWA air interface in the same way as shown in Fig. 7.88.

7.8.2.3 Implementation of Proposed Handover Scheme

To carry out the field trial, we developed application programs for the proposed handover scheme on the content server and MTs. The developed programs use multiple sockets to bind each air interface. Figure 7.89 shows the protocol stack of the multiple sockets. The MT selects an air interface after selecting a socket to send and receive packets.

7.8.2.4 Benefits of Proposed Handover Scheme

The above handover scheme using multiple sockets has the following benefits for the proposed heterogeneous wireless network.

(1) Location management at content server:

In the proposed network, only the content server manages the terminal location information, i.e., the service area the MT is in. The proposed network does not require present wireless infrastructure such as an MBWA or WLAN to manage the location information as a new function for handover. Thus, the present wireless infrastructure can be applied without modification to the proposed network.

(2) Any air interface applicable to proposed network:

Since the proposed handover scheme does not require the present wireless infrastructure to add functions for handover, any wireless interface can be applied to the proposed network. In our field trial, the IEEE 802.11g and Fast Low-Latency Access with Seamless Handoff (FLASH) OFDM air interfaces were used; however, air interfaces such as IEEE 802.11a/b/g/ac/ad, mobile Worldwide Interoperability for Microwave Access (WiMAX), 3G, Long Time Evolution (LTE), and LTE-Advanced can also be used to construct the proposed network. If the LTE and IEEE 802.11ac air interfaces are used, the proposed network can provide a wireless communication service with high throughput, such as 1 Gbit/s, and a wide coverage area, such as a cell radius of 1 or 2 km, to users, although the highest throughput is obtained under a low-mobility condition.

(3) No upgrades of wireless infrastructures and terminals:

Since the handover functions of the proposed scheme are implemented as application programs on the content server and MTs, only installation of the handover programs is required to construct the proposed network. Thus, no upgrades of the present wireless infrastructures and MTs are required to modify homogeneous networks to the proposed heterogeneous wireless network. We consider that the proposed network is suitable for smart phones with two air interfaces for the following reasons: (1) application software can be installed and (2) the additional implementation of an air interface is not required.

(4) Air interface selection while keeping packet transmission routes alive:

In the proposed handover scheme, one of the air interfaces can be selected using multiple sockets while keeping all the packet transmission routes alive. Air interface selection while keeping the routes alive results in a shorter outage time than that obtained in the conventional session initiation protocol (SIP)-based application-layer handover scheme [69] as well as in the soft handover schemes based on Mobile IPv6 [70] and SIP [71]. Note that the former requires updates of the infrastructure and terminals, and the latter requires additional equipment for soft handover. In contrast, the proposed handover scheme requires only installation of the handover application programs.

7.8.2.5 Field Trial Results

The measurements in the field trial were carried out in a building in the field trial area. The building was in the service areas of both a MBWA with wide coverage and a WLAN with high throughput. The MBWA service was experimentally

Table 7.6 Handover outage times from the MBWA to the WLAN

Measurement	Outage time (ms)
1	160
2	166
3	155
4	158
Average	159.8

Table 7.7 Handover outage times from the WLAN to the MBWA

Measurement	Outage time (ms)
1	57
2	44
3	112
4	57
Average	67.5

provided in the field trial area of Sendai city in Japan [58–63]. We deployed a WLAN access point in the building. The FLASH-OFDM MBWA network was used as a wide coverage air interface and the IEEE 802.11g WLAN network was used as a high-throughput air interface. The operating systems of the MT and the content server were Linux 2.6.9 and 2.6.14, respectively. The application programs of the proposed scheme on the server and terminal sides were written on Linux.

Table 7.6 shows the measured outage times in the handover from the MBWA to the WLAN. The number of trials was 4. The measured values ranged from 155 to 166 ms. Table 7.7 shows the measured outage times in the handover from the WLAN to the MBWA. The measured values ranged from 44 to 112 ms. Tables 7.6 and 7.7 show that the handover outage times from the MBWA to the WLAN and from the WLAN to the MBWA were approximately 160 and 60 ms, respectively. Since the same wired network accommodates the MBWA base station and the WLAN access point, we consider that the difference in the outage time is caused by the difference in performance between the MBWA and the WLAN such as the round-trip time. The above results suggest that the proposed heterogeneous wireless network is feasible since the handover outage time is less than 170 ms, which is tolerable in commercial services such as accessing web sites, transferring files, and streaming audio and video contents with buffering.

7.8.3 Hybrid Single-Carrier and Multicarrier Technology

7.8.3.1 Background

Robustness against multipath fading is required to realize high-speed transmission in next-generation wide-area wireless communications. Since a wider bandwidth yields more paths in the delay profile, the receivers of next-generation systems are required to demodulate signals in the presence of many paths. In this situation, multicarrier (MC) modulation such as OFDM yields a low error rate. Therefore, many next-generation wireless communication standards have adopted MC technologies.

However, MC signals have a high peak-to-average power ratio (PAPR). When the PAPR is high, the power efficiency of the transmitter power amplifier (PA) becomes low because the PA has to operate with high back-off (margin of power). In particular, in the uplink, a PA with high power efficiency is required because of a limitation on the power consumption of the MT. Thus, it is difficult to use MC signals for long-distance transmission. On the other hand, single-carrier (SC) signals have a low PAPR and are suitable for long-distance transmission. Therefore, SC signals are more suitable than MC signals for maintaining a wide coverage.

Using both SC signals with a wide coverage and MC signals with a high data rate in a hybrid network, the weaknesses of SC and MC can be overcome. Although communication methods using both SC and MC signals have been proposed [72, 73], these papers only discussed the combination of SC and MC signals. On the other hand, in our previous papers, a hybrid SC/MC system with reduced interference between SC and MC signals was proposed [66] and the uplink throughput of a hybrid SC/MC system was evaluated [67].

In this section, we discuss multiantenna transmission for the hybrid SC/MC system [68]. Space division multiplexing (SDM) is suitable for increasing the throughput when the MT is close to the BS. However, SDM decreases the throughput when the MT is away from the BS under the condition of constant total output power of the MT since the output power per antenna is decreased. To improve the throughput performance of the MT away from the BS, we propose the adaptive selection of joint frequency domain equalization (FDE)/antenna diversity [74] or SDM. No additional block in the receiver is required for the adaptive selection of joint detection or SDM since the selective signal detection of joint FDE/antenna diversity or SDM is carried out by rewriting a channel matrix, as will be described later.

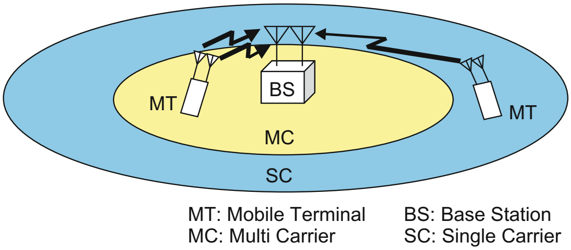


Fig. 7.90 Hybrid SC/MC system with adaptive multiantenna transmission for uplink

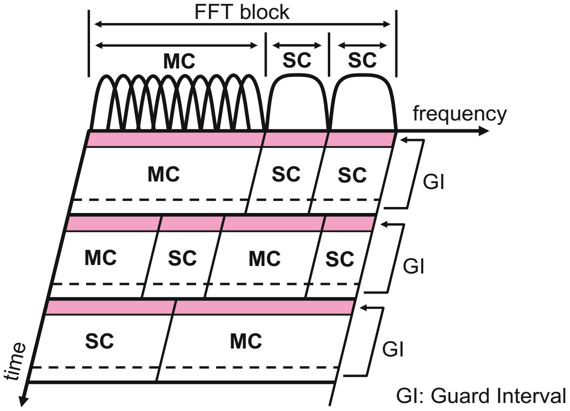


Fig. 7.91 Signal arrangement of hybrid SC/MC system

7.8.3.2 Hybrid SC/MC System with Adaptive Multiantenna Transmission Model

In this section, we describe the proposed hybrid SC/MC system with the optimal selection of SDM or the joint FDE/antenna diversity, which attain high throughput and wide coverage [68].

Figure 7.90 shows the proposed hybrid SC/MC system with adaptive multiantenna transmission. In this paper, the hybrid system is used for the uplink. The hybrid system prepares transmission schemes for both SC and MC signals in an MT and switches the transmission scheme depending on the situation. The switching threshold was based on the received signal-to-noise ratio (SNR) in the BS. If the received SNR was higher than the threshold, MC transmission was used, but if not, SC transmission was used. An MT near the BS used MC transmission, and an MT far from the BS used SC transmission. In the MC transmission, m-ary QAM was used as the modulation method for high-speed transmission. On the other hand, in the SC transmission, phase shift keying (PSK) was applied for a low PAPR, which allowed the PA to use the maximum transmission power. Thus, using both SC transmission to maintain a wide coverage and MC transmission for high-speed transmission, we were able to communicate effectively in the uplink.

The maximum throughput can be improved by increasing the number of antennas using SDM. However, the throughput at the cell edge is decreased because of the decrease in the transmission power per antenna under the condition that the total output power of the terminal is constant.

In the proposed hybrid system, multiple access is carried out in the time and frequency domains, and multiplexing is carried out in the space domain. Figure 7.91 shows the signal arrangement of multiple access in the proposed hybrid system. A channel was allocated for each MT with SC or MC transmission. These channels were allocated orthogonally in the frequency domain and synchronized within the guard interval (GI) gap as well as that of orthogonal frequency-division

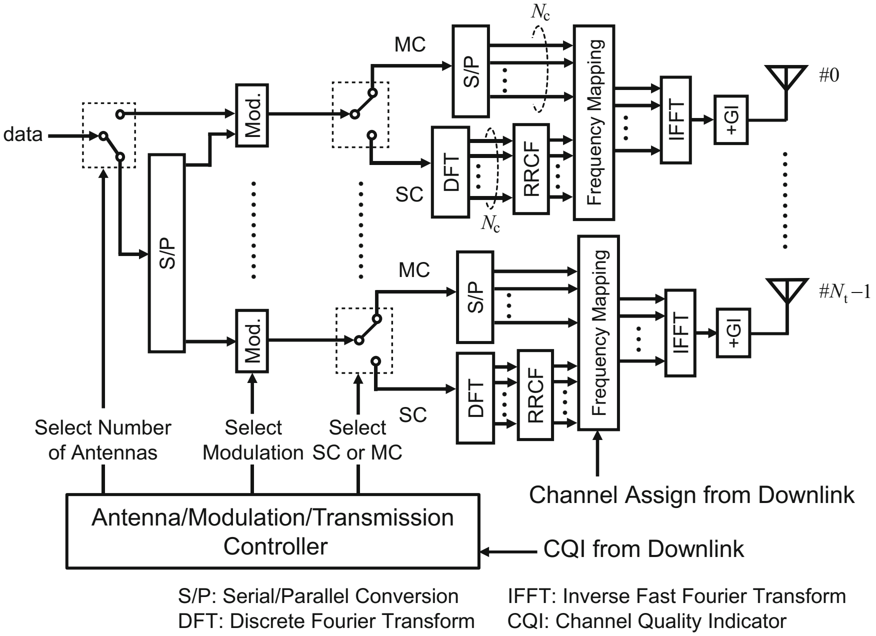

data
Mod.
Mod.
S/P
MC
SC
MC
SC
S/P
DFT
RRCF
N_c
N_c
Frequency Mapping
IFFT
+GI
#0
S/P
DFT
RRCF
Frequency Mapping
IFFT
+GI
#N_t−1
Select Number of Antennas
Select Modulation
Select SC or MC
Antenna/Modulation/Transmission Controller
Channel Assign from Downlink
CQI from Downlink
S/P: Serial/Parallel Conversion
DFT: Discrete Fourier Transform
IFFT: Inverse Fast Fourier Transform
CQI: Channel Quality Indicator

Fig. 7.92 Modulator of hybrid system

multiple access (OFDMA). Therefore, signal arrangement was carried out without interference among the channels.

Figure 7.92 shows the modulator of the proposed system. First, the number of antennas is selected. The number of transmitter antennas for joint FDE/antenna diversity is one. On the other hand, SDM uses N_t antennas. Before an SC signal is inputted to a frequency-mapping block, the SC signal is converted from the time domain to the frequency domain by a discrete Fourier transform (DFT). The frequency-mapping block specifies an inverse fast Fourier transform (IFFT) point, which is allocated to each MT. In the IFFT block, a time domain waveform is generated. Afterwards, to remove interblock interference, a GI is added. In the generation of SC and MC signals using the above structure, each signal is orthogonal and efficient communication is possible. An MT sends a pilot signal and data packets to the BS. In this paper, we used a Chu sequence for the pilot signal. The BS calculates a channel quality indicator (CQI) using the received pilot signal. The BS returns CQI information through the downlink and assigns a channel to the MT. The controller decides the number of antennas, the transmission scheme, and the modulation scheme for the uplink.

Figure 7.93 shows the demodulator of the proposed system. First, the GI of the received signal is removed. Second, the time domain waveform is converted into a frequency domain waveform by FFT processing. Then, in the frequency-demapping block, each signal element is extracted from each subcarrier. Third, the signal

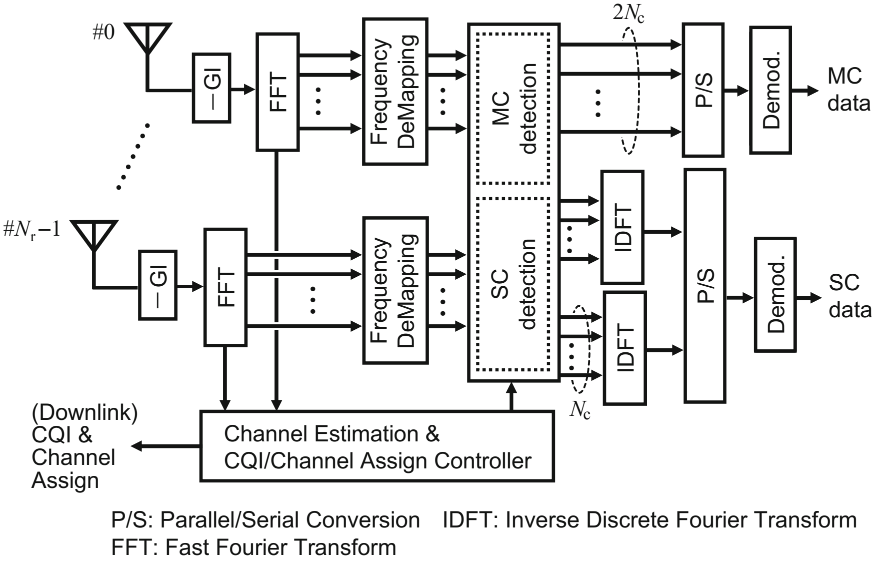

#0
#N_r−1
−GI
−GI
FFT
FFT
Frequency DeMapping
Frequency DeMapping
MC detection
SC detection
2N_c
N_c
IDFT
IDFT
P/S
P/S
Demod.
Demod.
MC data
SC data
(Downlink) CQI & Channel Assign
Channel Estimation & CQI/Channel Assign Controller
P/S: Parallel/Serial Conversion
IDFT: Inverse Discrete Fourier Transform
FFT: Fast Fourier Transform

Fig. 7.93 Demodulator of hybrid system

detection part corresponds to both SDM and joint FDE/antenna diversity. We describe the signal detection in detail in [68]. Since the MC signal records each data symbol in a subcarrier, the symbol is demodulated in the frequency domain. On the other hand, for an SC signal, an inverse DFT (IDFT) is used to convert it from the frequency domain into the time domain again. As a result of the above process, the SC and MC signals transmitted from each MT can be demodulated.

For the case of an SC, if a filter is not used, the SC signal has a steep attenuation characteristic in the frequency domain and a high PAPR in the time domain. To reduce the PAPR of the signal, the root-raised cosine filter is used in the SC modulation and demodulation for spectrum shaping.

7.8.4 Conclusions and Future Works

In this section, the problems of coverage and throughput in homogeneous mobile broadband wireless access (MBWA) networks were first discussed. We then showed that heterogeneous wireless communication networks are a viable solution to these problems. To provide a wireless data communication service with higher throughput and a wide coverage area to users of the proposed network, we proposed two schemes in this section: a seamless system handover scheme for heterogeneous wireless networks and a hybrid single-carrier and multicarrier (SC/MC) technology.

Future works are as follows: (1) standardization of the seamless system handover method and (2) transceiver implementation of the hybrid SC/MC technology using RF/analog circuits.

References

1. M. Shafi, T. Hattori, S. Ogose (eds.), Fundamentals of multiple access techniques, in *Wireless Communications in the 21st Century* (Wiley-IEEE Press, 2002)
2. T. Utano, Innovations and impacts of cellular phone systems (in Japanese). IEICE J. **90**(5), 350–356 (2007)
3. D. Astély et al., LTE: the evolution of mobile broadband. IEEE Commun. Mag. **47**(4), 44–51 (2009)
4. F. Adachi, M. Sawahashi, H. Suda, Wideband DS-CDMA for next generation mobile communications systems. IEEE Commun. Mag. **36**(9), 56–69 (1998)
5. H.G. Myung, J. Lim, D.J. Goodman, Single carrier FDMA for uplink wireless transmission. IEEE Veh. Technol. Mag. **1**(3), 30–38 (2006)
6. S.-Y. Lien, K.-C. Chen, Y. Lin, Toward ubiquitous massive accesses in 3GPP machine-to-machine communications. IEEE Commun. Mag. **49**(4), 66–74 (2011)
7. The situation of the information and communications in The Great East Japan Earthquake, in Telecommunications white paper 2011, Ministry of Internal Affairs and Communications (August 2011)
8. F. Adachi et al., R&D project of multilayered communications network—For disaster-resilient communications, in *Proceedings of the 15th International Symposium on Wireless Personal Multimedia Communications* (Taipei, Taiwan, Sept 2012)
9. T. Nakamura et al., Trends in small cell enhancements in LTE advanced. IEEE Commun. Mag. **51**(2), 98–105 (2013)
10. K. Tsubouchi, Strategy of IT device technology for wireless NGN, in *2007 Microwave Workshops & Exhibition (MWE 2007)* (Nov 2007 (invited, keynote, in Japanese))
11. K. Tsubouchi, Dependable wireless next generation network (NGN): network and device technologies, in *Global Symposium on Millimeter Waves 2009 (GSMM 2009)* (April 2009 (invited, keynote))
12. S. Kameda, Y. Miyake, K. Komatsu, M. Iwata, N. Suematsu, T. Takagi, K. Tsubouchi, ASIC implementation of multimode frequency domain equalizer for Dependable Air, in *27th International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC 2012)* (July 2012)
13. K. Tsubouchi, S. Kameda, N. Suematsu, Dependable Air. IEICE Trans. Electron. **J95-C**(12), 460–469 (2012) (invited, in Japanese)
14. T. Takagi, S. Kameda, N. Suematsu, K. Tsubouchi, Dependable Air and wireless dependability, in *6th Global Symposium on Millimeter-Waves 2013 (GSMM 2013)* (April 2013 (invited))
15. K. Tsubouchi, Extended Dependable Air: heterogeneous wireless network for surface, space and sea, in *Asia-Pacific Microwave Conference 2014 (APMC 2014)* (Nov 2014 (invited))
16. T.T. Ta, K. Gomyo, S. Tanifuji, S. Kameda, T. Takagi, N. Suematsu, K. Tsubouchi, A Si-CMOS 60 GHz receiver for phased array antenna with 7-stage LNA, wideband mixer and 5-bit baseband phase shifter, in *6th Global Symposium on Millimeter-Waves 2013 (GSMM 2013)* (Sendai, Japan, April 2013)
17. T.T. Ta, S. Tanifuji, A. Taira, S. Kameda, N. Suematsu, T. Takagi, K. Tsubouchi, A millimeter-wave WPAN adaptive phased array control method using low-frequency part of signal for self-directed system. IEEE Trans. Microw. Theory Tech. **63**(8), 2682–2691 (2015)

18. T.T. Ta, S. Tanifuji, S. Kameda, N. Suematsu, T. Takagi, K. Tsubouchi, A Si-CMOS 5-bit baseband phase shifter using fixed gain amplifier matrix, in *European Microwave Conference 2012 (EuMC 2012)* (Amsterdam, Netherland, Oct 2012)
19. T.T. Ta, S. Tanifuji, S. Kameda, N. Suematsu, T. Takagi, K. Tsubouchi, A calibrationless Si-CMOS 5-bit baseband phase shifter using a fixed-gain-amplifier matrix. IEICE Trans. Electron. **E96-C**(10), 1322–1329 (2013)
20. T. Takagi, E. Nakayama, T.T. Ta, S. Kameda, N. Suematsu, K. Tsubouchi, A novel planar type broadband CMOS on-chip balun with relative bandwidth of 158%, in *2012 Asia-Pacific Microwave Conference (APMC 2012)* (Kaohsiung, Taiwan, Dec 2012) pp. 178–180
21. K. Tsubouchi, M. Yokoyama, H. Nakase, A new concept of 3-dimentional multilayer-stacked system-in-package for software-defined-radio. IEICE Trans. Electron. **E84-C**(12), 1730–1734 (2001)
22. S. Yoshida, S. Tanifuji, S. Kameda, N. Suematsu, T. Takagi, K. Tsubouchi, Copper balls interconnection technology for 60 GHz band 3-D system-in-package modules, in *2010 Asia-Pacific Microwave Conference (APMC 2010)* (Yokohama, Japan, Dec 2010)
23. S. Yoshida, S. Tanifuji, S. Kameda, N. Suematsu, T. Takagi, K. Tsubouchi, 60-GHz band copper ball vertical interconnection for MMW 3-D system-in-package front-end modules. IEICE Trans. Electron. **E95-C**(7), 1276–1284 (2012)
24. S. Yoshida, S. Kameda, T. Takagi, K. Tsubouchi, Radiation characteristics of a planar monopole antenna integrated with a 60 GHz band WPAN module using organic substrates, in *4th European Conference on Antennas and Propagation (EuCAP 2010), C33P1–5* (Barcelona, Spain, April 2010)
25. N. Suematsu, S. Yoshida, S. Tanifuji, S. Kameda, T. Takagi, K. Tsubouchi, A 60 GHz-band 3-dimensional system-in-package transmitter module with integrated antenna. IEICE Trans. Electron. **E95-C**(7), 1141–1146 (2012) (invited)
26. S. Yoshida, Y. Suzuki, T.T. Ta, S. Kameda, N. Suematsu, T. Takagi, K. Tsubouchi, A 60-GHz band planar dipole array antenna using 3-D SiP structure in small wireless terminals for beamforming applications. IEEE Trans. Antennas Prop. **61**(7), 3502–3510 (2013)
27. N. Suematsu, Y. Suzuki, S. Yoshida, S. Tanifuji, S. Kameda, T. Takagi, K. Tsubouchi, A 60-GHz-band 2 × 4 planar dipole array antenna module fabricated by 3-D SiP technology, in *IOP Conference Series: Materials Science and Engineering*, Vol. 61 (2014) 012036 (2014 (invited))
28. S. Tanimori, K. Katayama, M. Motoyoshi, K. Takano, M. Fujishima, 80 GHz 12.2 mW p-MOS cross-coupled CMOS LC oscillator, in *2012 International Meeting for Future of Electron Devices, Kansai (IMFEDK)* (May 2012) pp. 1–2
29. M. Motoyoshi, R. Fujimoto, K. Takano, M. Fujishima, 140 GHz CMOS amplifier with group delay variation of 10.2 ps and 0.1 dB bandwidth of 12 GHz. IEICE Electron. Express **8**(4), 1192–1197 (2011)
30. A. Orii, K. Katayama, M. Motoyoshi, K. Takano, M. Fujishima, 118 GHz CMOS amplifier with group delay variation of 11.2 ps and 3 dB bandwidth of 20.4 GHz, in *2012 International Meeting for Future of Electron Devices, Kansai (IMFEDK)* (May 2012) pp. 1–2
31. A. Matsuzawa, High speed and low power ADC design with dynamic analog circuits, in *IEEE ASICON 2009* (Changsha, China, 20–23 Oct 2009)
32. Y. Miyake, K. Komatsu, H. Oguma, N. Izuka, S. Kameda, M. Iwata, N. Suematsu, T. Takagi, K. Tsubouchi, ASIC implementation of multimode frequency domain equalizer for heterogeneous wireless system, in *2013 IEEE 24th International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC 2013)* (2013)
33. R. Inagaki, T. Tanaka, M. Tsuru, E. Taniguchi, H. Fukumoto, S. Kameda, N. Suematsu, A. Taira, T. Takagi, K. Tsubouchi, A 5 GHz/60 GHz receiver front-end IC in 90 nm CMOS technology, in *EuMW 2014* (Italia, 6–10 Oct 2014)
34. Y. Natsukari, M. Fujishima, 36 mW 63 GHz CMOS differential low-noise amplifier with 14 GHz bandwidth, in *2009 Symposium on VLSI Circuits Design of Technical Papers, 24–4* (2009), pp. 252–253

35. S. Pellerano, Y. Palaskas, K. Soumyanath, A 64 GHz LNA with 15.5 dB Gain and 6.5 dB NF in 90 nm CMOS. IEEE J. Solid-State Circuits **43**(7), 1542–1552 (2008)
36. B. Heydari, P. Reynaert, E. Adabi, M. Bohsali, B. Afshar, M.A. Arbabian, A.M. Niknejad, A 60-GHz 90-nm CMOS cascode amplifier with interstage matching, in *IEEE EuMIC,* (2007), pp. 88–91
37. B. Razavi, A mm-wave CMOS heterodyne receiver with on-chip LO and divider. in *IEEE Journal of Solid-State Circuits Conference (ISSCC 2007)* (2007)
38. M. Tsuru, T. Tanaka, R. Inagaki, E. Taniguchi, M. Nakayama, S. Kameda, N. Suematsu, T. Takagi, K. Tsubouchi, Flip-chip assembly 60 GHz CMOS receiver front-end, in *IMWS 2012* (China, 18–20 Sept 2012)
39. E. Taniguchi et al., A 60 GHz-band CMOS transistor-pair type even-harmonic mixer utilizing λ/4 transmission line. IEICE Technical Report. (Japanese Edition), Microwaves **109**(342), 53–57 (2009)
40. R.G. Meyer, W.D. Mack, A DC to 1-GHz differential monolithic variable-gain amplifier. IEEE J. Solid-State Circuits **26**(11), 1673–1680 (1991)
41. B. Murmann, Digitally assisted analog circuits. IEEE Micro **26**(2), 38–47 (2006)
42. A. Matsuzawa, *Digitally-Assisted Analog and RF CMOS Circuit Design for Software-Defined Radio* (Springer, 2011)
43. F. Ohnheuser, *Analog-Digital Converters for Industrial Applications Including as Introduction to Digital-Analog Converters* (Springer, 2015)
44. S. Lee, H. Kawaraguchi, T. Hirato, M. Miyahara, A. Matsuzawa, A 12 b 50/70 MS/s 2.2/4.6 mW 0.03 mm^2 CMOS SAR ADC for a frequency, performance, and power scalable ADC, in *SSDM* (Sept 2013)
45. M. Miyahara, Y. Asada, D. Paik, A. Matsuzawa, *A-SSCC* (Nov 2008) pp. 269–272
46. W. Liu, P. Huang, Y. Chiu, *ISSCC,* Feb 2010, pp. 380–381
47. T. Morie, T. Miki, K. Matsukawa, Y. Bando, T. Okumoto, K. Obata, S. Sakiyama, S. Dosho, *ISSCC* (Feb 2013) pp. 272–273
48. D. Falconer, S.L. Ariyavisitakul, A. Benyamin-Seeyar, B. Edison, Frequency-domain equalization for single-carrier broadband wireless systems. IEEE Commun. Mag. **40**, 58–66 (2002)
49. F. Adachi, G. Garg, S. Takaoka, K. Takeda, Broadband CDMA techniques, special issue on modulation, coding and signal processing. IEEE Wireless Commun. Mag. **12**(2), 8–18 (2005)
50. V. Gheorghiu, S. Kameda, T. Takagi, K. Tsubouchi, F. Adachi, Implementation of single carrier packet transmission with frequency domain equalization, in *IEEE VTC 2008-Fall* (Sept 2008)
51. V. Gheorghiu, S. Kameda, T. Takagi, K. Tsubouchi, F. Adachi, Implementation of frequency domain equalizer for single carrier transmission, in *WiCOM 2008* (Oct 2008)
52. K. Komatsu et al., ASIC implementation of frequency domain equalizer for single carrier transmission, in *The XXX General Assembly and Scientific Symposium of the International Union of Radio Science (URSI-GASS 2011)* (Aug 2011)
53. D.C. Chu, Polyphase codes with good period correlation properties. IEEE Trans. Inf. Theory **18**, 531–532 (1972)
54. S. Hara, R. Prasad, *Multicarrier Techniques for 4G Mobile Communications* (Artech House, 2003)
55. H. Gacanin et al., Pilot-assisted channel estimation for OFDM/TDM with frequency-domain equalization, in *IEEE 62nd Vehicular Technology Conference (VTC 2005-Fall)* (Sept 2005)
56. S. Coleri et al., Channel estimation techniques based on pilot arrangement in OFDM systems. IEEE Trans. Broad. **48**(3), 362–370 (2002)
57. K. Takeda, F. Adachi, SNR estimation for pilot-assisted frequency-domain MMSE channel estimation, in *2005 IEEE Vehicular Technology Society Asia Pacific Wireless Communication Symposium (APWCS 2005)* (Aug 2005)
58. H. Oguma, S. Kameda, N. Izuka, Y. Asano, Y. Yamazaki, T. Takagi, K. Tsubouchi, Measured downlink throughput performance of MBWA system in urban area, in *IEEE International Symposium on Wireless Communication Systems (ISWCS 2008)* (2008)

59. N. Izuka, Y. Asano, Y. Yamazaki, H. Oguma, S. Kameda, T. Takagi, K. Tsubouchi, First-ever report on MBWA system field trial: interference issue in sectored cell layout, in *IEEE Vehicular Technology Conference (VTC 2008-Fall)* (2008)
60. S. Kameda, H. Oguma, N. Izuka, Y. Asano, Y. Yamazaki, T. Takagi, K. Tsubouchi, Feasibility study of downlink transmission with 256 QAM based on results of MBWA system field trial, in *European Wireless (EW 2009)* (2009)
61. H. Oguma, S. Kameda, N. Izuka, Y. Asano, Y. Yamazaki, T. Takagi, K. Tsubouchi, Uplink throughput performance of FH-OFDMA improved by 16 QAM: effect estimation and validation in MBWA system field trial, in *IEEE Personal, Indoor and Mobile Radio Communications Symposium (PIMRC 2009)* (2009)
62. H. Oguma, S. Kameda, N. Izuka, Y. Asano, Y. Yamazaki, T. Takagi, K. Tsubouchi, Coverage estimation of uplink 16 QAM signal up to 20 MHz bandwidth based on field trial results of FH-OFDMA system, in *IEEE Wireless Communications and Networking Conference (WCNC 2010)* (2010)
63. S. Kameda, H. Oguma, N. Izuka, Y. Asano, Y. Yamazaki, N. Suematsu, T. Takagi, K. Tsubouchi, Measured downlink throughput performance of MBWA system in urban area. IEICE Trans. Commun. **E96-B**(1), 329–334 (2013)
64. S. Kameda, H. Oguma, N. Izuka, F. Yamagata, Y. Asano, Y. Yamazaki, S. Tanifuji, N. Suematsu, T. Takagi, K. Tsubouchi, Proposal of heterogeneous wireless communication network with soft handover in application layer: Feasibility study based on field trial results, in *6th International ICST Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom 2011)* (June 2011)
65. S. Kameda, H. Oguma, N. Izuka, F. Yamagata, Y. Asano, Y. Yamazaki, S. Tanifuji, N. Suematsu, T. Takagi, K. Tsubouchi, Proposal of heterogeneous wireless network with handover in application layer: feasibility study based on field trial results. IEICE Trans. Commun. **E95-B**(4), 1152–1160 (2012)
66. I. Kashiwamura, S. Tomita, K. Komatsu, N. Tran, H. Oguma, N. Izuka, S. Kameda, T. Takagi, K. Tsubouchi, Investigation on single-carrier and multi-carrier hybrid system for uplink, in *IEEE 20th Personal, Indoor and Mobile Radio Communication (PIMRC 2009)* (Tokyo, Japan, Sept 2009)
67. S. Tomita, Y. Miyake, I. Kashiwamura, K. Komatsu, N. Tran, H. Oguma, N. Izuka, S. Kameda, T. Takagi, K. Tsubouchi, Hybrid single-carrier and multi-carrier system: improving uplink throughput with optimally switching modulation, in *IEEE 21th Personal, Indoor and Mobile Radio Communincation (PIMRC 2010)* (Istanbul, Turkey, Sept 2010)
68. Y. Miyake, K. Kobayashi, K. Komatsu, S. Tanifuji, H. Oguma, N. Izuka, S. Kameda, N. Suematsu, T. Takagi, K. Tsubouchi, Hybrid single-carrier and multi-carrier system: widening uplink coverage with optimally selecting SDM or joint FDE/antenna diversity, in *The 14th International Symposium on Wireless Personal Multimedia Communications (WPMC 2011)* (France, Oct 2011)
69. H. Schulzrinne, E. Wedlund, Application-layer mobility using SIP. ACM SIGMOBILE Mobile Comput. Commun. Rev. **4**(3), 47–57 (2000)
70. H. Rutagemwa, S. Pack, X. Shen, J.W. Mark, Cross-layer design and analysis of wireless profiled TCP for vertical handover, in *IEEE International Conference on Communications (ICC 2007)* (2007)
71. S. Salsano, L. Veltri, G. Martiniello, A. Polidoro, Seamless vertical handover of VoIP calls based on SIP session border controllers, in *IEEE International Conference on Communications (ICC 2006)* (2006)
72. M. Tanno, Y. Kishiyama, H. Taoka, N. Miki, K. Higuchi, A. Morimoto, M. Sawahashi, Layered OFDMA radio access for IMT-advanced, in *IEEE 68th Vehicular Technology Conference (VTC 2008)* (Calgary, Canada, Sept 2008)
73. K. Ban, Transmitting, receiving device, and wireless communication system, Japanese Patent Application 2008-42492 (Feb 2008) (in Japanese)
74. F. Adachi, H. Tomeba, K. Takeda Frequency-domain equalization for broadband single-carrier multiple access. IEICE Trans. Commun. **E92-B**(5), 1441–1456 (2009)

Chapter 8
Connectivity in Electronic Packaging

Hiroki Ishikuro, Tadahiro Kuroda, Atsutake Kosuge, Mitsumasa Koyanagi, Kang Wook Lee, Hiroyuki Hashimoto and Makoto Motoyoshi

Abstract This chapter deals with the issue of packaging and interconnects in electronic systems. An electronic system in general consists of multiple subsystem modules in certain form of packages and electrical interconnects between them. A module, in turn, consists of multiple VLSI chips and interconnects. Interconnects often become bottleneck of the performance of electronic systems because the performance gap between the bus bandwidth and processor core speed has increased as the process technology scales. Development in the performance of systems has thus been accompanied by the development of interconnects as well as VLSI chips. Exactly like what happened in the VLSI, the technology of packaging and interconnects has developed tremendously in terms of bandwidths, power dissipation, form factors (physical dimensions), and so forth. In fact, it has always been one of the central issues in the design of systems, involved sophisticated engineering, and required attention from the perspective of dependability. Section 8.1 gives an overview of the requirements for packaging and interconnects and highlights wireless technology for packaging as an emerging technology for packaging or integrating complex systems. Section 8.2 introduces wireless interconnect and compares it with conventional wired interconnect in a few practical examples. Section 8.3 describes the through-silicon via (TSV) in three-dimensional (3D) integration of silicon VLSI from the perspective of performance and dependability and introduces the concept of redundant vias.

Keywords Wireless interconnect · Inductive coupling · Transmission line coupler · Three-dimensional integration · TSV

H. Ishikuro (✉) · T. Kuroda · A. Kosuge
Keio University, Yokohama, Japan
e-mail: ishikuro@elec.keio.ac.jp

M. Koyanagi · K. W. Lee · H. Hashimoto
Tohoku University, Sendai, Japan

M. Motoyoshi
Tohoku MicroTech Co., Ltd., Sendai, Japan

S. Asai (ed.), *VLSI Design and Test for Systems Dependability*,
https://doi.org/10.1007/978-4-431-56594-9_8

8.1 Requirements for Dependable Electronic Packaging

Tadahiro Kuroda, Keio University
Atsutake Kosuge, Keio University

8.1.1 Historical Perspective

The integrated circuit was invented in response to the “tyranny of numbers” in device interconnection. In 1946, the ENIAC general-purpose electronic computer developed in the United States was constructed of 100,000 components with five million hand-soldered connections. The number of connections increases geometrically with system scale. At that time, Texas Instruments had been studying a micromodule scheme in which devices were mounted at high density on a circuit board, but Jack Kirby came up with a revolutionary idea that went far beyond that. Kirby’s idea was “monolithic integration”, where all of the devices would be integrated on a single semiconductor substrate. Since then, the integration scale of integrated circuits has grown exponentially. Today, billions of transistors can be integrated along with kilometers of wiring that has hundreds of billions of connections, all on one small chip. We have reached the point where a large-scale system can be integrated on a single chip, which is known as System-on-Chip (SoC) technology.

However, integrated circuit miniaturization is approaching a limit. On one hand, the amount of data being handled is increasing as we enter the Internet of Things (IoT) era, and an even higher level of computing performance is required for big data analysis. Now that we can no longer rely simply on higher levels of integration on a single chip, we need a revolutionary solution such as connections between chips within a package and connections between boards outside of packages.

Connectors have been widely used to interconnect the modules that make up a system. To give just a few examples, they have been used to interconnect a smartphone’s display and motherboard or a computer’s processor and external memory, or to make a connection to an automobile’s electronic control unit (ECU). Connectors were originally considered to be a highly dependable product as reflected by their extensive use in the aircraft industry. However, a drop in dependability has become evident with the trend toward inexpensive, small and light, and high-frequency-band connectors creating a serious problem for designers as described below in more detail. This section begins by outlining interconnect requirements. It then analyzes the problems with conventional mechanical (crimp-type) connectors and introduces electronic noncontact connectors that are expected to solve those problems. The key to dependability is now an innovative shift from mechanical connections to electronic connections. Specific applications and their related problems and solutions are presented in Chap. 21.

8.1.2 Interconnect Requirements

Interconnect requirements can be broadly divided into (1) high reliability and durability, (2) compact/low-profile and advanced design, and (3) high-speed and multi-electrode/high-density configuration.

8.1.2.1 High Reliability and Durability

Equipment and devices used in automobiles, trains, aircraft, and spacecraft must be highly reliable and durable. This requirement can be broken down into the following four points.

(1) **Vibration/shock resistant**: Connectors for automobiles, aircraft, spacecraft, etc. can be subjected to large vibrations while they are moving or flying or at takeoff or launch. Even a momentary disconnection of an electrode (instantaneous interruption) can lead to a serious incident. A robust protection mechanism is needed to prevent such instantaneous interruptions even when large external forces or accelerations are applied to connectors.
(2) **Resistant and durable in relation to temperature and humidity**: The engine compartment of an automobile is subjected to high temperatures and high humidity. A spacecraft, meanwhile, is subjected to a wide range of temperatures when launched from ground level into the atmosphere and outer space. Connectors must also be highly durable and resistant to such severity and drastic changes in environment.
(3) **Good insulation**: Voltages in automobiles may reach 200 V and higher in addition to 5, 12, and 40 V levels. There are many cases, however, in which the modules in an automobile are not grounded in common, so good insulation is required between them.
(4) **Insertion/extraction durability**: The frequent insertion and extraction of cable plugs into and from connectors used for charging as in mobile devices can cause extreme wear in the metallic terminals of those connectors. Connectors such as these must be highly robust against repeated plug insertion and extraction.

8.1.2.2 Compact/Low-Profile and Advanced Design/Operability

Printed circuit boards in mobile devices need to be made as small as possible to provide space to accommodate larger batteries and extended operation time. Advanced designs and improvements in operability are required here.

(1) **Compact/low profile**: Connectors can take up the largest volume among mounted components. Smaller connectors mean smaller circuit boards.

(2) **Advanced design and improved operability**: Mobile devices often include sliding or folding modules to achieve compact housing. Such a degree of freedom can be obtained by combining connectors with flexible cables. However, the mechanical stress at the point of connection is an issue, and it is difficult to achieve high-speed communications with such a configuration. There is therefore a need for a means of connection that can accommodate movable modules while preventing increases in mechanical stress or drops in communication speed.

8.1.2.3 High-Speed and Multi-electrode/High-Density Configuration

There is a strong requirement for high-speed, multi-electrode, and high-density data communications between computers and servers

(1) **High speed**: Backplane connections on a server must be capable of high-speed data communications and hot swapping. Recent specifications for servers call for data communication speeds on the terabyte-per-second order. There is also a strong requirement for uninterrupted operation in server applications. Shutting down the system every time a module needs to be replaced reduces the system's availability factor. Hot swapping enables modules to be replaced without interrupting system operation.

(2) **Multi-electrode/high density**: Signal wiring in CPUs, FPGAs, and other integrated components can consist of several hundred wires. However, arranging a large number of small pins in a high-density configuration makes the component susceptible to mechanical stress and damage. Degradation in signal quality caused by signal leaking between signal wires can also be a problem here. There is therefore a need for a connection system that can practically eliminate mechanical stress and signal leaking.

8.1.3 Problems with Conventional Mechanical Connectors

Conventional connectors employ a mechanical system in which spring action is used to hold electrodes in place (Fig. 8.1). This and the fact that electrodes are exposed create problems in reliability.

8.1.3.1 Low Reliability and Durability

The structure of conventional connectors is such that exposed electrodes mate with each other to conduct electricity. This makes it easy for electrodes to break down and for reliability to suffer.

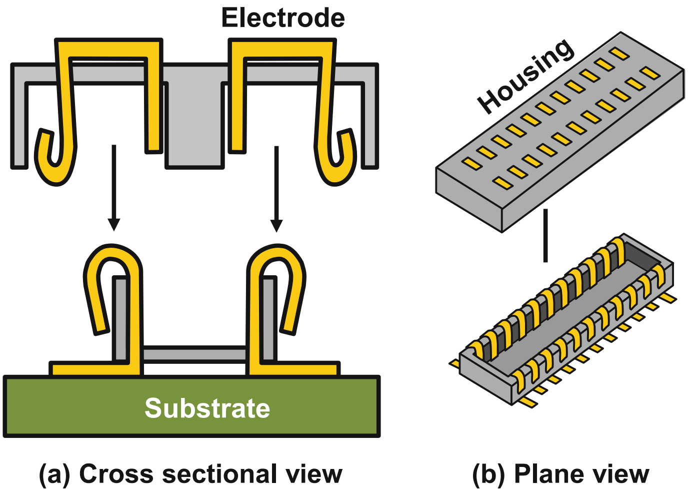


Fig. 8.1 Structure of conventional mechanical connector

(1) **Vibration/shock resistance**: Vibrations can cause two mating electrodes to separate thereby causing an instantaneous interruption that prevents the passage of signals or provision of power. The end result is a loss of information or function. A solid protection mechanism is therefore needed to keep two mating electrodes firmly in place so that no instantaneous interruptions occur, but this can lead to large and heavy connectors.

(2) **Environmental durability**: Due to the fact that electrodes are exposed, high-temperature and high-humidity conditions and the effects of chemicals in the environment can cause them to corrode. In addition, the presence of dirt or dust between electrodes can increase contact resistance and degrade high-frequency characteristics.

(3) **Insertion/extraction durability**: Given a structure in which exposed electrodes come into physical contact with each other, mating electrodes will be subject to frictional wear every time an insertion or extraction occurs making it easy for connectors to break down.

8.1.3.2 Large Size, High Profile

Connectors incorporate a housing element to protect the signal electrodes and facilitate the mechanical mating of electrodes (Fig. 8.1). Although progress is being made in the small-scale integration of electronic components, it is difficult to do so for connectors. Downsizing electrodes increases the difficulty of ensuring stable contacts thereby limiting the extent of miniaturization.

8.1.3.3 Low Speed, Low Density

In conventional connectors, impedance matching is difficult at the point of mechanical contact, and signal leaking in narrow-pitch and many-pin configurations is a problem.

(1) **Deterioration in signal quality**: In the connector section of a circuit board, arranging the GND plane (return path) nearby is troublesome because of geometrical constraints, and this makes impedance matching difficult. This, in turn, causes signal reflections to occur, which limits the bandwidth in data communications. In addition, adopting a coaxial configuration to achieve good impedance matching will increase the physical volume of the connector.

(2) **Signal leaking**: Signal electrodes can be arranged in a narrow pitch to support the many-signal wiring formats of integrated components like CPUs and FPGAs, but doing so generates crosstalk between electrodes. To prevent such crosstalk, a GND pin could be inserted between electrodes, but such a scheme would require twice as many connector pins as the number of signals.

8.1.4 Wireless Interconnect

Wireless interconnect technology has been investigated as one method for improving the dependability of interconnections. Typical examples of applying this technology are introduced below.

8.1.4.1 Overview

As the name implies, wireless interconnect technology enables signals and electric power to be transmitted between modules via wireless means. Specifically, it enables signals and electric power to be transmitted over a short distance of several mm via antennas or couplers. The advantage of a wireless interconnection is that it involves no mechanical mating or exposed electrode, meaning high resistance to mechanical wear and environmental fluctuations. In addition, a wireless interconnection is inherently contactless, so it is difficult for data communications to be affected by vibrations. It also means no instantaneous interruptions, which negates the need for a vibration-resistant mechanism, and since there is also no need for housing, a compact, low-profile, and lightweight configuration can be achieved opening the way to advanced designs and improved operability. Impedance matching can also be achieved with a wireless interconnection thereby enabling wider bandwidths and faster data communications.

8.1.4.2 Wireless Interconnect Systems

Wireless interconnections can be achieved by using radio frequency (RF)/millimeter waves, coil/capacitor lumped-constant coupling, or electromagnetic distributed-constant coupling. The main features of each of these systems are described below.

(1) **RF/millimeter waves**: Inter-module communication technology for achieving interconnections at a distance of several cm by RF/millimeter waves is being researched and developed (Fig. 8.2) [1–4]. The use of millimeter waves makes it possible to obtain wideband characteristics and achieve high-speed communications. This technology, however, has a problem in energy consumption. While the energy consumption of ordinary wired transceivers is less than 10 pJ/b, that of a transceiver using RF/millimeter waves is about 100 pJ/b or ten times greater.

(2) **Inductive/capacitive coupling**: Systems using magnetic-field (inductive) or electric-field (capacitive) near-field coupling are being researched (Fig. 8.3). Inductive coupling uses coils [5–7] while capacitive coupling uses capacitors [8]. In near-field communications, signal power attenuation is proportional to the cube of the distance.

As a result, signal leaking is minimal. Near-field coupling can also obtain a wider bandwidth compared to what is possible with antennas. Complicated modulation/demodulation is unnecessary, and transmission and reception can be achieved through digital circuits. This means that a level of energy consumption less than by using RF/millimeter waves. On the other hand, signal reflection can occur since matched termination cannot be performed. The data

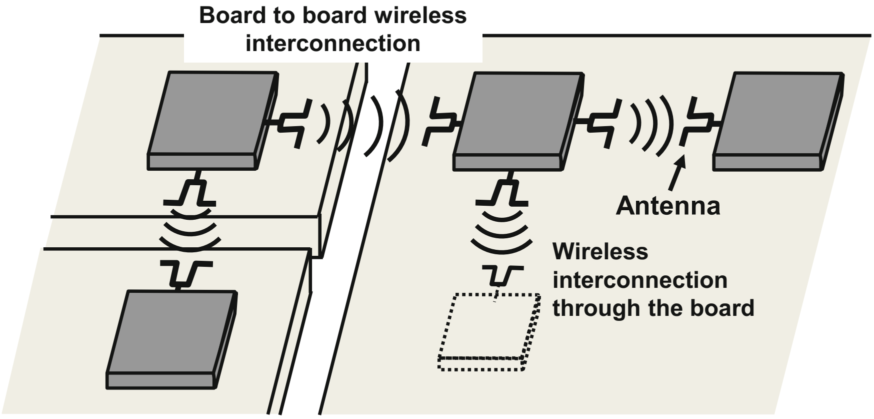

Board to board wireless interconnection
Antenna
Wireless interconnection through the board

Fig. 8.2 Wireless interconnection by millimeter wave technology

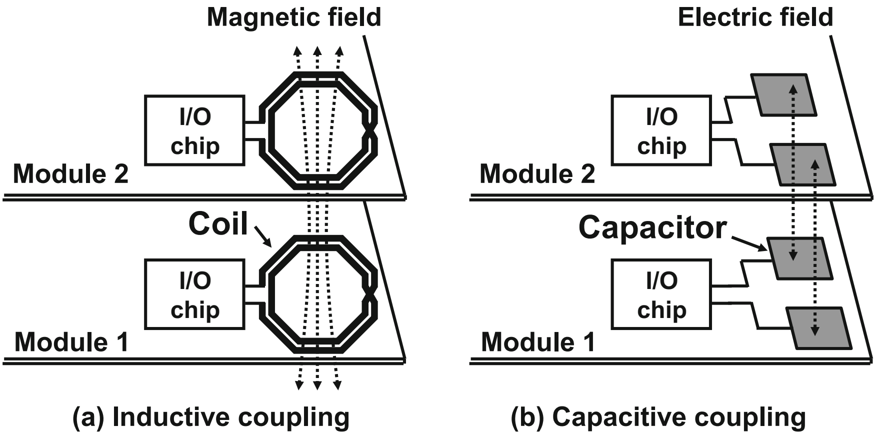


Fig. 8.3 Wireless interconnection by inductive/capacitive coupling

rate is consequently limited to values no greater than 5 Gb/s and it is necessary to position the I/O chips near the coupler.

(3) **Transmission line coupler (TLC)**: This technology is being researched as a means of achieving electromagnetic coupling in stacked transmission lines (Fig. 8.4) [9–12]. A TLC is advantageous because it can connect and branch signals without altering the characteristic impedances of the transmission lines. It can greatly improve the quality of communications. Transmission speeds of 12 Gb/s at a distance of 1 mm have been reported [9]. Here, however, signal energy drops as a result of electromagnetic coupling and DC signal components are lost, so amplification and restoration of those components are necessary at the receiver. Methods for achieving impedance matching and for achieving high-speed, low-energy communications are being researched (see Chap. 23).

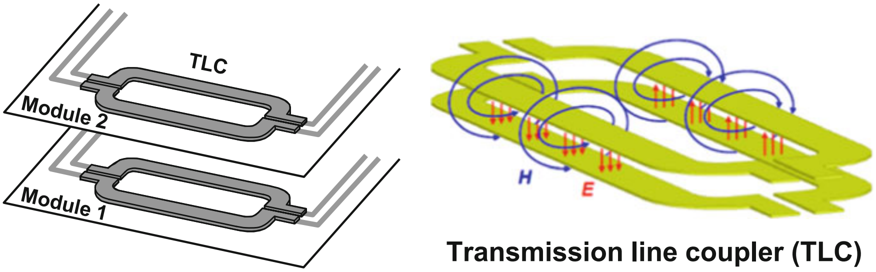


Fig. 8.4 Wireless interconnection by transmission line coupler (TLC)

8.1.4.3 Wireless Power Delivery

Power can be delivered wirelessly using magnetic coupling (see Chap. 24). This makes it unnecessary to equip a module with a power supply while also enabling connections to small modules. An electromagnetic induction system and electromagnetic resonance system for wireless power delivery are being researched. If the target of power delivery is an integrated circuit as opposed to a battery, the power supply current can change quickly and considerably due to load fluctuations, so high-speed power-delivery control is needed. Modulation control for suppressing unwanted radiation is being researched [13–15].

8.1.4.4 Problems and Countermeasures When Applying Wireless Interconnect Technology to Actual Systems

A major issue in wireless interconnect technology is the need for electromagnetic compatibility (EMC) measures. Effects and countermeasures for each of the items below are summarized.

(1) **Noise resistance**: Compared with conventional connectors, wireless interconnections can be easily affected by noise since received-signal power is low. Coding systems, the frequency band used, modulation/demodulation systems, and error detection and correction systems are being researched to improve noise resistance in wireless interconnections [12].

(2) **Unwanted radiation, intra-system EMC problem**: Couplers and antennas emit radio waves. This simple fact naturally raises concerns about Radio law compliance, interference with other wireless systems in the same cabinet or on the same chip, and mutual interference between wireless power-delivery and data communication systems. Research is being performed on means of reducing noise emissions through the use of industrial, scientific, and medical (ISM) radio bands, modulation control and coding techniques, etc. [12, 13].

8.1.5 Conclusion

The research and practical use of wireless interconnects have begun with the aim of improving the dependability of inter-module connections. Interest is growing, in particular, in noncontact connectors using near-field coupling.

8.2 Wireless Interconnect for Dependable Electronic Packaging

Hiroki Ishikuro, Keio University
Tadahiro Kuroda, Keio University

8.2.1 Demand of Wireless Interconnect for Electronic Packaging

The engineering of putting memory, processor, and other components together by mounting them on boards and connecting them each other to form a system is called packaging and has often been a challenge requiring a comprehensive and balanced approach covering systems performance, power dissipation, geometrical sizes, maintainability, costs, and so forth.

Required bus bandwidth between LSI chips such as processor and memory becomes wider and wider in recent electronic systems. In the conventional system-on-a-board, the performance of the processor core has been improved by 70% per year. However, the improvement of I/O bandwidth has stayed at 28% per year [16]. As a result, the performance gap between the bus bandwidth and processor core speed has increased as the technology is scaled.

Conventional wired interface suffers from the effect of parasitic inductance of bond wire and parasitic capacitance of ESD protection devices, resulting in limited bandwidth and increased power consumption. Wired connector for connection between modules also limits the bus bandwidth because it causes signal reflection by impedance mismatch and degrades signal quality. The other disadvantage of wired interface is high fabrication and assembly cost.

If wireless interconnect can be utilized for the interface or connector, various kinds of merits are obtained. Since the parasitic components can be reduced, the bandwidth can be increased, and in some cases, power consumption can be reduced. Assembly cost can also be decreased and flexibility of system configuration is improved because the package or module can easily be attached and detached. Dependable issue can be relaxed because mechanical metal contacts are eliminated. Wireless interconnect also brings waterproof and dust-resistant property to electronic systems.

8.2.2 Applications of Dependable Wireless Interconnect

There are many applications which can utilize the merits of wireless interconnect. Figure 8.5 shows some examples of such applications.

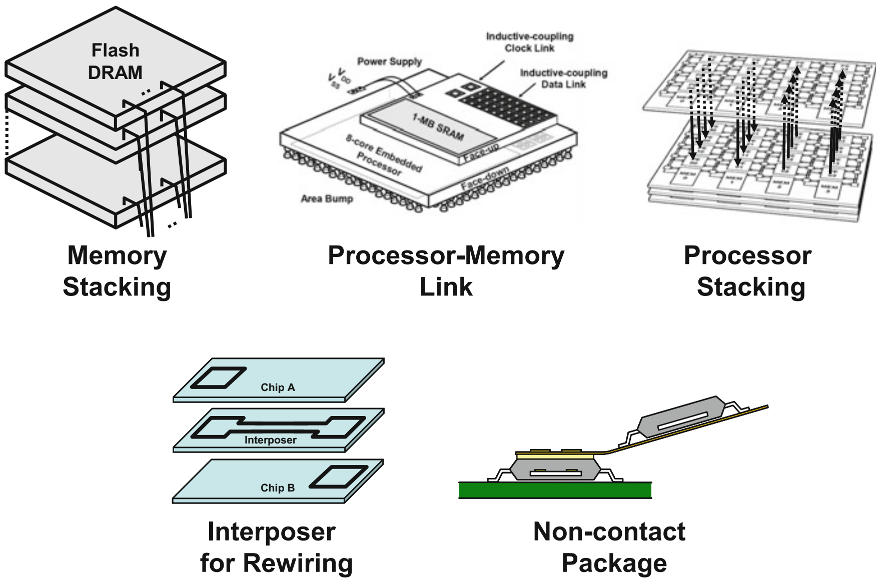


Fig. 8.5 Applications of wireless interconnect

3D system integration such as memory stacking [17], processor to memory link [18], and processor stacking [19] will enable high-performance, small size systems. Wireless interposer [20] will bring about flexibility to the chip assembling. Through-silicon-via (TSV) [21, 22] or through-package-via (TPV) is being intensively studied for wired interconnect in 3D system integration. However, the fabrication cost is high and yield of the assembly would be decreased by the contact failure, which increase the total module cost. If wireless interconnect can be used for 3D system integration, the fabrication and assembly cost can be dramatically decreased. Furthermore, it will allow system configurations to be more versatile and flexible and help reduce the turnaround time for system development.

Noncontact connector is another interesting wireless application. As described previously, the conventional connector has mechanical contacts. There is impedance mismatch at the contact which becomes the cause of signal reflection and limits the bandwidth by inter-symbol interference [23], which is eliminated in wireless connectors. The other problem of the conventional connector is that the form factor of a connector is determined by the contracting mechanism. Even a smallest connector is about 1 mm high to keep enough pressure at the contact surface. The wireless technique used for noncontact connector can be applied for noncontact bus probing in software debugging [24] as well.

Three types of couplers can be used for wireless proximity interconnect. The first one is an inductive coupling [25, 26] which uses small size inductors as a coupler. The second one uses capacitive coupling [27] between two metal plates. The third one is electromagnetic near-field coupling between transmission lines [9].

Since the magnetic field can penetrate into the silicon chip, inductive coupling technique can be used for face-up chip stacking and suited for scalable 3D integration. Inductive coupling can be used for noncontact connector as well. Capacitive coupling uses simple metal plates and can be easily patterned onto the silicon or PCB. However, electric field is easily shielded by silicon wafer, and therefore, capacitive coupling can only be used for face-to-face connections. Both inductive and capacitive couplings use lumped components (inductors or capacitors); their self-resonant frequency determines the bandwidth of the channel. Especially, if they are used for noncontact connector, the components will roughly be a millimeter in size for a practical coupling strength. The self-resonant frequency would therefore fall in several GHz, limiting the maximum data rate within around several Gb/s. On the other hand, if transmission lines with characteristic impedance matched with the impedance of feeding line are used for noncontact coupler, bandwidths wider than 10 GHz can be attained with millimeter dimensions, as described below in more detail.

8.2.3 Design of Wireless Interconnect Interfaces

8.2.3.1 Coupler Design

Figure 8.6 shows the conceptual view of the wireless interconnects which use lumped elements (inductive coupling) (a) and transmission lines (b). As previously mentioned, for the inductor sized about a millimeter, the resonance at several GHz limits the bandwidth of coupling. On the other hand, the frequency response of the transmission line coupler (TLC) is flat in a wide frequency range up to 10 GHz and higher (Fig. 8.7c).

For the same transmission distance, the size of the inductor is smaller than the TLC. As a result, inductors can be arranged in dense array as shown in Fig. 8.6. Figure 8.7 shows the relation between the inductor size and self-resonant frequency. The characteristics of an inductor patterned on flexible printed circuit (FPC) board and fabricated on silicon chip are shown. Since the parasitic capacitance between the inductor and silicon substrate is larger than between the inductor and FPC, the self-resonant frequency of on-chip inductor is lower than that of inductor on FPC board. If the required data rate is 1 Gbps, the width of the pulse signal used for communication should be shorter than 1 ns. The spectrum of the 1 ns band-limited pulse signal ranges from DC to 1 GHz. To prevent a ringing in the received signal, the self-resonant frequency should be several times higher than the spectrum of the pulse. Therefore, the size of the FPC inductor and on-chip inductor should be smaller than 1 mm and 0.6 mm, respectively. The size determines the communication distance between the inductors. There is thus a tradeoff between the data rate and communication distance.

Figure 8.8 shows simulated characteristics of TLC. The transmission lines of transmitter and receiver both have a differential structure. The frequency response

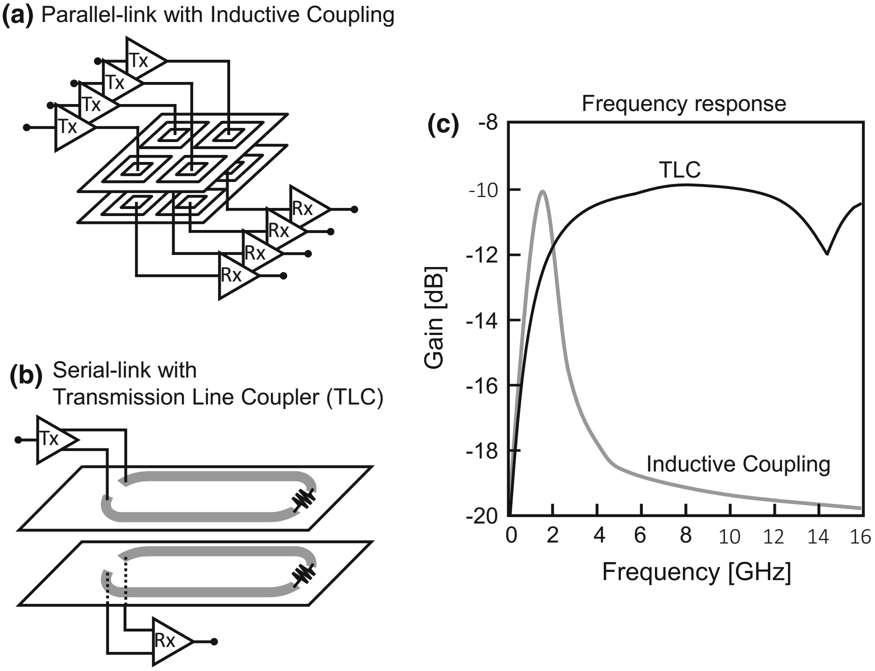


Fig. 8.6 Conceptual views of wireless link by inductive coupling (**a**) and transmission line type coupler (**b**). The channel frequency responses are shown in (**c**)

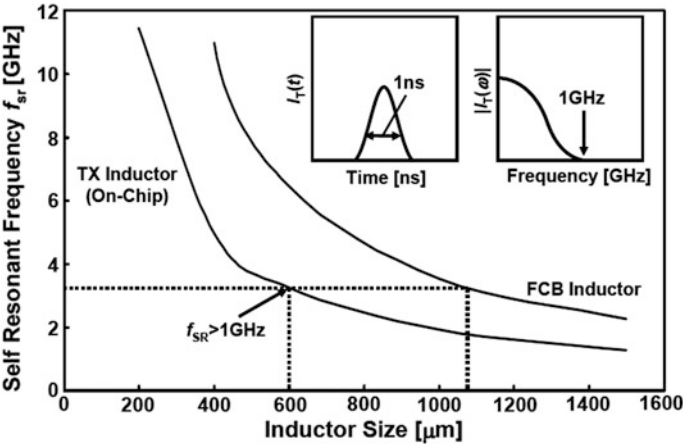


Fig. 8.7 Inductor design for inductive coupling link channel

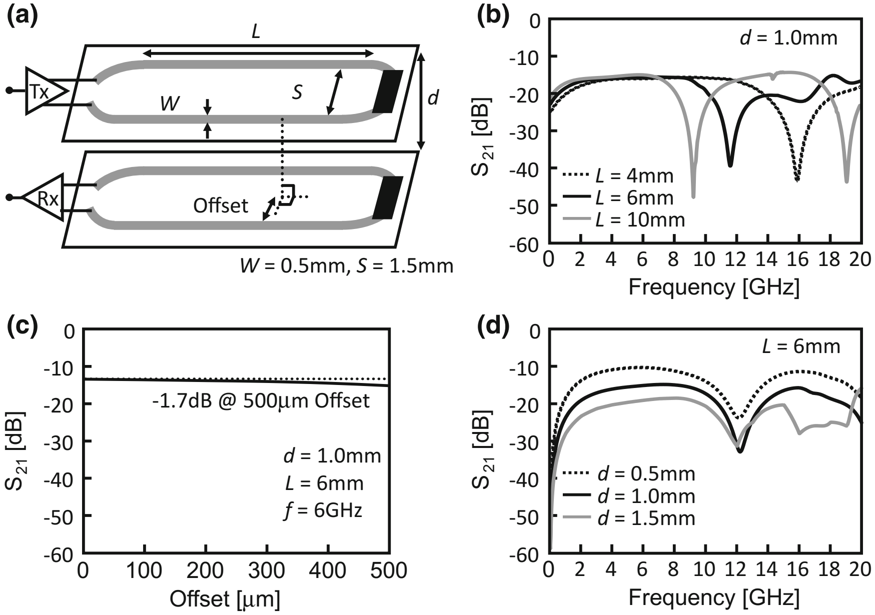


Fig. 8.8 Transmission line coupler and dependence of frequency response on design parameters

of the coupler is determined by three major design parameters. The length (L) of the coupler determines the bandwidth of the coupler. The width (W) and spacing (S) of the transmission lines determine the characteristic impedance and misalignment tolerance.

As shown in Fig. 8.8, if the coupler length is 6 mm, the bandwidth of the coupler is around 10 GHz, which is much wider than in the inductive coupling link. Even for an offset between the transmitter side and receiver side of 500 μm, the coupling coefficient (S_{21}) decreases only by 1.7 dB. Even when the distance between the coupler is changed, the coupling bandwidth of the coupler remains unchanged. These results demonstrate that the TLC has enough tolerance against misalignment and distance variation, and can be used for wireless interconnect.

8.2.3.2 Transceiver Circuit Design

Implementation of the transceiver circuit for wireless interconnect is simple. Unlike transceivers used in wireless telecommunications, the transceiver for wireless interconnect does not involve either carrier or intermediate frequencies so that local oscillator can be eliminated, which makes it possible to use a simple circuit with low power operation.

There are two signaling schemes (Fig. 8.9). One is for synchronous detection and the other is for asynchronous detection. In both schemes, the receiver receives

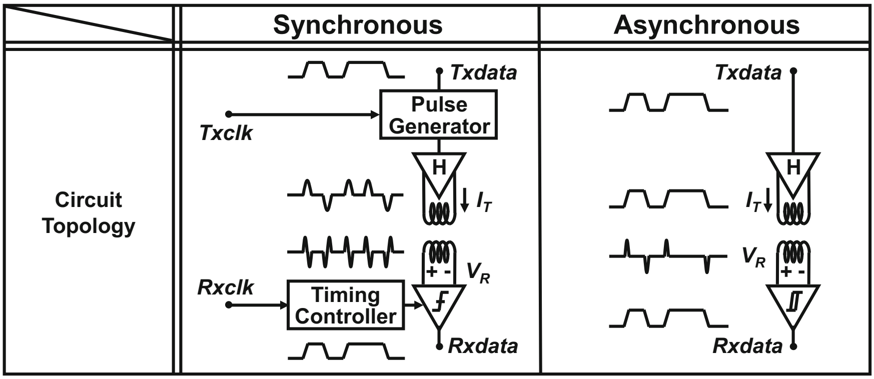


Fig. 8.9 Signaling for high-speed wireless interconnect

pulse signal because the coupler cannot transfer low-frequency component of the transmitted signal.

In the synchronous scheme, the current pulses are generated by a transmitter circuit and fed into the coupler. The polarity of the pulse is determined by the transmitting binary data. That is, a positive pulse is generated if the transmitting data is "1" and a negative pulse is generated if the data is "0". On the receiver side, the pulse polarity is detected by a comparator at the timing of RX clock edge which is synchronized with the transmitter clock by a clock recovery circuit. Since both the transmitter and receiver (clocked comparator) consume power only at the rising edge of the clock, the transceiver operates at low power with a high noise immunity. However, precise timing control is required to decide the polarity of the received short pulses.

In the asynchronous scheme, a current signal whose waveform is same as the transmitting NRZ data is fed into the transmitter coil, inducing pulses on the receiver side at the transition points of the transmitted data. The original NRZ data can be recovered by using a hysteresis comparator. Since the data can be recovered asynchronously, the precise clock timing control for data recovery is not required. On the other hand, the receiver circuit is always active and can be disturbed by the noise. The power consumption is larger compared with the synchronous receiver.

8.2.4 System Examples of Wireless Interconnect

8.2.4.1 Wireless Bus Probe System with Inductive Coupling Link

Figure 8.10 shows a detachable wireless interface developed in the authors' group [24] for the purpose of processor bus monitoring in firmware debugging. The wireless probe consists of inductors that are patterned in a flexible circuit board

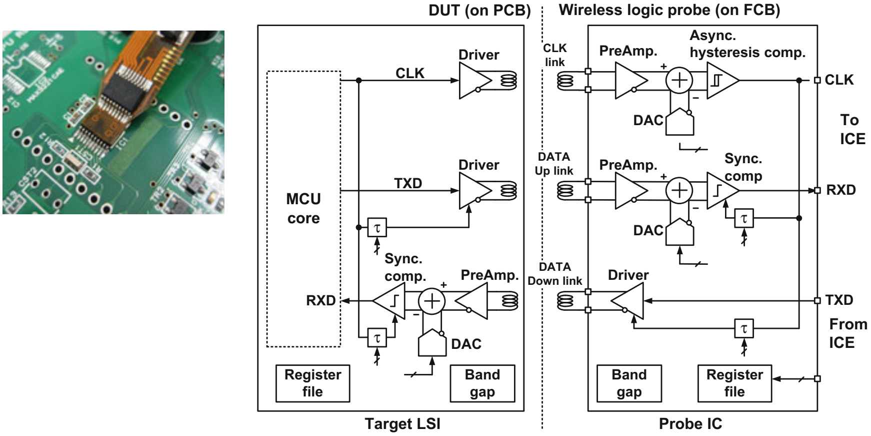


Fig. 8.10 System diagram of wireless bus probe

(FCB) and a transceiver IC. In this experiment, an MCU chip housed in a 1-mm-thick SSOP package was chosen as the target LSI. The target LSI also contains a pulse transceiver with on-chip inductors formed by the top metal layer. An asynchronous channel for clock link and synchronous channels for full-duplex data up/downlinks are integrated. System clock of the target LSI is transmitted to the wireless probe, recovered by a hysteresis comparator, and then used for data synchronization in probe IC. The inductors in the FCB and the target LSI are 1.0 mm and 0.6 mm^2, respectively. Considering that the self-resonant frequency is 2 GHz, the pulse width is set to 1 ns.

To extend the communication range under the size limitation of the inductor, received signals are amplified by 30 dB using a 2-stage complementary differential amplifier prior to the comparator. DC offsets of the amplifier and the comparator could cause a serious problem during signal detection. In this receiver, a 6-bit current steering DAC is used for the offset cancellation.

In Fig. 8.11, measured received pulse waveform (a) and alignment tolerance (b) are shown. The received waveform has distinct double peaks with a small ringing, confirming that it can be easily decoded back into the original signals. The alignment tolerance of 0.5 mm is sufficient to allow hand attachment of the probe. Since this application does not require a wide bandwidth, the data rate of the interface is set at 20 Mbps. Detachable wireless interface with much wider total bandwidth (2.5 Gbps) has been also reported [26].

8.2.4.2 Wideband Wireless Interconnect with TLC for Memory Card

Figure 8.12 shows the chip micrograph and the evaluation module of wireless interface for a wideband noncontact connector [9]. A test chip fabricated in 90 nm

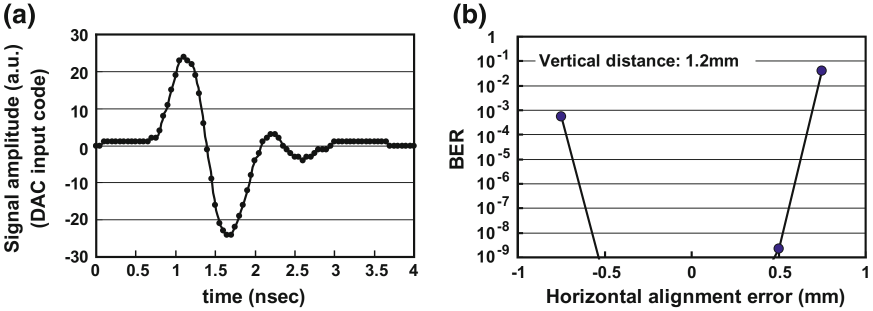


Fig. 8.11 The measured waveform and bathtub curve for alignment

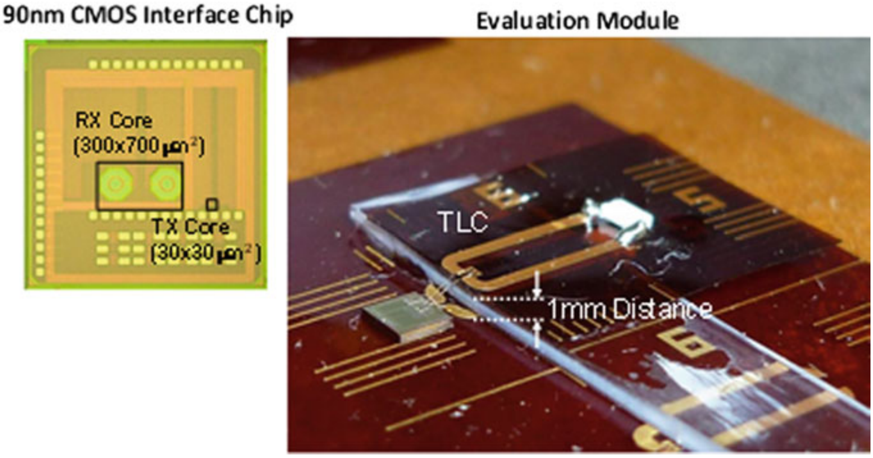


Fig. 8.12 Wireless connector with TLC

CMOS process integrates a transmitter and a receiver. The transmission line coupler was designed to have a 3 dB bandwidth from 2.6 to 9 GHz. The coupling coefficient (S_{21}) of the designed link at 1 mm is −16 dB.

The system BER is evaluated at various data rates. The transceiver successfully achieves BER < 10^{-13} at 12.5 Gb/s with d = 0.5 mm and 12 Gb/s with d = 1 mm. To evaluate the interference due to the wireless power delivery at 13.56 MHz, a 20 mm × 20 mm coil is built outside the data link on the same FPC boards. The measured bathtub curves with and without power delivery are presented in Fig. 8.13. With a current of 75 $\mathrm{mA_{rms}}$ at 13.56 MHz surrounding the data channel, the timing margin with power delivery is slightly smaller but still sufficient. This confirms that the directional coupling link can be implemented together with power-delivery inductors.

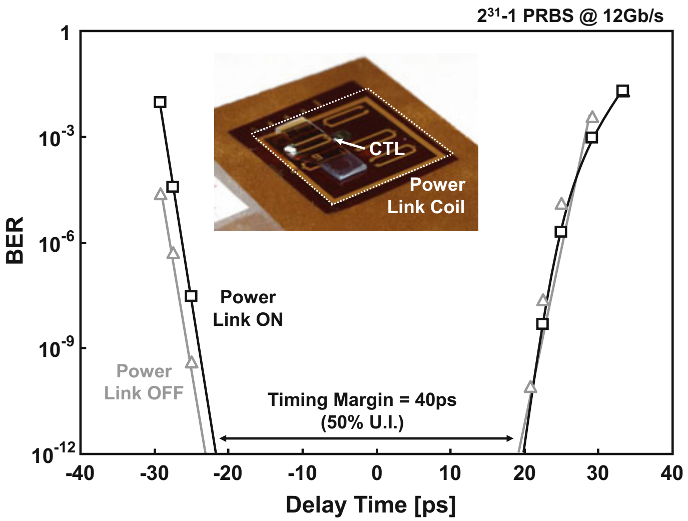


Fig. 8.13 Measured bathtub curve with and without simultaneous wireless power transmission

8.3 Connectivity Issues in 3D Integration

Mitsumasa Koyanagi, Tohoku University
Kang Wook Lee, Tohoku University
Hiroyuki Hashimoto, Tohoku University
Makoto Motoyoshi, Tohoku MicroTech Co., Ltd

8.3.1 Connectivity in 3D Integration

The signal propagation delay and the power consumption by the interconnections seriously increase as the LSI capacity and packing density increase in conventional 2D LSIs. In addition, I/O circuits in LSI tend to consume more power to rapidly drive the output pins and the external wiring with large capacitances and inductances in package and printed circuit boards. As a result, it becomes more and more difficult to achieve high performance and low power consumption in 2D LSIs. To overcome these concerns in conventional 2D LSIs caused by scaling-down the device size, it is indispensable to introduce the concept of 3D integration into 2D integration. The problems in 2D LSIs can be solved by vertically stacking several chips and connecting them with the through—silicon vias (TSV's) after dividing a large chip into several smaller chips as shown in Fig. 8.14. The 3D integration provides many advantages such as short interconnect length and high connectivity,

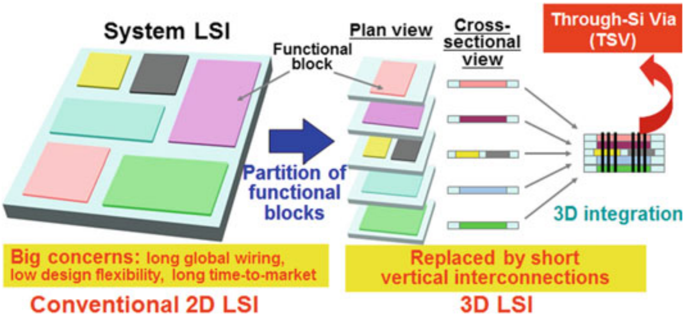

System LSI
Functional block
Plan view
Cross-sectional view
Through-Si Via (TSV)
Partition of functional blocks
3D integration
Big concerns: long global wiring, low design flexibility, long time-to-market
Conventional 2D LSI
Replaced by short vertical interconnections
3D LSI

Fig. 8.14 Advantages of 3D LSI over conventional 2D LSI

high packing density, high performance, and low power consumption. In 3D LSIs, a huge number of short vertical interconnections can be easily formed using TSVs which are suited for parallel processing. In addition, the 3D integration enables a heterogeneous integration in which various kinds of device chips with different sizes, different devices, and different materials are vertically stacked. Therefore, chip stacking using the TSV has been attracting considerable attention from many researchers in the LSI device and package technology areas [28–35]. We can easily reduce the wiring length, the pin capacitance, the chip size, and the microbump pitch by employing 3-D LSIs and consequently we can increase the signal processing speed and decrease the power consumption. 3-D LSIs are also useful for increasing the wiring connectivity within a chip. It, therefore, becomes possible to produce new LSIs with high connectivity such as real-time image processing chips, neuromorphic chips, memory-merged processor chips, and intelligent memory chips by using 3-D LSIs [36–39]. However, several connectivity issues have to be solved to achieve reliable 3D LSIs.

8.3.2 Reliability Issues of Connectivity in 3D Integration

Several thinned LSI chips with TSVs and metal microbumps are vertically stacked in a 3D LSI as shown in Fig. 8.15 [40, 41]. We have various kinds of reliability issues in 3D integration as shown in Fig. 8.16. The 3D integration technology is classified into three categories by TSV fabrication process, namely, the via-first, via-middle, and via-last. The via-middle and back-via type via-last methods are widely used to fabricate 3D LSIs. Deep trenches are formed by RIE (Reactive Ion Etching) after the transistor formation in the via-middle process. These deep trenches are filled with Cu by electroplating after forming the oxide liner, barrier metal layer, and Cu seed layer inside trenches. Then, the multilevel metallization layers are formed on the TSVs after Cu CMP (Chemical Mechanical Polishing). The LSI wafer with Cu-TSVs is temporarily bonded onto a support wafer after the formation

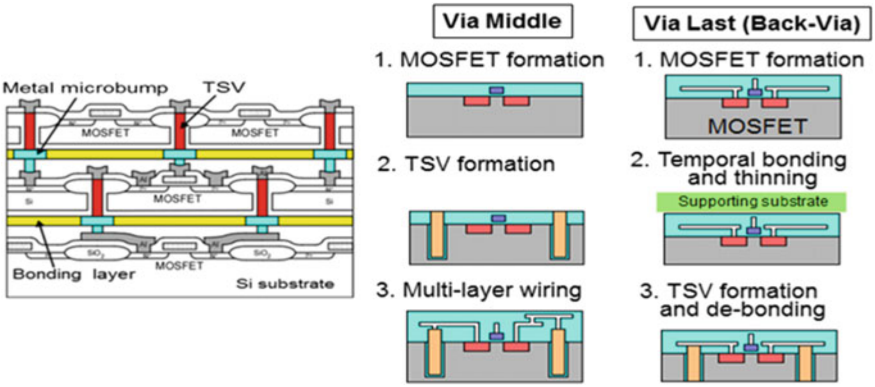


Fig. 8.15 Two kinds of TSV technologies, via-middle versus back-via

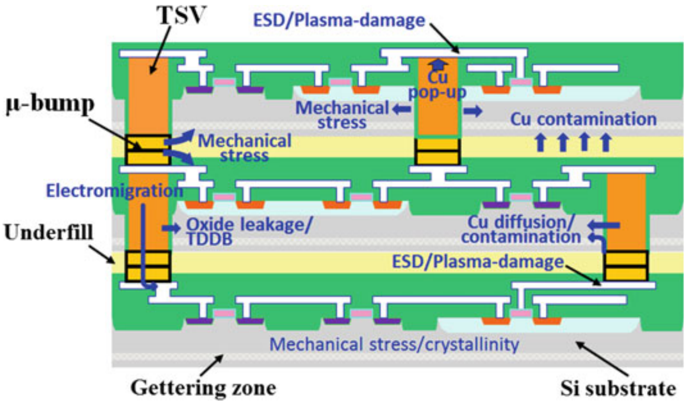


Fig. 8.16 Reliability issues in 3D LSI

of metal (CuSn or CuSnAg) microbumps, and then thinned from the backside by the mechanical grinding and CMP. Metal microbumps are again formed on the bottom of Cu-TSVs after exposing them. Then, the support wafer is de-bonded from the thinned LSI wafer and thinned chips with Cu-TSVs and metal microbumps are vertically stacked. In such via-middle process, serious issue of Cu pop-up occurs in the BEOL process step since the Cu-TSVs are exposed to the thermal treatment at higher than 350 °C [42]. A rapid crystal grain growth occurs in Cu of TSV at the annealing temperature higher than 350 °C which causes the Cu protrusion upward in TSV as shown in Fig. 8.17a. Such Cu pop-up gives rise to serious damages to lower level metallization layers and low-k interlayer dielectrics and consequently causes serious reliability issues of connectivity in 3D LSIs. We also have to be careful with Cu contamination from the Cu-TSV and the backside surface in the via-middle process since the process temperature is higher than that of

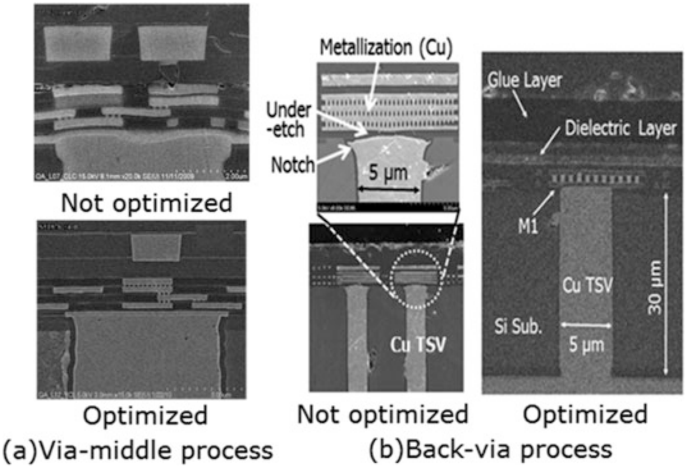


Fig. 8.17 Connection failures associated with TSVs in 3D LSI

back-via process [43–45]. The Cu diffusion constant in Si and oxide rapidly increases as the process temperature increases.

In the back-via process, Cu-TSVs are fabricated after the Si substrate thinning. The LSI wafer with metal microbumps is temporarily bonded onto a support wafer and then the deep trench is formed from the backside by RIE after thinning the Si substrate. After that, the interlayer dielectric under the first-level metallization exposed at the bottom of deep trench is etched off by RIE to expose the first-level metallization layer (M1) and then the oxide liner is deposited. This process step is followed by the selective etching of oxide liner at the bottom of deep trench to expose again the first-level metallization layer (M1). Then, the deep trench is filled with Cu by electroplating after the formation of barrier metal layer and Cu seed layer. Metal microbumps are also formed on the Cu-TSV at the backside. Then, thinned chips with Cu-TSVs and metal microbumps are vertically stacked after the support wafer is de-bonded. In such back-via process, serious issue of Si “notch” occurs in the deep trench formation by RIE since the interlayer dielectric under the first-level metallization is exposed after the deep Si trench etching. This exposed interlayer dielectric is charged up during over-etching, and consequently the Si substrate around the bottom of deep trench is side-etched to cause Si “notch” as shown in Fig. 8.17b. Another difficult process step is the oxide liner removal at the bottom of deep trench. The oxide liner at the bottom of deep trench has to be selectively removed by RIE without damaging the oxide liner at the trench sidewall. Highly anisotropic plasma etching is necessary for the selective removal of the oxide liner at the bottom of deep trench. These “notch” and the oxide liner remaining at the bottom of deep trench cause serious reliability issues of connectivity in 3D LSLs as well. Mechanical stress induced by Cu-TSVs and metal microbumps, and crystal defects and crystal structure changes produced by thinning the Si substrate are also big concerns in 3D LSIs [46, 47]. Both tensile and compressive stresses are induced by Cu-TSVs and metal microbumps. These mechanical stresses cause significant changes in transistor current. The current change increases as the distance between the transistor and TSV or metal microbump is reduced. Therefore, transistors should not be placed inside a specific area around a TSV or a metal microbump which is called a keep-out zone (KOZ) to minimize the current change by mechanical stresses. Crystal defects and crystal structure changes produced by thinning the Si substrate decrease the minority carrier lifetime.

In order to solve these reliability issues of connectivity in 3D integration, it is indispensable to employ TSV self-test and self-repair circuits [48]. Vertical connections using TSVs should be repaired avoiding the faulty TSVs by the TSV repair techniques as shown in Fig. 8.18. Various TSV repair technologies such as the multiplexed TSV technique and the redundant TSV technique have been proposed so far [21, 49]. More TSVs are required for each signal pin in the multiplexed TSV technique. For example, the double TSV or quadruple TSV needs two or four times TSVs compared to single TSV. Meanwhile, extra switching circuits are necessary for the redundant TSV technique. The overall TSV stacking yield is plotted as a function of TSV failure rate in Fig. 8.19 [50]. As is obvious in the figure, the stacking yield is significantly improved by introducing the multiplexed TSV technique and the redundant TSV technique. In addition, it turns out that the quadruple TSV gives rise to the highest stacking yield among all of TSVs shown. For large-pitch TSVs, TSV with repair circuit has much smaller area impact than double or quadruple TSV although it needs additional circuits for repair in order to assign signals uniquely to an appropriate TSV. As shown in Fig. 8.19, the redundant TSV technique with larger selectors, especially 16 signals of 20 TSVs, provides much higher stacking yield as compared to 4 signals of 6 TSVs or 8 signals of 10 TSVs although wider switches are needed to implement the selector.

The quadruple TSVs are useful for bonding pads because it is difficult to implement repair circuit for input/output pads or power/ground pads. On the other

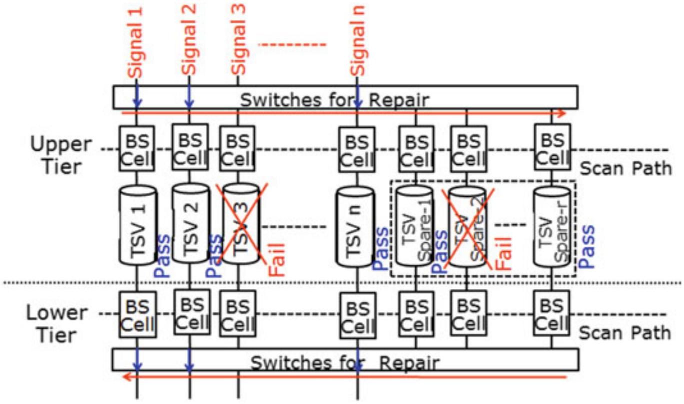


Fig. 8.18 Self-test and self-repair for TSVs by boundary scan

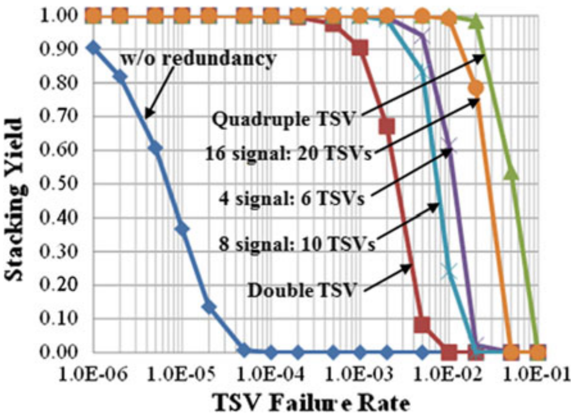


Fig. 8.19 Overall TSV stacking yield for 100,000 vertical signals as a function of TSV failure rate

hand, TSVs with repair circuit using the selectors for 16 signals of 20 TSVs are preferred for internal signals and adopted to achieve higher repairability and lower area cost without using extra redundant TSVs.

8.3.3 Circuit Design Issues of Connectivity in 3D Integration

We can significantly increase the connectivity and the data bandwidth using TSVs in 3D LSIs decreasing the total wiring length. To maximize such advantages in 3D LSIs, the resistance and capacitance of TSV should be minimized. The power delivery to upper or lower layers in 3D LSIs is performed through TSVs, and hence resistances of TSVs for power line and ground line should be as small as possible to guarantee power integrity (PI) and signal integrity (SI). It is preferable to employ Cu-TSVs with larger diameter as those for power line and ground line since the TSV resistance decreases. It is also effective to connect several TSVs in parallel to decrease the TSV resistance. On the other hand, capacitances of TSVs for signals should be reduced as much as possible to increase the data transfer speed through TSVs. It is also effective to reduce TSV capacitances for decreasing the power consumption of TSV driver circuits. The diameter and length of TSV should be decreased increasing the oxide liner thickness in order to reduce TSV capacitance as shown in Fig. 8.20a. The delay time of TSV driver circuit is plotted as a function of TSV length in Fig. 8.20b where the oxide liner thickness is changed as a parameter. The TSV diameter is 5 μm. The driver circuits were optimized for each technology node. It is obvious from the figure that the delay time decreases down to 100 ps by employing TSVs with the diameter less than 5 μm, the length less than 50 μm, and the oxide liner thicker than 0.5 μm. This means that an extremely high data bandwidth of more than 1 TBps can be achieved by parallel data bus with a thousand of TSVs. In such 3D LSIs with high data bandwidth, the clock skew is

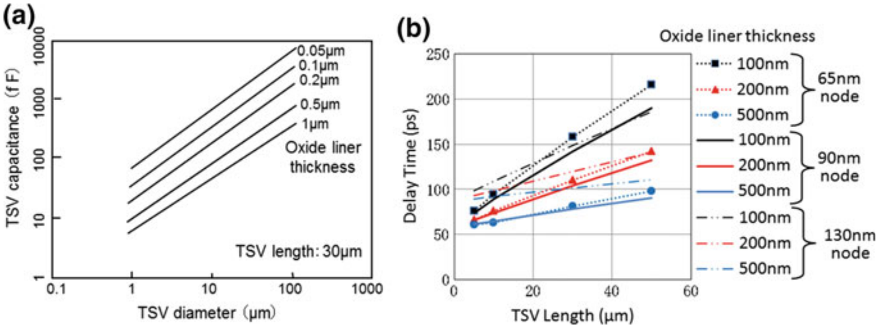


Fig. 8.20 **a** TSV capacitance as a function of TSV diameter and **b** delay time of TSV driver circuit as a function of TSV length

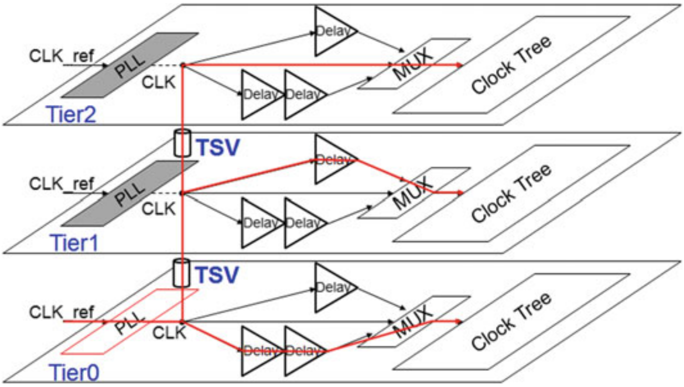


Fig. 8.21 Clock delivery in 3D LSI

another crucial issue since the clock delivery among many layers in 3D LSI is also performed through TSVs as shown in Fig. 8.21. Therefore, careful design to minimize the clock skew is indispensable in 3D LSIs introducing delay circuits.

References

1. J. Lee et al., A low-power fully integrated 60 GHz transceiver system with OOK modulation and on-board antenna assembly, in *IEEE International Solid-State Circuits Conference (ISSCC'09). Digest of Technical Papers*, February 2009, pp. 316–317
2. Y. Tanaka et al., A versatile multi-modality serial link, in *IEEE International Solid-State Circuits Conference (ISSCC'12). Digest of Technical Papers*, February 2012, pp. 332–333
3. T. Abe et al., A 2 Gb/s 150 mW UWB direct-conversion coherent transceiver with IQ-switching carrier recovery scheme, in *IEEE International Solid-State Circuits Conference (ISSCC'12). Digest of Technical Papers*, February 2012, pp. 442–443

4. M. Tamura et al., A 1 V 357 Mb/s-throughput transferjet™ SoC with embedded transceiver and digital baseband in 90 nm CMOS, in *IEEE International Solid-State Circuits Conference (ISSCC'12). Digest of Technical Papers*, February 2012, pp. 440–441
5. S. Kawai et al., A 2.5 Gb/s/ch inductive-coupling transceiver for non-contact memory card, in *IEEE International Solid-State Circuits Conference (ISSCC'10). Digest of Technical Papers*, February 2010, pp. 264–265
6. H. Cho et al., A 1.2 Gb/s 3.9 pJ/b, mono-phase pulse-modulation inductive-coupling transceiver for mm-range board-to-board communication, in *IEEE International Solid-State Circuits Conference (ISSCC'13). Digest of Technical Papers*, February 2013, pp. 202–203
7. K. Hijioka et al., A 5.5 Gb/s 5 mm contactless interface containing a 50 Mb/s bidirectional sub-channel employing common-mode OOK signaling, in *IEEE International Solid-State Circuits Conference (ISSCC'13). Digest of Technical Papers*, February 2013, pp. 406–407
8. K. Ikeuchi et al., 500 Mbps, 670 μW/pin capacitively coupled receiver with self reset scheme for wireless connectors, in *IEEE Asian Solid-State Circuits Conference (A-SSCC'08). Digest of Technical Papers*, November 2008, pp. 93–96
9. T. Takeya et al., A 12 Gb/s non-contact interface with coupled transmission lines, in *IEEE International Solid-State Circuits Conference (ISSCC'11). Digest of Technical Papers*, February 2011, pp. 492–493
10. W.-J. Yun et al., A 7 Gb/s/Link non-contact memory module for multi-drop bus system using energy-equipartitioned coupled transmission line, in *IEEE International Solid-State Circuits Conference (ISSCC'12). Digest of Technical Papers*, February 2012, pp. 52–53
11. W. Mizuhara et al., A 0.15 mm-thick non-contact connector for MIPI using vertical directional coupler, in *IEEE International Solid-State Circuits Conference (ISSCC'13). Digest of Technical Papers*, February 2013, pp. 200–201
12. A. Kosuge et al., An electromagnetic clip connector for in-vehicle LAN to reduce wire harness weight by 30%, in *IEEE International Solid-State Circuits Conference (ISSCC'14). Digest of Technical Papers*, February 2014, pp. 496–497
13. R. Shinoda et al., Voltage-boosting wireless power delivery system with fast load tracker by ΔΣ-modulated sub-harmonic resonant switching, in *IEEE International Solid-State Circuits Conference (ISSCC'12). Digest of Technical Papers*, February 2012, pp. 288–289
14. K. Tomita et al., 1 W 3.3 V-to-16.3 V boosting wireless power transfer circuits with vector summing power controller, in *IEEE Asian Solid-State Circuits Conference (ASSCC'11). Digest of Technical Papers*, November 2011, pp. 177–180
15. Y. Hasegawa et al., Single-inductor-dual-output wireless power receiver with synchronous pseudo-random-sequence PWM switched rectifiers, in *IEEE Asian Solid-State Circuits Conference (A-SSCC'13). Digest of Technical Papers*, November 2013, pp. 261–264
16. H. Ishikuro, T. Kuroda, Wireless proximity interfaces with a pulse-based inductive coupling technique. IEEE Commun. Mag. **48**(10), 192–199 (2010)
17. M. Saito, N. Miura, T. Kuroda, A 2 Gb/s 1.8pJ/b/chip inductive-coupling through-chip bus for 128-Die NAND-Flash memory stacking, in *IEEE International Solid-State Circuits Conference (ISSCC). Digest of Technical Papers*, February 2010, pp. 440–441
18. K. Niitsu, Y. Shimazaki, Y. Sugimori, Y. Kohama, K. Kasuga, I. Nonomura, M. Saen, S. Komatsu, K. Osada, N. Irie, T. Hattori, A. Hasegawa, T. Kuroda, An inductive-coupling link for 3D integration of a 90 nm CMOS processor and a 65 nm CMOS SRAM, in *IEEE International Solid-State Circuits Conference (ISSCC'09). Digest of Technical Papers*, February 2009, pp. 480–481
19. Y. Kohama, Y. Sugimori, S. Saito, Y. Hasegawa, T. Sano, K. Kasuga, Y. Yoshida, K. Niitsu, N. Miura, H. Amano, T. Kuroda, A scalable 3D processor by homogeneous chip stacking with inductive-coupling link, in *2009 Symposium on VLSI Circuits. Digest of Technical Papers*, June 2009, pp. 94–95
20. S. Kawai, H. Ishikuro, T. Kuroda, A 4.7 Gb/s inductive coupling interposer with dual mode modem, in *2009 Symposium on VLSI Circuits. Digest of Technical Papers*, June 2009, pp. 92–93

21. U. Kang et al., 8 Gb 3D DDR3 DRAM using through-silicon-via technology, in *IEEE International Solid-State Circuits Conference Digest of Technical Papers (ISSCC)*, February 2009, pp. 130–131
22. H. Yoshikawa et al., Chip scale camera module (CSCM) using through-silicon-via (TSV), in *IEEE International Solid-State Circuits Conference (ISSCC). Digest of Technical Papers*, February 2009, pp. 476–477
23. B. Razavi, *RF Microelectronics*, 2nd edn., Chap. 3 (Prentice Hall, 2011)
24. H. Ishikuro, T. Sugahara, T. Kuroda, An attachable wireless chip access interface for arbitrary data rate using pulse-based inductive-coupling through LSI package, in *IEEE International Solid-State Circuits Conference (ISSCC). Digest of Technical Papers*, February 2007, pp. 360–361
25. D. Mizoguchi, Y.B. Yusof, N. Miura, T. Sakurai, T. Kuroda, A 1.2 Gb/s/pin wireless superconnect based on inductive inter-chip signaling (IIS), in *IEEE International Solid-State Circuits Conference (ISSCC). Digest of Technical Papers*, February 2004, pp. 142–143
26. N. Miura, D. Mizoguchi, M. Inoue, K. Niitsu, Y. Nakagawa, M. Tago, M. Fukaishi, T. Sakurai, and T. Kuroda, A 1 Tb/s 3 W inductive-coupling transceiver for 3D-stacked inter-chip clock and data link. IEEE J. Solid-State Circuits **42**(1), 111–122 (2007)
27. A. Fazzi, L. Magagni, M. Mirandola, B. Charlet, L. Di Cioccio, E. Jung, R. Canegallo, R. Guerrieri, 3-D capacitive interconnections for wafer-level and die-level assembly. IEEE J. Solid-State Circuits **42**(10), 2270–2282 (2007)
28. M. Koyanagi, in *8th Symposium on Future Electron Devices* (1989), pp. 50–60
29. T. Matsumoto, M. Koyanagi et al., in *International Conference on Solid State Devices and Materials (SSDM)* (1995), pp. 1073–1074
30. M. Koyanagi et al., IEEE Micro **18**(4), 17–22 (1998)
31. J.A. Davis, J.D. Meindl et al., Proc. IEEE **89**(3), 305–324 (2001)
32. P. Ramm et al., in *International Interconnect Technology Conference (IITC)* (2001), pp. 160–162
33. J. Burns et al., in *International Solid State Circuits Conference (ISSCC)* (2001), pp. 268–269
34. M. Bohr, in *International Electron Devices Meeting (IEDM). Technical Digest* (2011), pp. 1–4
35. M. Koyanagi, in *International Electron Devices Meeting IEDM. Technical Digest* (2013), pp. 8–15
36. M. Koyanagi et al., in *International Solid State Circuits Conference (ISSCC)* (2001), pp. 270–271
37. H. Kurino, M. Koyanagi et al., in *International Electron Devices Meeting (IEDM)* (1999), pp. 879–882
38. K.W. Lee, M. Koyanagi et al., in *International Electron Devices Meeting (IEDM)* (2000), pp. 165–168
39. T. Ono, M. Koyanagi et al., in *International Symposium on Low-Power and High-Speed Chips (COOL Chips V)* (2002), pp. 186–193
40. M. Koyanagi et al., IEEE Trans. Electron Devices **53**(11), 2799–2808 (2006)
41. M. Koyanagi et al., Proc. IEEE **97**(1), 49–59 (2009)
42. M. Murugesan, M. Koyanagi et al., in *International Electron Devices Meeting (IEDM)* (2011), pp. 139–142
43. J.-C. Bea, M. Koyanagi et al., IEEE Electron Device Lett. **32**(1), 66–68 (2011)
44. J.-C. Bea, M. Koyanagi et al., IEEE Electron Device Lett. **32**(7), 940–942 (2011)
45. K.-W. Lee, M. Koyanagi et al., IEEE Electron Device Lett. **33**(9), 1297–1299 (2012)
46. H. Kino, M. Koyanagi et al., Jpn. J. Appl. Phys. **52**(4, 2), 04CB11-1–04CB11-6 (2013)
47. K.-W. Lee, M. Koyanagi et al., IEEE Electron Devices Lett. **34**(8), 1038–1040 (2013)
48. H. Hashimoto, M. Koyanagi et al., in *International Conference on Solid State Devices and Materials (SSDM)* (2011), pp. 168–169
49. L. Jiang et al., IEEE Trans. Comput. Aided Des. Integr. Circuits Syst. 559–571 (2013)
50. H. Hashimoto, M. Koyanagi et al., IEEE 3DIC, October 2013

Chapter 9
Responsiveness and Timing

Tomohiro Yoneda, Yoshihiro Nakabo, Nobuyuki Yamasaki, Masayoshi Takasu, Masashi Imai, Suguru Kameda, Hiroshi Oguma, Akinori Taira, Noriharu Suematsu, Tadashi Takagi and Kazuo Tsubouchi

Abstract This chapter deals with the issue of timing and synchronicity, which is fundamental in the architecture design of computer, communication, and control systems. In fact, if a signal took too long to travel from one point in a system to another exceeding the predetermined length of time, then the system would involve an error, fault, or failure. An electromechanical robot would lose intended integrity in coordinated limb motions without responsive signals arriving in time from elsewhere in its distributed hard real-time control system. Successful delivery of a universal clock signal would be indispensable for distributed coupled computer-and-communication systems for real-time financial transactions. Section 9.1 describes

T. Yoneda (✉)
National Institute of Informatics, Tokyo, Japan
e-mail: yoneda@nii.ac.jp

Y. Nakabo
National Institute of Advanced Industrial Science and Technology (AIST), Tsukuba, Japan
e-mail: nakabo-yoshihiro@aist.go.jp

N. Yamasaki · M. Takasu
Keio University, Yokohama, Japan
e-mail: yamasaki@ny.ics.keio.ac.jp

M. Takasu
e-mail: takasu@ny.ics.keio.ac.jp

M. Imai
Hirosaki University, Hirosaki, Japan
e-mail: miyabi@eit.hirosaki-u.ac.jp

S. Kameda · A. Taira · N. Suematsu · T. Takagi · K. Tsubouchi
Tohoku University, Sendai, Japan
e-mail: kameda@riec.tohoku.ac.jp

N. Suematsu
e-mail: suematsu@riec.tohoku.ac.jp

T. Takagi
e-mail: t-takagi@riec.tohoku.ac.jp

S. Asai (ed.), *VLSI Design and Test for Systems Dependability*,
https://doi.org/10.1007/978-4-431-56594-9_9

the requirements in hard real-time control system such as industrial and humanoid robots. Section 9.2 is a proposal of a computer architecture for hard real-time control that is capable of pre-emptive multiple-thread computation on demand and noise-immune communications between distributed sensor–actuator nodes. This architecture, called RMTP (Real-Time Multithread Processor), has been implemented in compact 3-D modules and made available for academic uses along with the design tools. Section 9.3 describes asynchronous networks which can efficiently and reliably connect on-chip and off-chip functions in a distributed system against timing errors. The use of a global synchronization in public wireless telecommunication is proposed in Sect. 9.4 to provide dependable connectivity and maximized throughput using the satellites and cellular base stations with heterogeneous air interfaces.

Keywords Cyber-physical system • Feedback control • D-RMTP Prioritized SMT execution • IPC control • Networks-on-chip Asynchronous circuits • Synchronized SS-CDMA • Nanosecond order clock synchronization

9.1 Responsiveness for Hard Real-Time Control

Yoshihiro Nakabo, National Institute of Advanced Industrial Science and Technology (AIST)

9.1.1 Dependability of Real-Time Control Systems

In this section, we discuss dependability in communication and control. With respect to the safety of communication and control, there is a framework for functional safety of IEC 61508 [1] as criteria of dependability of systems. On the other hand, real-time property becomes a major problem of dependability for the time response of the systems. We discuss how dependability ensures safety and time response to communication and control systems.

There are two types of real-time system which takes priority in response time: soft real-time and hard real-time. The hard real-time system is that the system has no meaning to respond or fall into a dangerous or undesirable state as a system when a certain response time or deadline has passed. On the other hand, the soft

K. Tsubouchi
e-mail: tsubo@riec.tohoku.ac.jp

H. Oguma
National Institute of Technology, Toyama College, Toyama, Japan
e-mail: oguma@nc-toyama.ac.jp

real-time system is that the system responses faster to the deadline, more valuable for its application.

For example, in a mobile robot, recognition and avoidance of obstacles are hard real-time requirements, because these have no meaning after the collision occurs. But the user interface is a soft real-time requirement, because the user can wait for a response, even if it is delayed.

In real-time systems, it becomes a priority problem whether to take the logical correctness or a temporal accuracy. As shown in the termination or computability problems of computer systems ideally represented by a Turing machine, whether a calculation will be completed within a time determined cannot be proved theoretically. Therefore, a real-time requirement is difficult to ensure in nature, there is no choice but to achieve proximity of the outputs by putting various constraints depending on the conditions of execution contexts. It can be said that the hard real-time property is giving more priority to the accuracy in time than the correctness of the calculation.

9.1.2 Requirements of Real Time

To ensure the dependability of the systems, definition and analysis of requirements are important where what kind of dependability is required and why the system needs real time. In the functional safety standards [1], exhaustive risk assessment to analyze any risks exist in the system is set to be performed first to avoid an undesirable or unsafe condition of the system.

The systems which require real time are a simultaneous and accurate time data acquisition system or man–machine interface of remote control, a virtual reality system, and a digital control system which performs feedback control in the real world. In such systems, for examples in a data acquisition system, jitter of the sampling time appears to be a data error. In the case of a feedback control system, if error detection which is determined as a safety requirement was delayed, then error handling will be delayed and finally the risk must increase. These systems can be called as a cyber-physical system of which the system interfaces with the computer world and the physical world. And the gap between the computer based on the order of its commands and the physical world consisting of a continuous time turns out to be a dependability problem.

9.1.3 Realization of Real-Time Systems

Once the request is determined, designer of the system must consider how to realize the requirements in next. In the implementation of dependable service systems, a safe state is first required to be defined. In order to avoid risk or undesirable conditions, it is necessary to define what states are safe and the system should be

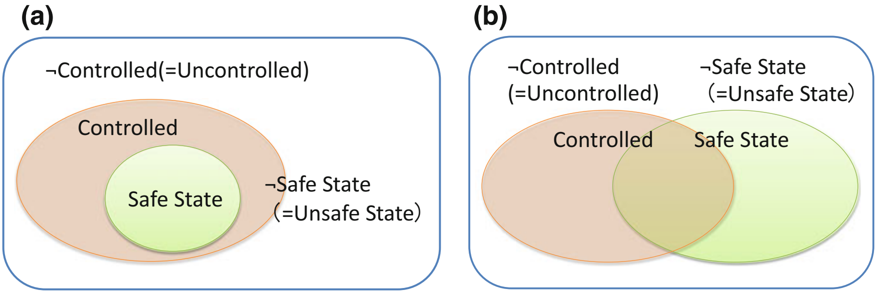


Fig. 9.1 **a** Fail operational (left figure) and **b** fail safe (right figure)

designed to remain always in that safe state. The fail-operational system is the system whose safety is not secured if it is not properly controlled (Fig. 9.1a). The fail-safe system is the system which can transit to the safe state despite the loss of control (Fig. 9.1b). Fail-operational systems are more difficult to realize than fail-safe systems.

For examples, an aircraft in flight or robots of the inverted pendulum type, such as the Segway, are the fail-operational systems because they cannot reach to their safe state when their control is lost and it is not possible to control such a system in soft real-time.

To compare the methods of implementing hard real-time and soft real-time computer systems [2], static allocation of computer resources and time-triggered communication can guarantee deterministic behavior and certain response time for the hard real-time system. On the other hand, behavior of the system with event-triggered communication and/or dynamic resource allocation inevitably become stochastic so that the communication must only be the best effort in a strict sense and it only satisfies soft real time in such systems.

9.1.4 An Application of Feedback Control System

A block diagram of a feedback control system is shown in Fig. 9.2. If a system is controlled by a computer, it must be a digital control system, in which the output is sampled at regular intervals to feedback the result of calculation to control the target system. As an example of a feedback control system, a robot handling system by visual tracking [3] is shown in Fig. 9.3.

From the sampling theorem, it is theoretically derived that twice the natural frequency (or response frequency) of the target is required as the frequency response of the digital control system. In the second row in Fig. 9.4, the original waveform can no longer be reproduced because the sampling period is longer than the oscillation period of the target so that the folding occurred. In a robot control,

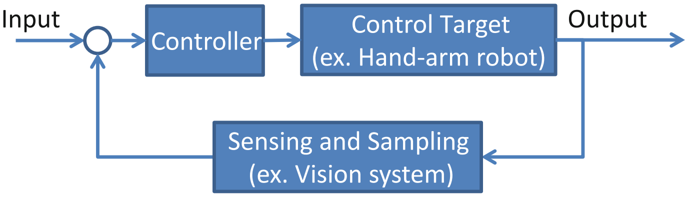


Fig. 9.2 Block diagram of a feedback control system

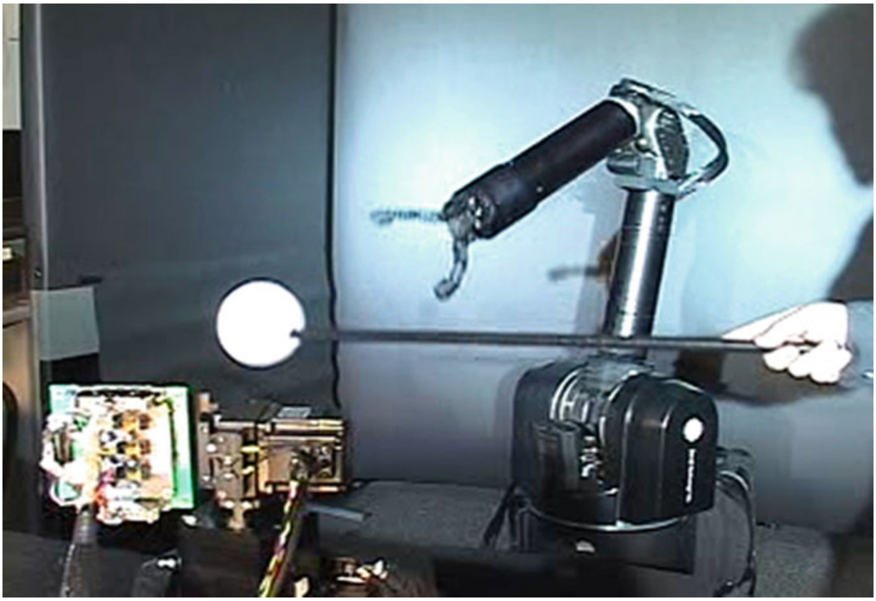


Fig. 9.3 Visual feedback control system (lower left in the photo is a tracking camera which captures a position of a white ball in front which is attached to the tip of a rod moved randomly by a person. And a black-colored hand-arm robot is controlled by a hard real-time control system aimed to grab the ball quickly)

such as shown in Fig. 9.3, a frequency of about 10 times the response frequency of the control target is required for the dependable digital control [4] as a rule of thumb.

9.1.5 Predictability of System Behavior

In the previous sections, we have introduced the dependability and real-time requirements and the realization methods of the computer systems, control systems, and application service systems. We have seen that the hard real time to realize the

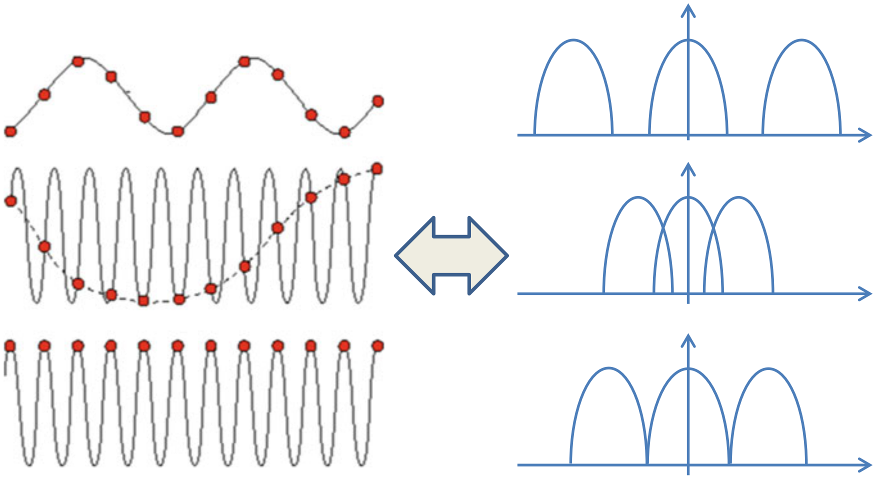


Fig. 9.4 An example of the folding in sampling theorem [wave signal and sampling points (red dots) in time domain (left figure) and its amplitude in frequency domain (right figure)]

safe state required by the system risk assessment can be realized by deterministic behavior and/or sampling time of 10 times faster response of the control target. However, today, in a large-scale system called system of systems (SoS), from the hierarchy of every different levels of view of the systems, there exist the situations that even a deterministic system needs to be captured stochastically as a whole system (Fig. 9.5). Too large-scale control software and/or widely distributed network, for example, accumulates error and uncertainty which cannot be observed, and its deterministic behavior will be lost.

As shown in Fig. 9.6, on the other hand, by applying sufficient costs for developing and testing, and also prohibiting changes of completed systems, such as aircrafts or industrial plants, even an extra large-scale system can be built deterministic. Or, as an example in embedded systems, e.g., car electrical systems, extra large numbers of sample of system behavior in a closed environment lead to dependability ensured by constructing a predictable system even by its stochastic behavior. When designing or developing the system, it is important to choose available and appropriate approach to achieve necessary (or unnecessity of) required dependability levels.

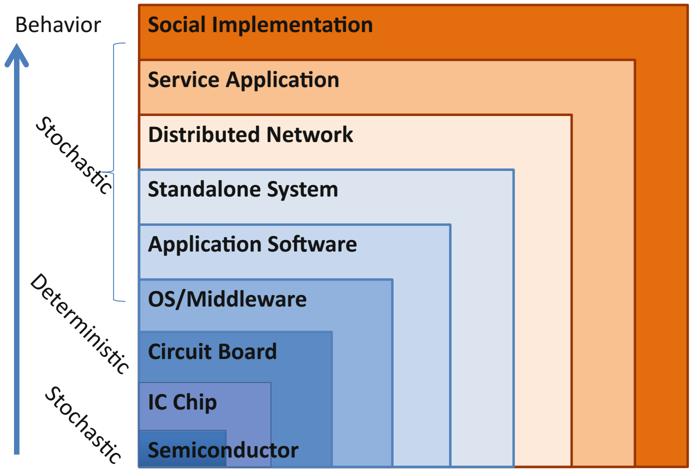


Fig. 9.5 Stochastic behaviors and the hierarchy of the system

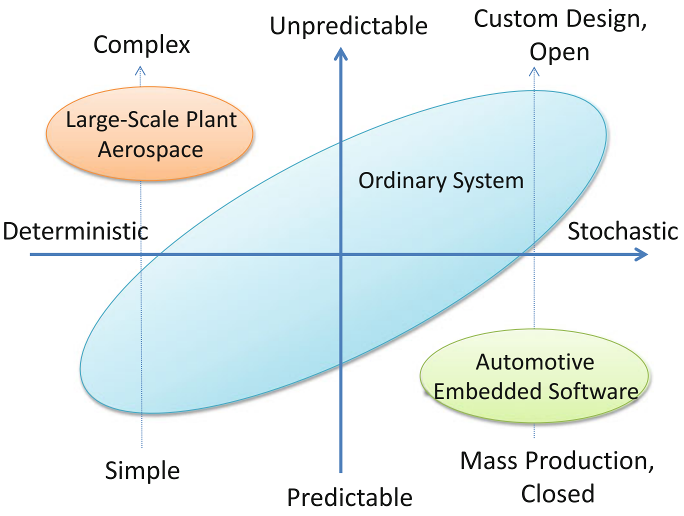


Fig. 9.6 Predictability and various behaviors of the system

9.1.6 Summary

We have discussed hard real time and soft real time of dependable systems from the viewpoint of requirements and realization, deterministic, or stochastic behaviors of the system. The outlook for future implementations of the system is also described.

9.2 Microprocessor Architecture for Real-Time Processing

Nobuyuki Yamasaki, Keio University
Masayoshi Takasu, Keio University

9.2.1 Dependable Responsive Multithreaded Processor

A distributed real-time system including a humanoid robot integrates a set of hardware and software components designed with the time constraints for specific control functions. All computation and communication in the system require priority-based control to satisfy their time constraints because most real-time task scheduling algorithms require priority-based preemption [5]. Dependability is also required because they are used as a part of social infrastructure and expected to run continuously without errors. Dependable Responsive Multithreaded Processor (D-RMTP) [6] introduces responsive multithreaded processing unit (RMT PU) and *Responsive Link* [7] for this purpose. The RMT PU provides prioritized SMT (simultaneous multithreading) execution, IPC (instructions per clock cycle) control, context caches, and 2D vector processing units, for real-time processing.

A complicated robot has required high time resolution and robustness. However, traditional complicated robots become complex due to the hardware and software complexities, and hence these robots have low time resolution and un-robustness. We try to design and implement hardware and software platforms with high time resolution and robustness by hardware–software codesign for such robots as shown in Fig. 9.7.

Figure 9.8 shows the requirements and solutions for a humanoid robot. A leg module [8], which is a part of a humanoid robot, requires severe time constraint, high throughput, high current/voltage, noise tolerant, and heat dissipation. However, it is difficult for existing processors to satisfy these requirements at a time. In order to satisfy the requirements, we research and develop a new processor, called Dependable Responsive Multithreaded Processor (D-RMTP) [6].

We illustrate the design and implementation of the D-RMTP for distributed real-time systems. Generally, these systems require real-time execution and real-time communication, in which tasks have the time constraints. The goal is to replace non-real-time microprocessors and networks with the D-RMTPs that have the RMT PU and *Responsive Link* [7], ISO/IEC 24740:2008 communication standard, to improve dependability. Small controllers with the D-RMTPs are embedded at every joint of the robot and are interconnected via *Responsive Link* for distributed control. Therefore, the D-RMTP is designed to meet severe requirements in terms of footprint, latency, scalability, real-time capability, and dependability.

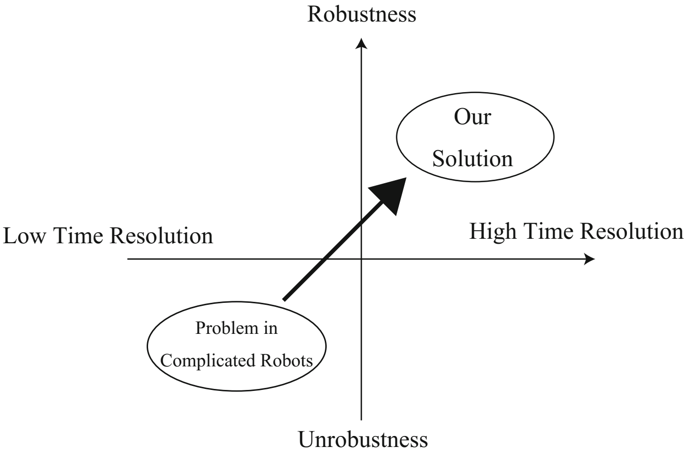


Fig. 9.7 Our solution in complicatable robots

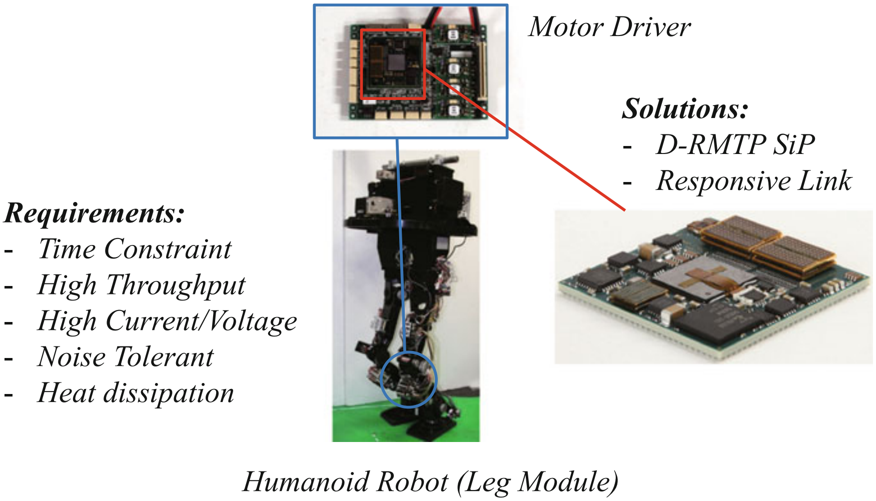


Fig. 9.8 Requirements and solutions to a typical robotic application

The detail of how to apply the D-RMTP to robotic applications and implement real-time operating systems on the D-RMTP is described in Chap. 24. Also, the detail of *Responsive Link* is described in Chap. 4, Sect. 4.

We propose a multifaceted approach that introduces priority-based control with dependability for both the computation and communication so that the D-RMTP can meet the various requirements. The D-RMTP SoC (system-on-chip) integrates RMT processing unit (RMT PU) for real-time processing, *Responsive Link* for real-time communication, and various I/O peripherals (see Fig. 9.9).

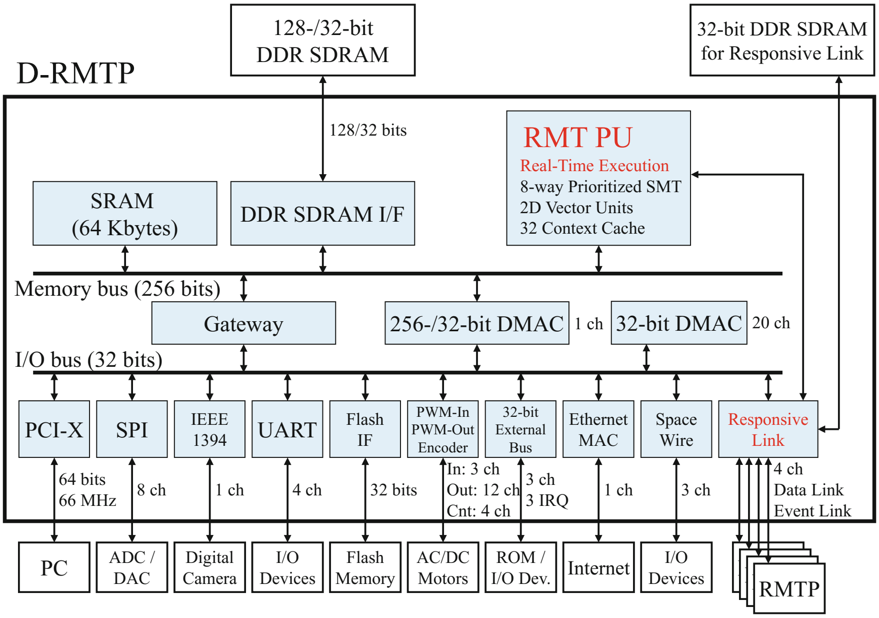


Fig. 9.9 Block diagram of D-RMTP SoC

In various I/O peripherals of the D-RMTP, PCI-X is an I/O interface to PC, SPI is mainly used to connect with A/D and D/A converters for sensing and control, IEEE 1394 is mainly used to capture digital camera information, UART is used for control and console, Flash I/F is used to connect with a nonvolatile flash memory, PWM-in and PWM-out encoders are used to control AC/DC motors, 32-bit external bus is connected with ROM and other I/O devices, Ethernet MAC is used to connect with Internet, SpaceWire is used to communicate with I/Os in spacecraft, and *Responsive Link* is used to communicate with other D-RMTPs in real time.

The D-RMTP integrates 32-Kbytes level-1 instruction and data caches and a 64-Kbyte SRAM for on-chip memory. The D-RMTP SiP integrates 128-Mbyte DRAM as main memory. In general, the access latency of SRAM is shorter than that of DRAM. Therefore, small size operating systems such as favour OS that is our original real-time OS and μITRON OS [9] are executed in SRAM, and large size operating systems such as Linux are executed in DRAM due to size constraint.

Here, we introduce some unique architectures used in the D-RMTP SoC. Real-time execution is a key requirement for real-time systems, and the multi-faceted approach combines the following four hardware mechanisms: prioritized SMT execution, context cache, instructions per cycle (IPC) control, and 2D vector processing units.

9.2.2 Prioritized SMT Execution

Generally, real-time systems are controlled by real-time scheduling algorithms including earliest deadline first [10] and rate monotonic [10]. In these algorithms, priorities are assigned to tasks according to their time constraints and they are executed in priority order. The RMT PU has eight prioritized hardware threads and can execute eight tasks in priority order without context switching [11]. These priorities are held as a part of context information and expressed in eight bits (i.e., the supported priority level is 256 levels). An eight-bit priority is sufficient for most complex rate-monotonically scheduled systems [12]. Figure 9.10 illustrates a block diagram of the RMT PU, in which priority control is applied to the functional units surrounded by dashed boxes.

The system applies priority control to all levels in the RMT PU and assigns hardware resources to a hardware thread with higher priority. This mechanism enables hardware to execute real-time threads, which are conventionally scheduled and executed by a real-time operating system, so far and results in load reduction of the operating system.

Figure 9.11 illustrates the sample scheduling of eight prioritized hardware threads. The eight prioritized tasks are executed simultaneously among all ready tasks in priority order.

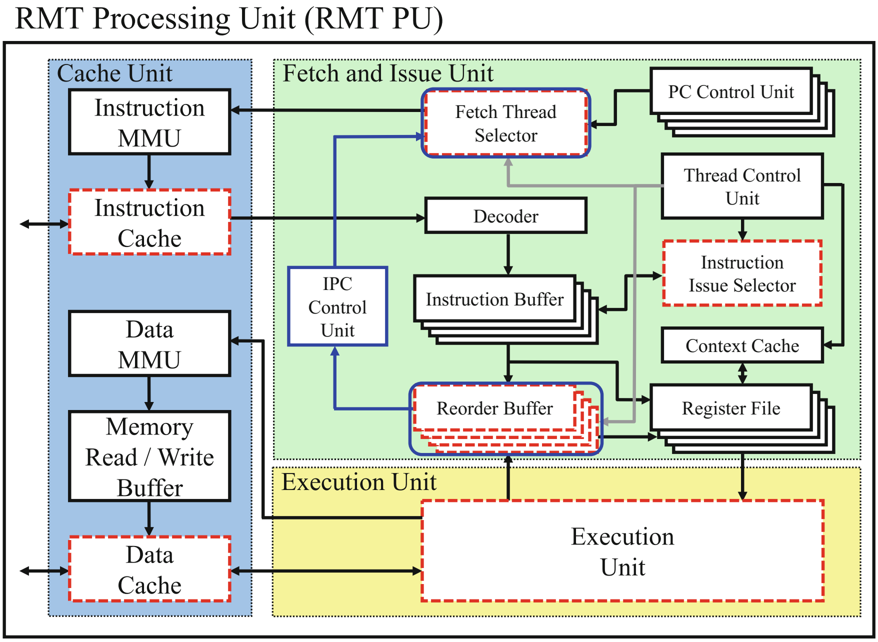


Fig. 9.10 Block diagram of RMT PU

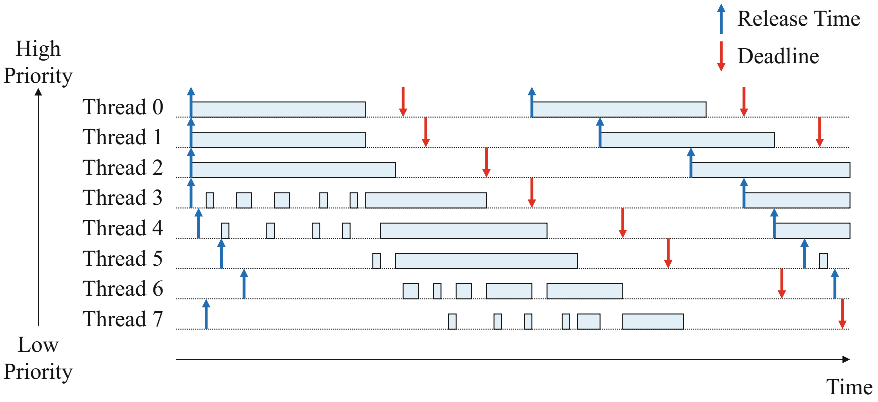


Fig. 9.11 Example of scheduling eight prioritized hardware threads

9.2.3 Context Cache

In the D-RMTP, a context switch occurs to switch tasks when there are more than eight threads. Generally, a software-based context switch causes a lot of overhead to save and restore the contexts including register files and program counters into memory. A real-time scheduling algorithm determines tasks to be executed according to priority assigned to them, which may invoke many context switches, and their overhead decreases schedulability.

To reduce the context switch overhead when there are more than eight threads, the D-RMTP introduces a hardware-based context switch mechanism, called context cache that is an SRAM-based cache memory that can save 32 hardware thread contexts including GP registers, FP registers, status registers, and program counters. If there are less than or equal to 40 threads on the D-RMTP, every context switch is completed within four clock cycles by using the context cache.

9.2.4 IPC Control

Although most real-time scheduling algorithms rely on task's worst-case execution time (WCET), WCET analyses are increasingly pessimistic due to the complexity of recent systems, and such pessimistic WCET analyses decrease schedulability. The IPC control mechanism introduces a new approach that does not rely on WCET analyses but directly controls each thread's speed (IPC). The IPC control mechanism limits the number of instructions per a given control period. The control period is specified as the number of clock cycles, and the number of instructions to be executed within the control period is also set by a software scheduler. A fetch unit in the RMT PU controls instruction fetches to execute the preset number of instructions within the control period. The RMT PU terminates the instruction fetch until next control period when the number of fetched instructions reaches the target one, and then instructions of the thread with the next highest priority will be fetched.

Although the original IPC control relies on the heuristic algorithm [13], the D-RMTP equips the improved version of the IPC control based on the proportional–integral–derivative (PID) control theory because it is well established and various parameter tuning methods are available for each of use. The IPC control mechanism with PID control is performed on the basis of the following formula:

$$output = K_{\mathrm{P}}e(t) + K_{\mathrm{I}}\int_{0}^{t} e(\tau)d\tau + K_{\mathrm{D}}\frac{d}{dt}e(t)$$
$$e(t) = target - input$$

where K_{P} is a proportional gain, K_{I} is an integral gain, K_{D} is a derivative gain, *target* is a target IPC, *input* is the number of committed instructions, and *output* is the upper limit of the instruction fetch. On start-up, the gain coefficients are given default value ($K_{\mathrm{P}} = 1/2, K_{\mathrm{I}} = 1/8, K_{\mathrm{D}} = 1/4$) by hardware. Default parameters are optimized for commonly used applications of humanoid robots. After start-up, the gain coefficients can be reconfigured by software. A user can determine the gain factors by using existing methods, for example, the Ziegler–Nichols method [14].

Predictability of task's execution time greatly varies by the presence or absence of IPC control. Figure 9.12 illustrates IPC of multithreaded execution without IPC control. Benchmarks including md5, gzip, sort, and matrix are assigned to each hardware thread and the priority order is md5 < gzip < sort < matrix. IPC of each thread widely fluctuates without IPC control, which causes a considerable reduction of predictability of task's execution time. Figure 9.13 illustrates IPC of multithread

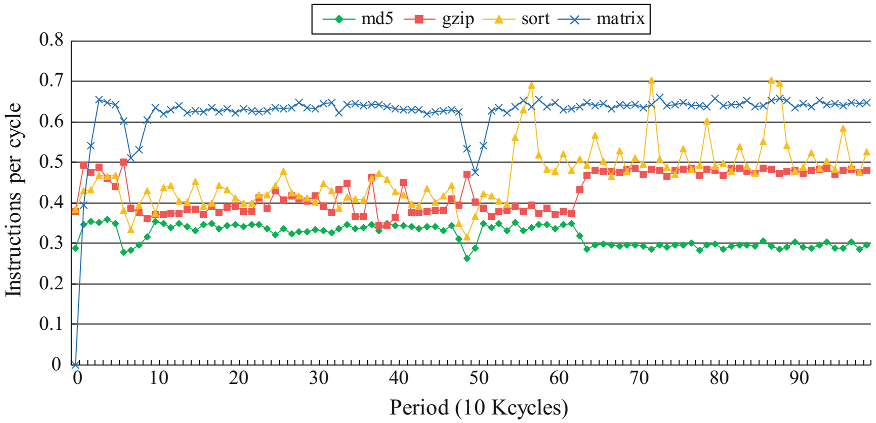


Fig. 9.12 IPC of multithread execution without IPC control

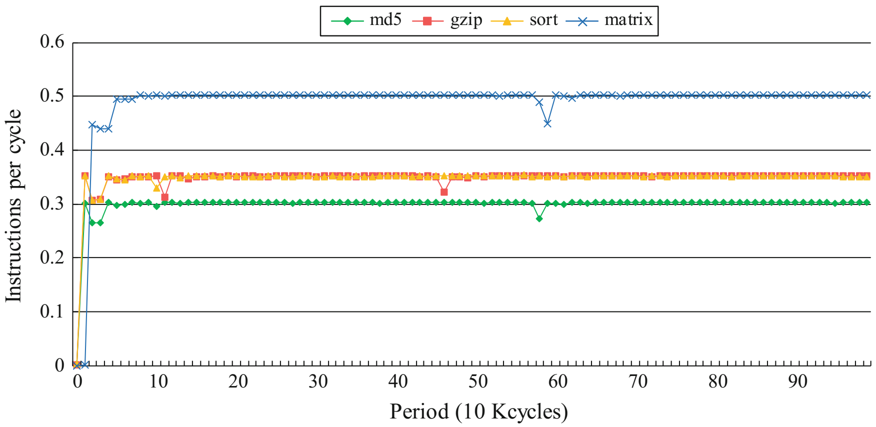


Fig. 9.13 IPC of multithread execution with IPC control

execution with IPC control. IPC of each thread is steady and predictability of task's execution time is improved. In some parts of Fig. 9.13, IPC is below target IPC within a certain control period but is over within the next control period. When a fetch unit cannot achieve target IPC within a control period, it tries to make up for insufficient IPC within the next control period, and hence average IPC is nearly equal to target IPC.

No context switch is required to execute up to eight threads in the RMT PU, and the IPC control enables a cycle-level precise execution speed control of each task. Since a motor control task is completed within a few hundred cycles, this mechanism achieves a fine-grained motor control of less than 10 μs.

9.2.5 Vector Processing Unit

Current real-time applications require high computing performance for multimedia processing including image processing, voice processing, etc. Therefore, flexible and powerful 2D vector operation units for multimedia processing are designed [15]. Since multiple threads are executed in parallel in the RMT PU, some of them may want to perform vector operations at the same time. Thus, shared vector registers by multiple threads are designed. Figure 9.14 shows a block diagram of a vector processing unit.

An integer vector processing unit consists of two integer vector execution units. An integer vector execution unit consists of eight 32-bit integer SIMD units. A 32-bit integer SIMD unit can execute a 32-bit integer operation, two 16-bit integer operations, or four 8-bit integer operations. Therefore, the integer vector processing unit can execute 64 8-bit integer operations per clock cycle. Two integer vector execution units share 32-bit 512-entry integer vector registers.

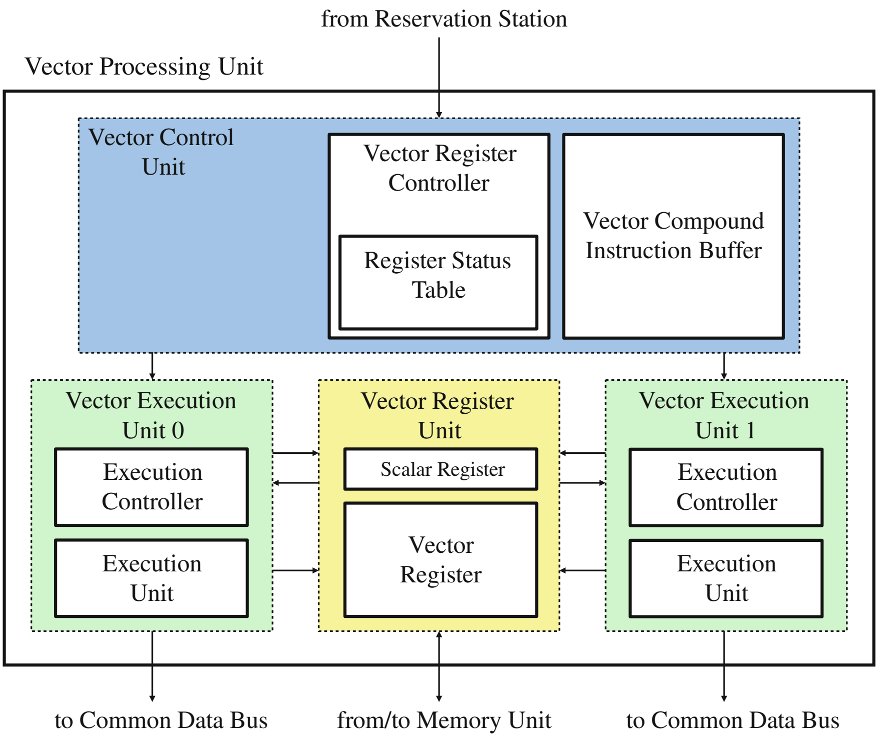


Fig. 9.14 Block diagram of vector processing unit

Similarly, an FP vector processing unit consists of two FP vector execution units. An FP vector execution unit consists of four 64-bit FP SIMD units. A 64-bit FP SIMD unit can execute a 64-bit IEEE754 FP operation or two 32-bit IEEE754 FP operations. Therefore, the FP vector processing unit can execute 16 32-bit IEEE754 operations per clock cycle. Two FP vector execution units share 64-bit 512-entry FP vector registers.

Each vector execution unit can be independently used by different threads simultaneously. A thread can use all vector processing units at the same time.

Many soft real-time applications repeat the same operations including the multiply–add operation. In addition, the issue rate of the lower priority threads that executes soft real-time applications including a multimedia application may become lower. A compound operation mechanism is designed so that a programmer can define a series of vector operations performed repeatedly. A compound operation, which consists of the series of vector operation and becomes a long latency instruction, can execute multiple vector operations at a time. Therefore, the number of instructions of the program can be reduced to execute the vector instructions and to control vector units. The utilization of vector units can also increase.

9.2.6 Summary

This section summarizes the features of the D-RMTP including RMT execution, context cache, IPC control, and 2D vector processing units. Thanks to these features, the requirements including severe time constraint and high throughput can be satisfied to build a humanoid robot.

9.3 Asynchronous Networks-on-Chip

Tomohiro Yoneda, National Institute of Informatics
Masashi Imai, Hirosaki University

In a system level, one basic approach to designing a dependable hardware platform is to use redundancy. A *network-on-chip* (NoC) architecture makes it easy, because many identical components such as processors can be connected easily and efficiently in an NoC. On the other hand, in a circuit level, due to various variations such as process, voltage, and temperature (PVT) variations in advanced process technologies, it becomes difficult to design efficient synchronous circuits. One solution to this problem is to design circuits based on local handshaking instead of relying on global clocks. This type of circuits is called *asynchronous circuits*. This chapter introduces a combination of the NoC and asynchronous circuit approaches, which has great potential for a dependable hardware platform in advanced process technologies.

9.3.1 Asynchronous Circuits

Synchronous circuits use global clocks for synchronizing the store timing of each register component. On the other hand, no global clocks are used in asynchronous circuits, because the register store operations are synchronized by local handshaking between those registers. Figure 9.15 shows an asynchronous circuit that performs an operation to the data stored in registers *REG*1 and *REG*2, and stores the result into register *REG*3. The request signal from the previous stage indicates that new data are available at the inputs of *REG*1 and *REG*2. On the other hand, the acknowledgment signal from the next stage indicates that the current data kept in the registers are no longer needed. Thus, when a handshake controller receives both of these signals, it gives a trigger signal to *REG*1 and *REG*2 in order to store new data into those registers. Simultaneously, an acknowledgment signal is sent to the previous stage in order to indicate that the current data have already been stored at this stage, and so they can be updated in the previous stage. Finally, a request signal is sent to the next stage through a delay element as shown in the figure. The delay

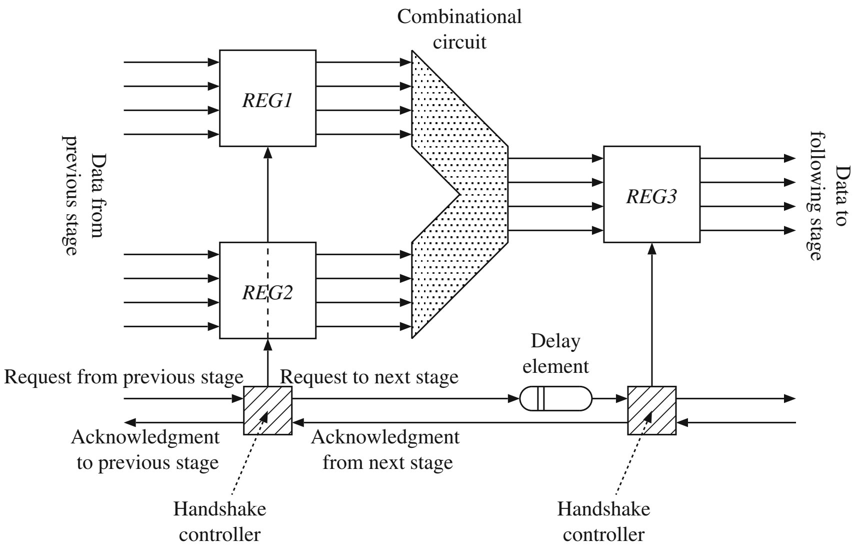


Fig. 9.15 An asynchronous circuit

value of this delay element is matched to that of the combinational circuit between the registers. Thus, the handshake controller in the next stage can use it as a request signal for that stage, which allows *REG*3 to store the stable (and so correct) result from the combinational circuit.

9.3.2 Packet Switching in Networks-on-Chip (NoCs)

Figure 9.16 shows a two-dimensional (2D) mesh NoC structure, where *Core*, *R*, and *NI* represent a computational core, a router, and a network interface, respectively.

In NoCs, a message to be sent is divided into a set of packets in a source computational core, and those packets are sent to the router that is connected to the computational core through the network interface, as well as the destination information. Each packet is further divided into a set of flits in a network interface, where a flit is a unit handled at the same time in routers and network links, and the flits are propagated in a network as shown in Fig. 9.17. As mentioned below, a *head flit* and a *tail flit* are used, besides carrying data, to occupy a route in the network and to release the occupied route, respectively. A *data flit* just carries data.

Each router executes a routing algorithm, when it receives a head flit and decides the output link which the head flit is sent to. This route is occupied for this particular packet. Thus, when the following data or tail flits arrive, they are sent to the same output link without executing the routing algorithm. This route is released when the tail flit goes through this router. It can happen that several different

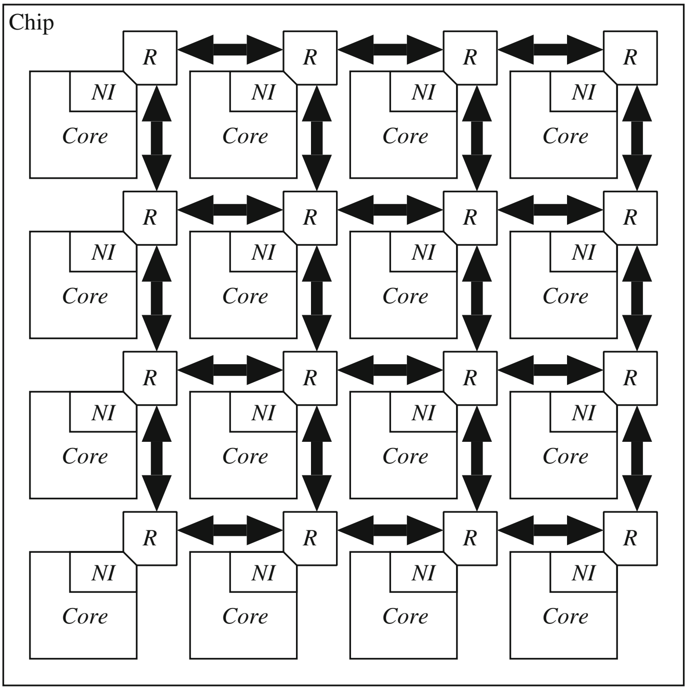


Fig. 9.16 A 2D mesh NoC structure

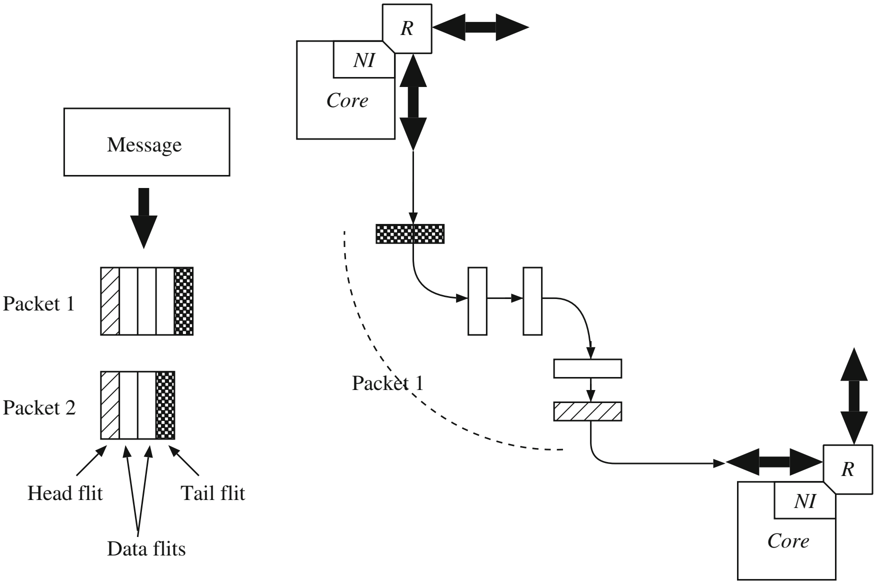


Fig. 9.17 Packet communication method

packets want to go through the same network link. When a head flit of a packet arrives, and the output link that the head flit wants to go through is already occupied by another packet, this head flit should wait until the route is released. Even if an output link is not yet occupied, it is possible that several head flits are simultaneously trying to occupy the same output link. Thus, each output link (or port) in a router has an arbiter that chooses one request among many requests. This style of packet routing method is called *wormhole switching*. When the whole flits arrive at the destination network interface, they are reconstructed into a packet, and the whole packets are reconstructed into a message, which is sent to the computational core.

9.3.3 Advantages of Asynchronous NoCs

NoCs can be implemented based on either synchronous or asynchronous design style. The advantages of asynchronous NoCs are as follows.

(1) In synchronous circuits, global clocks should be distributed into the entire chip. Especially for high-speed clocks, this causes a situation where some register elements have different clock timings due to the clock propagation delays, which is called *a clock skew problem*. Furthermore, such global clocks should be continuously supplied to every router, even if some routers are not handling packets for some amount of time. This unnecessarily increases the power dissipation. On the other hand, in asynchronous circuit implementation, no global clocks are used, and the exact portion of the circuits that actually handle the packets consumes the power, thanks to the local handshaking scheme. Thus, the asynchronous NoCs are free from the above problems.

(2) The elements in a chip have performance and delay variation due to various reasons. Furthermore, environmental changes in, for example, supply voltages and temperature as well as performance degradation due to aging cause delay variation. In synchronous implementations, the clock frequencies should be decided considering the worst case in these variations. Asynchronous implementation is robust to uniform variation and/or degradation, because the local handshaking and the data path circuits are similarly affected by the uniform changes. In cases that random variation or degradation should be considered, or the estimation of data path delays is not easy due to, for example, long transmission wires with large delays, data path encoding schemes can be used. One of such a scheme used for a link is shown in Fig. 9.18. This is called *LEDR (Level-encoded dual-rail)* scheme [16], where one-bit information is represented by using two wires, and two different encodings are used in odd and even cycles (see Sect. 9.3.4.3 for details). Thanks to this encoding scheme, the receiver side can detect the exact timing when the codewords arrive and can

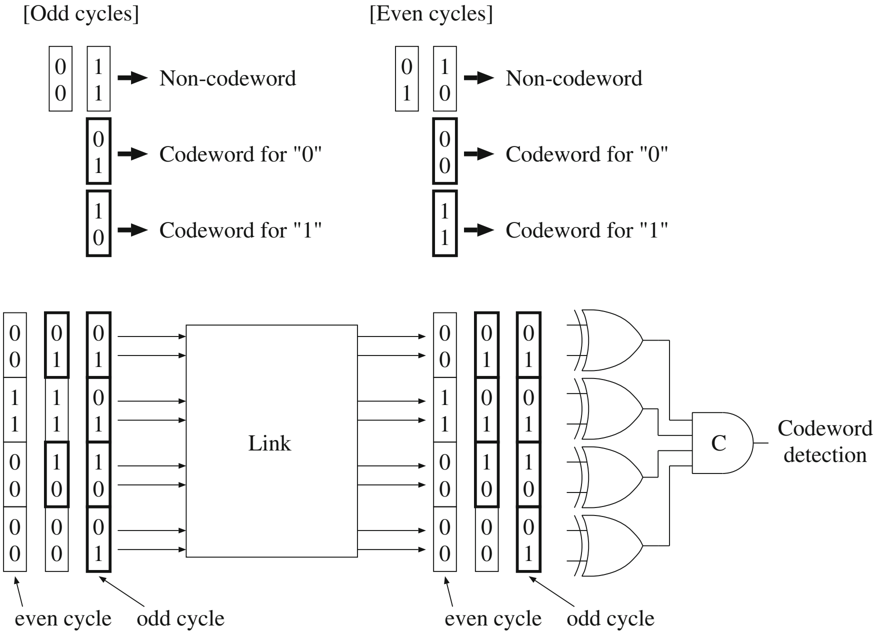


Fig. 9.18 An encoded link

generate the request signal based on the detection. Thus, in spite of any large delay or delay variation, the data transmission is performed correctly.

(3) In a simple wormhole switching, a routing computation is performed, when a head flit arrives at a router, in order to decide which output link the flit is sent to. For complicated routing algorithms such as a dependable routing algorithm (e.g., Chap. 19, Sect. 3), the computational cost for this routing computation is not small. On the other hand, when the succeeding data and tail flits arrive, they are immediately passed to the output link already decided by their head flit. Thus, the cost of handling them is much smaller than that for the head flit. In a simple implementation of a synchronous circuit, the clock cycle is determined based on the most time-consuming steps. Hence, it can happen that the cycle decided for the routing computation is too long for data and tail flits. The upper part of Fig. 9.19 shows an example of computational costs of a synchronous router needed for each cycle and flit. The x-axis is a timescale. In this example, it is assumed that the synchronous router has four pipeline stages, and the second pipeline stage for the routing computation decides the clock cycle. The router is idle for some time on the other stage. Furthermore, when handling data and tail flits, more idle time is spent, because the clock cycle is fixed by the routing computation stage. An asynchronous router, however, does not have such a constraint. That is, the time needed for each pipeline stage depends on the actual computational cost, and thus, the (dummy) routing computation stage

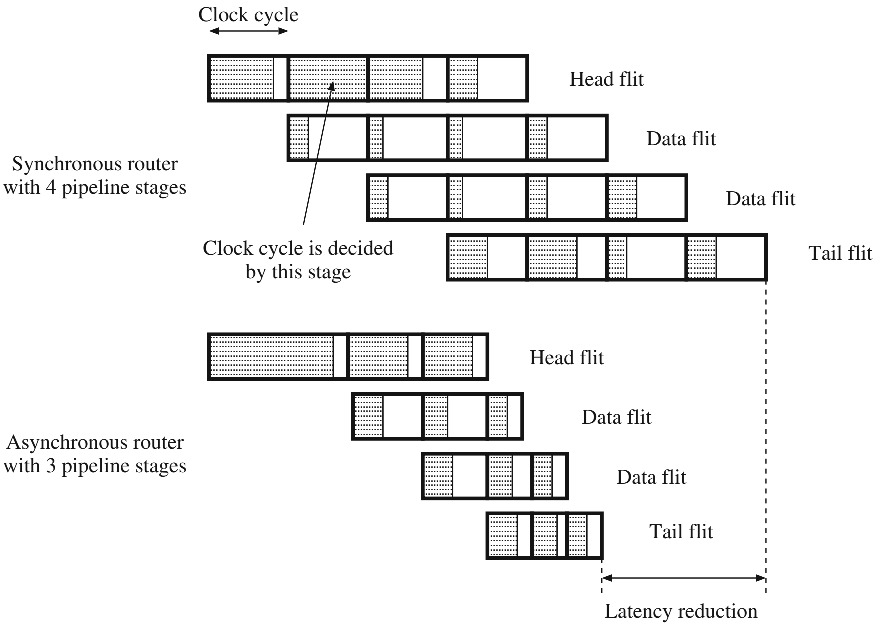

Clock cycle
Head flit
Data flit
Data flit
Tail flit
Synchronous router with 4 pipeline stages
Clock cycle is decided by this stage
Head flit
Data flit
Data flit
Tail flit
Asynchronous router with 3 pipeline stages
Latency reduction

Fig. 9.19 Packet handling in synchronous and asynchronous routers

for data and tail flits can end quickly. The lower part of Fig. 9.19 shows this situation, where an asynchronous router with 3 stage pipeline is assumed. Note that this number of pipeline stages (i.e., 3) is just one example, but the pipeline stages of asynchronous routers may tend to be shorter than those of synchronous ones, because so much fine grain pipelines are not usually needed in asynchronous routers. As shown in the figure, handling the head flit may take longer time, but the other flits can be handled very quickly. Although some time overhead for handshaking is needed, the total time for handling a head flit, data flits, and a tail flit can be reduced in the asynchronous router. Note that this also reduces the packet blocking times by releasing the occupied routes quickly.

9.3.4 Implementation of Asynchronous Routers

In this section, several techniques for implementing asynchronous routers are introduced mainly from [17]. These ideas are used to build actual chips for various applications (e.g., [18–21]).

9.3.4.1 Asynchronous Pipelines

Although several implementations for asynchronous pipelines are proposed, this section introduces an implementation called *MOUSETRAP* [22], which is simple but has high performance.

Figure 9.20 shows the *MOUSETRAP* pipeline stages. Let us focus on *Stage N*. A transparent latch propagates the input values to its output, when G_N input is 1, and holds its values, when G_N input is 0. Let *transparent mode* denote the former situation, and *hold mode* denote the latter. The bold arrows in the figure represent the data paths. In addition to them, control signals (e.g., req_N) are also put into inputs of transparent latches, which are output as $done_N$ and so on. The structural feature of the *MOUSETRAP* pipeline is that it is very simple, i.e., its control circuit consists of only one EXNOR (Exclusive NOR) gate and one bit of transparent latch.

This *MOUSETRAP* pipeline behaves as follows. In the initial state, req_N, $done_N$, and ack_N are 0, and so $G_N = 1$. Thus, the transparent latch of *Stage N* is in the transparent mode. Eventually, req_N changes from 0 to 1 to indicate that the data from the combinational circuit are stable. Since the latch is in the transparent mode, this change is propagated to $done_N$, which changes G_N from 1 to 0. This causes the latch to go into the hold mode, and $data_N$ (as well as the data from the combinational circuit in the previous stage) is stored and kept in this latch. At the same time, $done_N$ is propagated to the previous stage as ack_{N-1}, which allows the previous stage to destroy the current data and update its data. These two actions, i.e., the transparent latch moves to the hold mode and $data_N$ is destroyed, are caused by the change of $done_N$, but for the correct behavior of *MOUSETRAP* pipeline, the former should happen earlier than the latter. This is one timing constraint for the circuit delays of the *MOUSETRAP* pipelines to be satisfied.

Furthermore, $done_N$ as well as the data stored in the transparent latch is propagated to the next stage through the delay element and the combinational circuit. The next stage similarly stores and holds the data and sends back its *done* as ack_N to *Stage N*. This causes ack_N to change from 0 to 1, and G_N becomes 1. Since this latch is now in the transparent mode, its output can be updated for the next data.

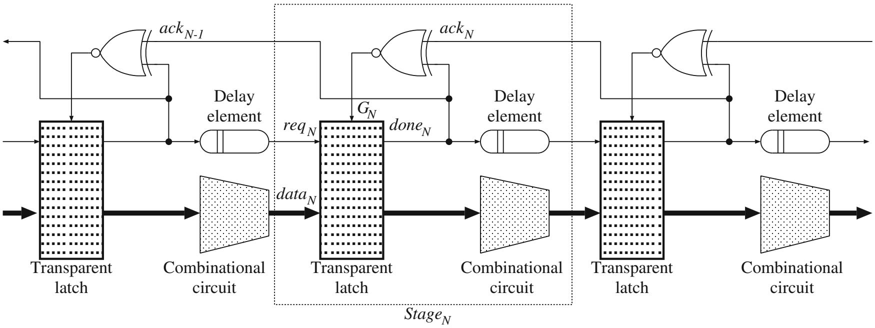


Fig. 9.20 *MOUSETRAP* pipeline

Note that req_N has been 1 for the previous data, and now it changes from 1 to 0 to indicate that the next data is available at $data_N$. Since ack_N is already 1, this change causes G_N to be 0, and the latch holds this new data. In this way, the control signals such as *req* and *ack* indicate their information by the transition of the values (i.e., the changes from 0 to 1 and from 1 to 0). This handshake protocol is called *two-phase signaling*.

In the above scenario, the transparent latch is already in the transparent mode, when the new req_N change happens. If the new req_N arrives in a situation that the data in *Stage N* are still used by the next stage and so should be kept, the req_N change is simply blocked by the transparent latch that is in the hold mode. In this case, when ack_N arrives and the latch becomes transparent, req_N is accepted, and the latch immediately goes into the hold mode again.

The *MOUSETRAP* pipelines are used in many portions of asynchronous routers, such as the queues of the input channels and the pipeline stages in the routing computation.

9.3.4.2 Asynchronous Arbiters

When several units want to use the same resource simultaneously, their requests should be arbitrated. An arbiter is used for this purpose, i.e., it chooses one request among the several requests, and gives a grant for using the resource to the corresponding unit. As for a synchronous arbiter, the requests are given in synchronization with a clock signal, which means that the request signals are stable when the decision is made. Thus, a priority-based approach or a token-based approach can be easily implemented. On the other hand, for an asynchronous arbiter, the request signal can change at arbitrary timing, and the earliest one should be chosen. It is in general not easy due to a phenomenon called metastability (see below) to handle such request signals that can happen at the same time.

Figure 9.21a shows a core circuit block for an asynchronous arbiter. Assume $(R1, R2) = (0, 0)$ initially. Then, $(V1, V2)$ is $(1, 1)$. Now, if $R1$ goes to 1, then $V1$ becomes 0, and even if $R2$ goes to 1, $V1$ remains 0. $V1$ can go to 1 only when $R1$ goes back to 0. After that, $V2$ reacts to the change of $R2$. Therefore, this circuit can be considered to be a two-input asynchronous arbiter, where $V1$ and $V2$ are the inverted signals for grants. This circuit, however, has a big problem. When $R1$ and $R2$ go to 1 at almost the same time, $V1$ and $V2$ also try to go to 0, and these changes are propagated to the input sides of the gates. As a result, those outputs take unstable voltages between 0 and 1. This is called *metastability*, and theoretically it is unknown when this situation ends. If these unstable voltages are sent back as grant signals, the circuits that receive these signals may behave incorrectly. Thus, this should be avoided.

Fortunately, since this phenomenon actually lasts for a very short time, an approach that the arbiter outputs are kept 0 during the metastability lasts is a practical solution. Figure 9.21b uses a metastability detection circuit to implement this idea [23] and is called *ME* (*Mutual exclusion*) element. The two NMOS

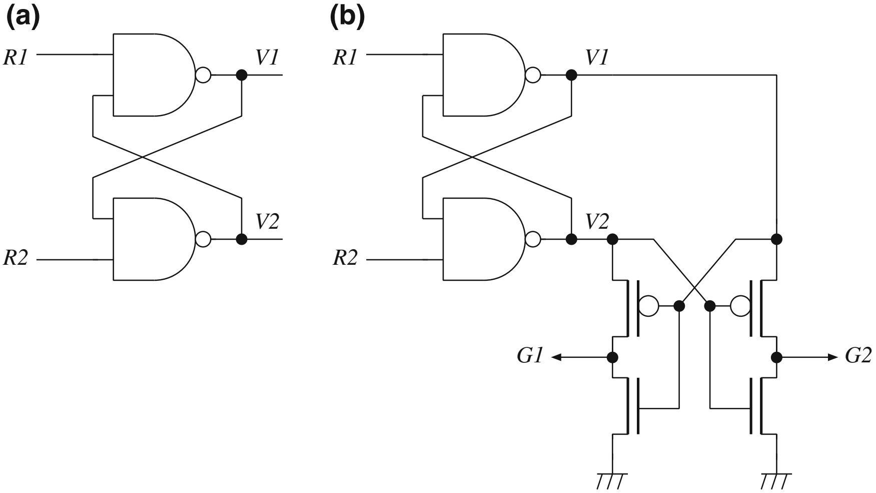


Fig. 9.21 Two input asynchronous arbiters

transistors detect the intermediate voltages at $V1$ and $V2$, and keeps $G1$ and $G2$ almost 0 voltage level until $V1$ and $V2$ go to either logical value 0 or 1. Thanks to this metastability detection, even if $R1$ and $R2$ go to 1 at the same time, only either $G1$ or $G2$ goes to 1 after the metastability has gone. This is a two-input asynchronous arbiter.

Asynchronous arbiters with more inputs can be constructed by connecting several ME elements. Several implementations are proposed. See [24–26] for more details.

9.3.4.3 Encoded Links

The encoded link shown in Fig. 9.18 is actually implemented with an encoding circuit, a code detector, and a control circuit, as shown in Fig. 9.22.

The encoding circuit applies two different encoding schemes depending on the number of transmission (or cycles), as shown in Fig. 9.18. In the first transmission, third transmission, fifth transmission, and so on, which are denoted by *odd cycles*, the codeword for the value 0 is (01), and that for the value 1 is (10). In *even cycles* (i.e., second transmission, fourth transmission, and so on), the codewords for the value 0 and 1 are (00) and (11), respectively. Here, remember that *req S* shown in Fig. 9.22, which is a request signal indicating that the input data is available, changes from 0 to 1 in odd cycles, and from 1 to 0 in even cycles. Thus, the encoding circuit uses EXOR gates and obtains (d, $d \oplus$ *req S*) for an input bit d, in order to perform these two encodings. That is, in the odd cycles, the values 0 and 1 are encoded to (0, 1) and (1, 0), because *req S* becomes 1. In the even cycles when *req S* changes to 0, they are encoded to (0, 0) and (1, 1). The encoded signals are

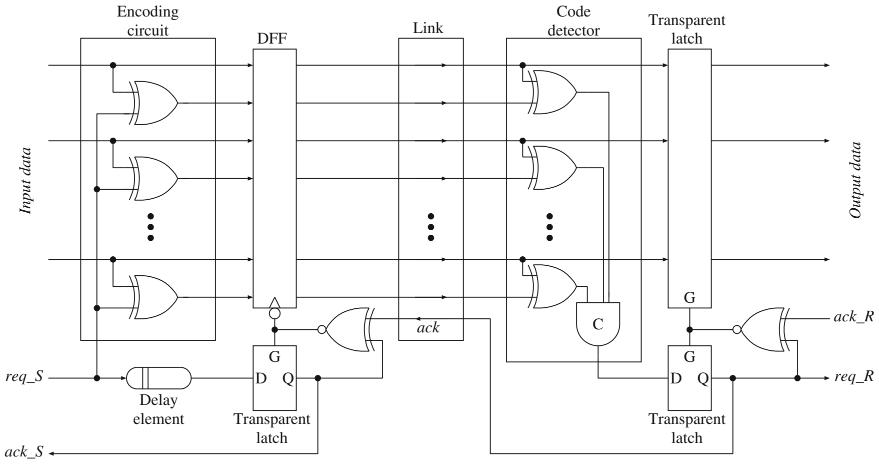


Fig. 9.22 Implementation of an encoded link

stored into the D-flipflop (DFF) at the falling edge of the control signal, where the control signal is generated in a similar way as the *MOUSETRAP* pipeline. Note that a DFF instead of a transparent latch is used for this data path. This is to prevent unstable data that are being encoded from propagating to the link. If a transparent latch is used here, it is in the transparent mode when *ack* is given, and thus, the output of the encoding circuit is directly propagated to the receiver side. Consider a case that all bits of the input data change from 0 to 1 temporally in an even cycle before *req* signal changes. Due to the delays of the EXOR gates, the encoding circuit produces (1, 0) for each bit for a very short time, and then produces (1, 1). These changes appear in the link, and they may be recognized as a complete codeword in an odd cycle in the receiver side, which is incorrect. Thus, the output of the encoding circuit should be propagated to the link, only when the encoding operation that follows the *req* signal change completes. The implementation shown in Fig. 9.22 uses a delay element, whose delay value is matched to the delay of the encoding circuit, to guarantee that the output of the encoding circuit is stored into DFF certainly after its encoder output becomes stable.

The code detector applies an EXOR gate for each signal pair that conveys codewords. When every signal pair has a codeword, their output is (11…1) in odd cycles and (00…0) in even cycles. They are sent to an n-input C-element (a gate with “C” in Fig. 9.22), where n is the number of the signal pairs. A C-element produces 1 when all of its inputs are 1, and produces 0 when all of its inputs are 0. Otherwise, the C-element keeps the current output. Thus, it is a kind of a memory element. Hence, exactly when every signal pair of the link shows a codeword, the code detector produces 1 in odd cycles and produces 0 in even cycles. Since this output can be used as a request signal for the two-phase signaling, it is connected to a *MOUSETRAP* pipeline stage as shown in Fig. 9.22 (Compare the rightmost part of Fig. 9.22 and a *MOUSETRAP* pipeline stage shown in Fig. 9.20).

The acknowledgment signal from this *MOUSETRAP* pipeline stage is sent to the sender side through the link. Note that decoding codewords are very simple as shown in the figure. This is because the encoding scheme is done by (d, $d \oplus req\ S$), and so, the data itself is propagated in one of the signal pairs.

9.3.5 Some Quantitative Comparisons

This section shows some quantitative comparisons of a synchronous router and an asynchronous router, in order that readers can feel some difference in the nature of those designs. For this purpose, the following two simple NoCs have been designed.

- Topology: 2 × 2 mesh.
- Flit size: 32 (data) + 2 (flit attribute) bits.
- Routing algorithm: dependable and adaptive algorithm (see Chap. 19, Sect. 3 for details).
- Pipeline stages: 5 (synchronous version) and 4 (asynchronous version).
- Process technology: 130 nm bulk CMOS.
- Router distance on a chip: 2 mm.

Through the Verilog simulation of the placed and routed designs, the areas, performance, and power consumption of those two designs are compared. Note that this is one experimental trial without any intensive optimization in both designs. Thus, one cannot conclude from only these results any general tendencies between synchronous and asynchronous design styles.

The whole asynchronous NoC (containing four routers) includes 14,694 logic elements, while the synchronous one includes 29,225 logic elements. The area of a single router on a chip occupies 305 μm × 305 μm in the asynchronous version and 370 μm × 370 μm in the synchronous version. The breakdown of the used logic elements is shown in Fig. 9.23. This result is mainly because transparent latches used in asynchronous pipelines are simpler than flipflops used in synchronous design, and also the synchronous router has one more pipeline stage than the asynchronous design.

The average throughput of each router (after obtaining routing paths) is 262 MHz for an asynchronous router and 208 MHz for a synchronous one. This causes the performance difference between two versions as shown in Fig. 9.24, where “Flit latency” means the difference of the time when a flit is injected into an ideal input queue of the source router and the time when it arrives at the destination router. In this experiment, a random traffic pattern is assumed, and each packet has eight flits. As shown here, the asynchronous version has about twice the performance of the synchronous one.

Finally, Fig. 9.25 shows the power consumption of two designs for various packet injection rates. This reveals that the asynchronous router consumes power

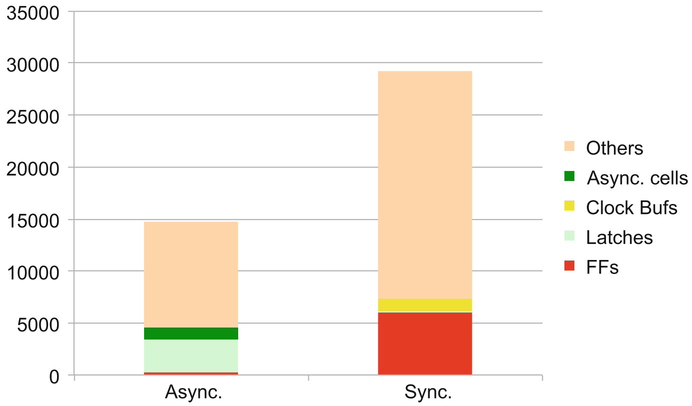


Fig. 9.23 Breakdown of used logic elements in the whole NoCs

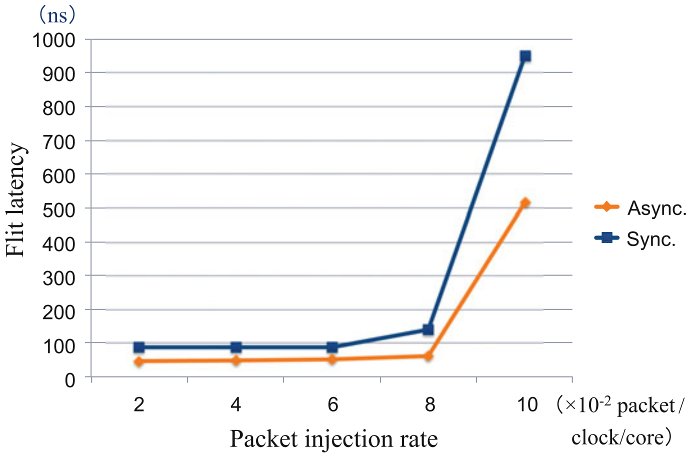


Fig. 9.24 Performance comparison

only when activities actually happen. In contrast, the synchronous router dissipates considerable power independently of the activities. It is easily guessed that the clock distribution circuits and the clock input sub-circuits of registers consume such power, because those circuits continuously work even if no valid data flow occurs.

9.3.6 Summary

This chapter has introduced some details of an asynchronous NoC. An NoC is a useful approach to constructing a dependable hardware platform using redundancy.

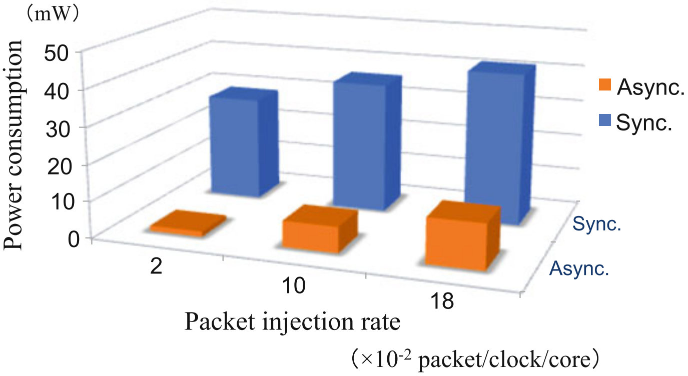


Fig. 9.25 Power consumption

Furthermore, by implementing NoC routers in an asynchronous design style, the robustness against various variations is obtained. In addition, asynchronous implementations have potential that they achieve better performance and consume less power compared to the corresponding synchronous ones. Chapter 19 shows an application of this asynchronous NoC to a safety-critical automotive control system. It is intended for readers who are interested in further details of more practical and complicated examples.

9.4 Timing and Synchronicity for Dependable Wireless Network

Suguru Kameda, Tohoku University
Hiroshi Oguma, National Institute of Technology, Toyama College
Akinori Taira, Tohoku University
Noriharu Suematsu, Tohoku University
Tadashi Takagi, Tohoku University
Kazuo Tsubouchi, Tohoku University

Communication traffic in wireless systems in the next 10 years is predicted to be 1000 times heavier than it is today. It is difficult to overcome this problem only by using conventional cellular networks. Therefore, the next-generation wireless communication network will evolve into a system that consists of multiple heterogeneous wireless network systems (see Sects. 7.1 and 7.2 for details), which allows for increased throughput and connectivity through flexible and versatile routing.

One of the main issues of heterogeneous wireless networks is seamless handover between heterogeneous wireless systems, which requires precise timing and highly accurate synchronization. In the system handover process, connection loss and throughput degradation are serious problems.

First of all, wireless communication networks have so far been designed without using a common clock signal because of very long distances between terminals and base stations, so terminals and base stations of wireless communication systems are designed assuming asynchronous clocks. For communicating, it is necessary to synchronize between the terminal and the base station at the start of communication. Since overhead time for synchronization is necessary, throughput of wireless system would degrade. Especially in heterogeneous wireless networks, the asynchronous problem is more serious because more initial synchronization is necessary.

Moreover, asynchronicity of wireless systems causes the interference between wireless channels. For example, in uplink of code division multiple access (CDMA) systems, the timing jitter between CDMA channels causes co-channel interferences leading to the degradation of the throughput of uplink with timing jitters.

To solve the abovementioned asynchronous problem, we have discussed a universal clock synchronized wireless system that uses high-accuracy positioning signals from Global Navigation Satellite Systems (GNSS) such as the Global Positioning System (GPS) and the Quasi-Zenith Satellite System (QZSS), which is a Japan-specific satellite system [27]. Since terminals and base stations in wireless networks have a common clock, high-throughput heterogeneous wireless network with reliable system handover will be realized.

In this section, at first, we will discuss the issues of timing and synchronicity for next-generation dependable wireless networks. Next, we will evaluate the synchronization accuracy of GNSS by field tests. Finally, we will explain an overview of global networks and computing systems with highly accurate clock synchronization with GNSS. Three possibilities of applications using highly accurate clock synchronization will be explained: (1) A large capacity satellite communication system using QZSS, (2) A heterogeneous wireless system with a network selection scheme using positioning information, and (3) Computer coordination using ns-order clock synchronization.

9.4.1 Synchronization for Wireless Communication Systems

9.4.1.1 Synchronization in Conventional Systems

In this subsection, we will begin by looking at the synchronization scheme used in conventional wireless communication systems as shown in Fig. 9.26. Although a wireless terminal usually has a reference oscillator, its accuracy is sometimes insufficient because the frequency offset causes the degradation of reception performance and increases co-channel interference. So in usual wireless system, the carrier signal is recovered on the receiver by using received signals from transmitters. The carrier recovery, including frequency synchronization and phase synchronization, is processed mainly in radio frequency (RF) and/or intermediate frequency (IF). After the recovery of a received carrier signal, an automatic frequency control (AFC) is used for stabilizing reference signals in the receiver.

The received signal is very noisy because the signal includes additive white Gaussian noise (AWGN) and interference. Since a wireless channel normally consists of multiple paths (direct wave plus some reflected waves), the received signal is affected by fading. Therefore, it is necessary for carrier recovery to consider these effects.

In baseband circuits, the clock signal is used for chip,[1] symbol, and frame synchronizations. Chip synchronization, also called despread, is the synchronization method of spreading code for spread spectrum (SS) CDMA technology. Symbol synchronization is for the demodulation of the received signal. Frame synchronization is a process that detects headers of framed data streams. For these synchronization processes, especially chip synchronization, a high-accuracy clock is needed. For the third-generation (3G) cellular system of wideband CDMA using 3.84 Mchips/s, a timing accuracy of 260 ns is necessary for chip synchronization.

Moreover, in conventional wireless systems, there is no synchronization between terminals of wireless system. For example, in the uplink of a cellular system, since the transmission timing from terminals is not synchronized and the distances between terminals and base station are not constant, the receiving timing at the base station is not synchronized. The asynchronicity between terminals is a very serious issue in the case of system handover of heterogeneous wireless systems.

9.4.1.2 Synchronization in Universal Clock Synchronized Wireless Network

To solve the abovementioned problem, we propose the universal clock synchronized wireless network, called the synchronized spread spectrum code division multiple access (synchronized SS-CDMA) [28–33]. Since terminals and base stations in the network of synchronized SS-CDMA have a universal clock signal, they can synchronize by using the universal clock signal with each other. At the time of a communication start, terminals and base stations can synchronize in less time than that of asynchronous wireless network. Since overhead time for synchronization is not necessary, throughput of wireless system does not degrade.

Moreover, since the terminals can get highly accurate location information by using the GNSS signal, each terminal can calculate its own location and time precisely and synchronize its own clock and frequency to those of the QZSS. The terminal transmits it in synchronization with other terminals. As a result, in the system handover process, it can decrease connection loss and throughput degradation.

[1] The "chip" is a pulse of a direct-sequence spread spectrum (DSSS) code.

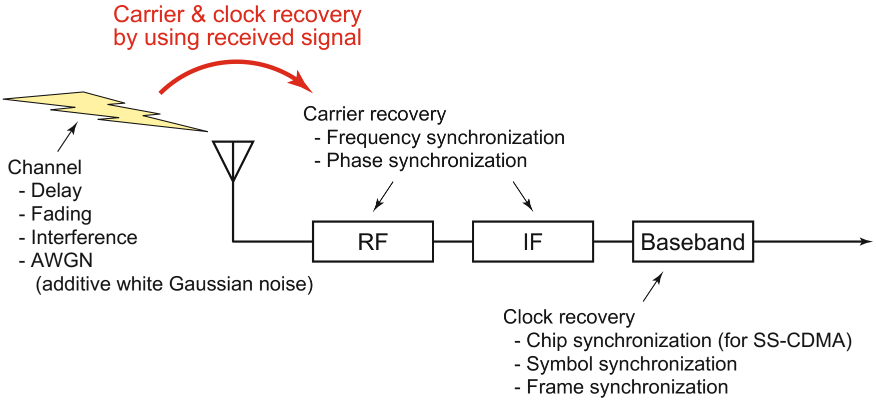


Fig. 9.26 Synchronization in conventional wireless systems. The carrier and clock signals are recovered on the receiver by using signals received from the transmitter

Figure 9.27 shows the synchronization scheme of the synchronized SS-CDMA. In the proposed scheme, the carrier and clock recovery methods use high-accuracy positioning signals from GNSS such as the GPS and the QZSS. The received GNSS signals are not noisy because there are less interferences and fewer multiple paths. Therefore, by using global synchronization via satellites, it can be done much more easily and with highly accurate to recover carrier and clock signals.

For getting highly accurate timing and location information, the terminal needs at least four received positioning signals from GNSS satellites. Moreover, since one

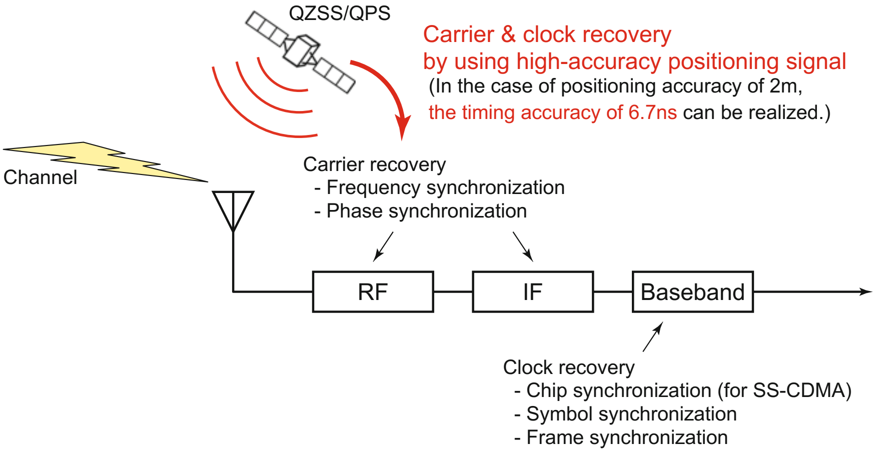

QZSS/QPS
Carrier & clock recovery
by using high-accuracy positioning signal
(In the case of positioning accuracy of 2m,
the timing accuracy of 6.7ns can be realized.)
Channel
Carrier recovery
- Frequency synchronization
- Phase synchronization
RF
IF
Baseband
Clock recovery
- Chip synchronization (for SS-CDMA)
- Symbol synchronization
- Frame synchronization

Fig. 9.27 Synchronization in the synchronized spread spectrum code division multiple access (synchronized SS-CDMA) scheme (the universal clock synchronized wireless network). In the proposed scheme, the carrier and clock recovery methods use high-accuracy positioning signals from GNSS such as QZSS and GPS

satellite of QZSS always appears near the zenith above the region of Japan, the QZSS can contribute to the accuracy of location and timing information.

Recently, the positioning signal of QZSS has reached a high accuracy of sub-meter class. For the positioning accuracy of 2 m, the timing accuracy will be 6.7 ns. Therefore, by using positioning signal, the synchronized wireless network will be realized.

9.4.2 System Synchronization by Using Global Navigation Satellite System (GNSS)

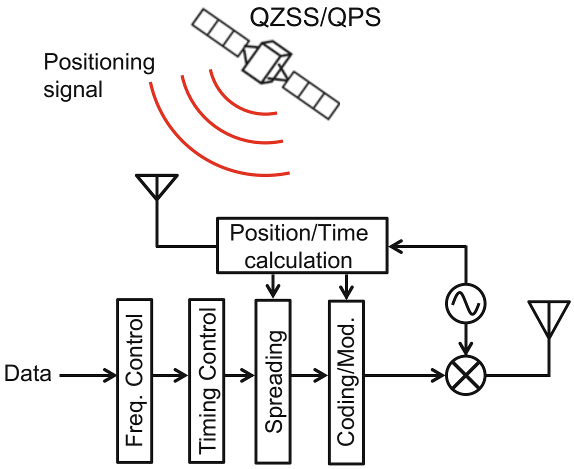
In this subsection, the timing synchronization accuracy of GNSS will be discussed. At first, the synchronization method by using GNSS will be explained. Next, the experimental evaluations of the timing synchronization accuracy will be shown.

9.4.2.1 Synchronization Method by Using GNSS

Figure 9.28 shows the block diagram of synchronized SS-CDMA terminal. Each terminal adjusts the transmit timing and carrier frequency using the location and timing information, which are derived from the received positioning signals of GNSS satellites.

Figure 9.29 shows the mechanism of timing synchronization on the receiver. All terminals calculate their own propagation time and adjust the transmit timing so as to set the reception timing at the same time. There are two factors in the timing error of the synchronized SS-CDMA: (1) timing error among terminals and (2) transmission timing jitter depending on the position error. The target timing error of the

Fig. 9.28 Block diagram of synchronized SS-CDMA terminal



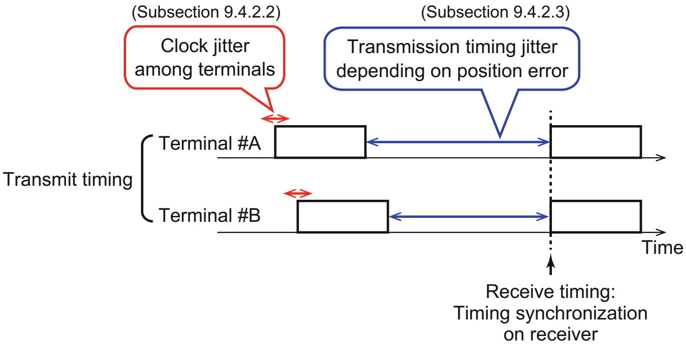

(Subsection 9.4.2.2)
Clock jitter among terminals
(Subsection 9.4.2.3)
Transmission timing jitter depending on position error
Transmit timing
Terminal #A
Terminal #B
Time
Receive timing: Timing synchronization on receiver

Fig. 9.29 Mechanism of timing synchronization on receiver. All terminals calculate own propagation time and adjust transmit timing so as to set the reception timing same time

synchronized SS-CDMA is tentatively set at 50 ns for realizing large capacity QZSS SS-CDMA short-message communication system written in Sect. 9.4.3.1. This target timing error of 50 ns is the precision that is feasible at 100% of accommodation rate of the QZSS SS-CDMA short-message communication system (see Sect. 23.2 and Ref. [29] for details).

In Sects. 9.4.2.2 and 9.4.2.3, experimental evaluations of two errors will be explained.

9.4.2.2 Measurement of Timing Error Among Terminals by Using GPS Oscillator

In this subsection, for realizing the synchronized SS-CDMA, timing error among terminals (written in Fig. 9.29) will be evaluated by using a clock signal output from a GPS oscillator module. Figure 9.30 shows a GPS oscillator module (Furuno GF-180TC) [34]. Output of the GPS oscillator module is a clock signal called 1 pulse per second (1PPS). This module has a temperature compensated crystal oscillator (TCXO). Although GF-180TC was developed for the base station at first, we evaluated this as an oscillator on the mobile terminals in this measurement.

Figure 9.31 shows the measurement system of the clock jitter between two GPS oscillators. In this evaluation, a clock jitter is assumed as a difference of 1PPS clock signal. Figure 9.31a shows the block diagram of the measurement system. The antenna connected with the GF-180TC (A) was in open sky conditions. In the case of Fig. 9.31a, there was a radar absorbent material near the antenna connected with the GF-180TC (B) for reducing number of visible satellites. The clock jitter can be observed by a measurement of the difference of 1PPS signal between two GF-180TC oscillators. Figure 9.31b shows a photograph of the measurement systems without radar absorbent material.

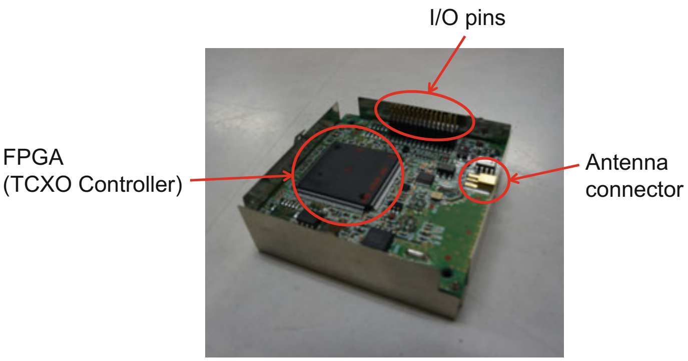
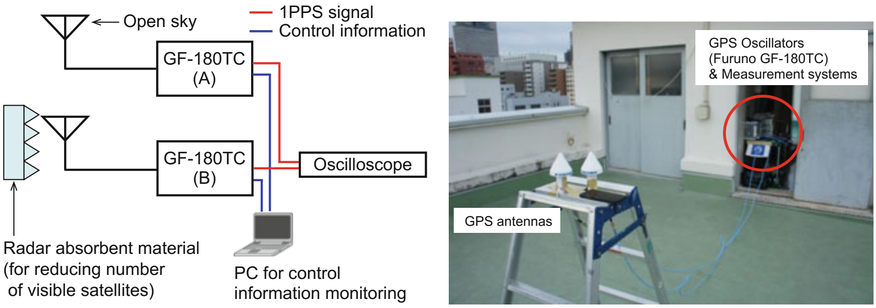


Fig. 9.30 GPS oscillator module (Furuno GF-180TC) [34]. The GF-180TC has a temperature compensated crystal oscillator (TCXO)

Figure 9.32 shows a cumulative distribution function (CDF) of the number through the visible satellites of GF-180TC. The horizontal axis is the number of visible satellites through the GF-180TC. The vertical axis is CDF. The number of visible satellites can be monitored by the control information of the GF-180TC. The number of visible satellites in the presence of the radar absorbent material is smaller than without the radar absorbent material.

Figure 9.33 shows an example of the clock jitter measurement on two GPS oscillators. The horizontal axis is time. The vertical axis is amplitude. In the following evaluations, the ideal timing, e.g., Coordinated Universal Time (UTC), is assumed as the middle value of the jitter between two 1PPS signals. So, the 1PPS relative error from the ideal timing is assumed as shown in Fig. 9.33.



(a) Block diagram of measurement system of clock jitter

(b) Photograph of the measurement system without a rader absorbent material

Fig. 9.31 Measurement system of clock jitter between two GPS oscillators

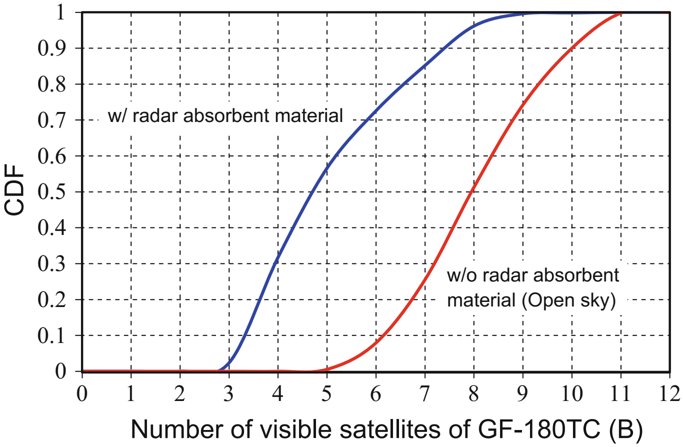


Fig. 9.32 CDF of number of visible satellites through the GF-180TC

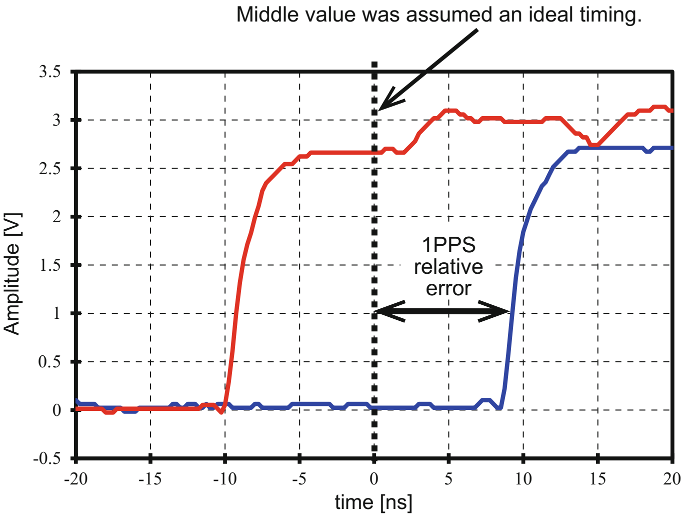
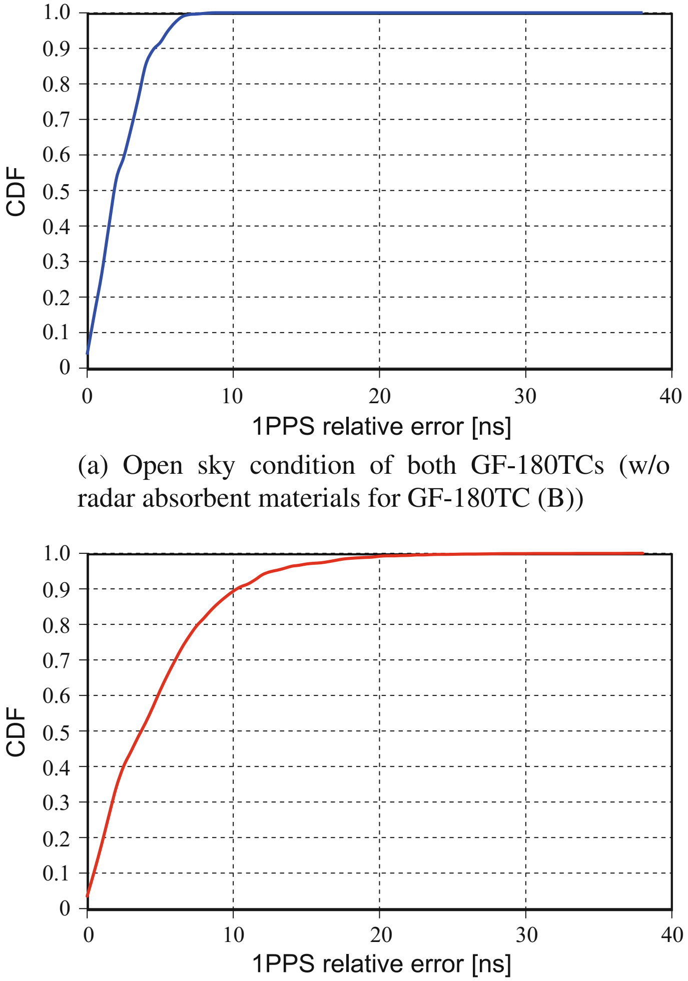


Fig. 9.33 Measurement result example of clock jitter of two GPS oscillators

Figure 9.34 shows the CDFs of the measurement timing error. In the case of Fig. 9.34a, both oscillators were in open sky (w/o radar absorbent materials), so this evaluation is for an individual difference of oscillators. The horizontal axis is 1PPS relative error. The vertical axis is CDF. The maximum value of timing error is 10.0 ns. The timing error in the case of a CDF of 0.9 is 5.0 ns. In the case of Fig. 9.34b, there was a radar absorbent material with GF-180TC (B). The maximum value of timing error is 38.0 ns. The timing error in the case of a CDF of 0.99 is 20.0 ns.



(a) Open sky condition of both GF-180TCs (w/o radar absorbent materials for GF-180TC (B))

(b) With radar absorbent materials for GF-180TC (B)

Fig. 9.34 CDFs of the measurement timing error

Figure 9.35 shows the CDF of the measurement timing error with elevation angle masks (w/o radar absorbent materials for GF-180TC (B)). The elevation angle masks correspond to the sky view factor. In the case of elevation angle masks of 0°, 20°, and 30°, the sky view factor is 100% (open sky condition), 60%, and 44%, respectively. In the case of a sky view factor of 60% and 44%, the maximum value of timing error is 19.0 ns and 26.5 ns, respectively.

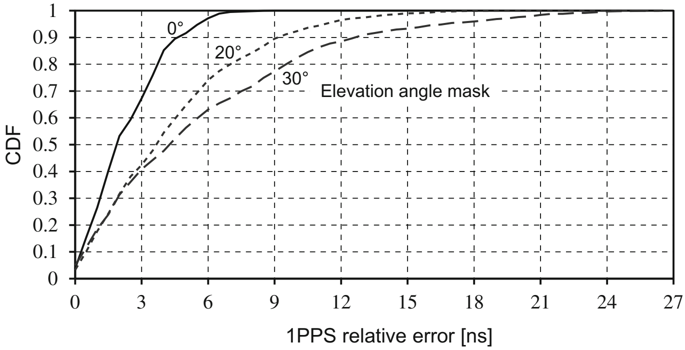


Fig. 9.35 CDF of the measurement timing error with an elevation angle mask [w/o radar absorbent materials for GF-180TC (B)]

9.4.2.3 Measurement of Transmission Timing Jitter Depending on Position Error by Using QZSS and GPS

In this subsection, for realizing the synchronized SS-CDMA, the transmission timing jitter depending on the position error (written in Fig. 9.29) will be evaluated by using a QZSS/GPS receiver. Figure 9.36 contains photographs of the measurement system of the positioning error by using QZSS and GPS. Figure 9.36a is a photograph of the QZSS/GPS receiver (Core CD311 [35]). The receiver can receive the high-accuracy L1-band submeter-class augmentation with integrity function (L1-SAIF) signal of the QZSS. Figure 9.36b shows a photograph of the measurement environment.

Figure 9.37 shows the measurement results of the positioning errors. Figure 9.37a, b, c shows the elevation angle masks of 0°, 20°, and 30°, respectively. The measurement times of Fig. 9.37a–c are 30 min each. Each plot is

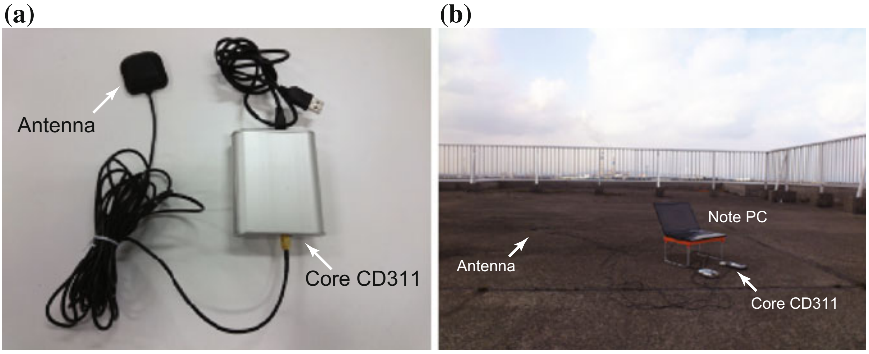


Fig. 9.36 Photographs of the measurement system of the positioning error by using QZSS and GPS

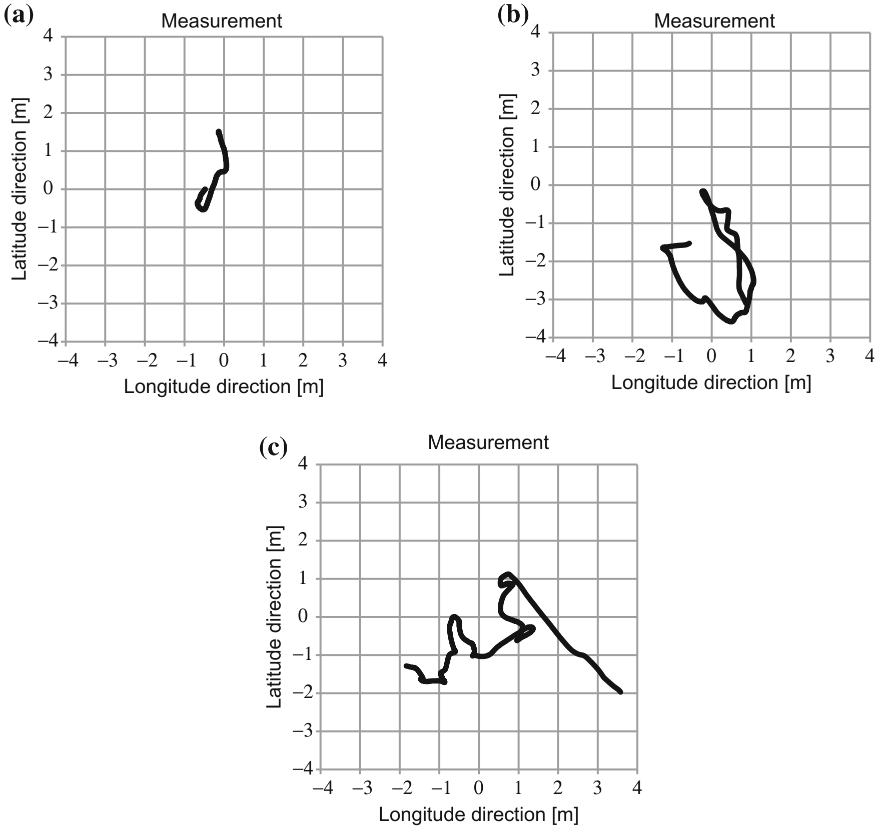


Fig. 9.37 Measurement results of the positioning error

determined by averaging values every 5 min. As shown in Fig. 9.37a, in the case of a sky view factor of 100% (elevation angle mask of 0°, open sky condition), the maximum value of positioning error is less than 2 m.

The transmission timing error can be calculated from the position error. Figure 9.38 shows the CDF of the transmission timing control error calculated from Fig. 9.37 with elevation angle masks. In the case of a sky view factor of 100%, 60%, and 44%, the maximum value of the timing error is 5.1 ns, 12.1 ns, and 13.7 ns, respectively.

Table 9.1 shows the receive timing error in the receivers. As shown in Fig. 9.29, the total timing error in the receivers is given by the summation of timing errors among terminals (from Fig. 9.35) and the transmission timing error due to positioning error (from Fig. 9.38). In the case of a sky view factor of 100%, 60%, and 44%, the maximum value of the timing error is 15.1 ns, 31.1 ns, and 40.2 ns, respectively, which is smaller than the target timing error of the synchronized SS-CDMA of 50 ns for realizing large capacity satellite communication system

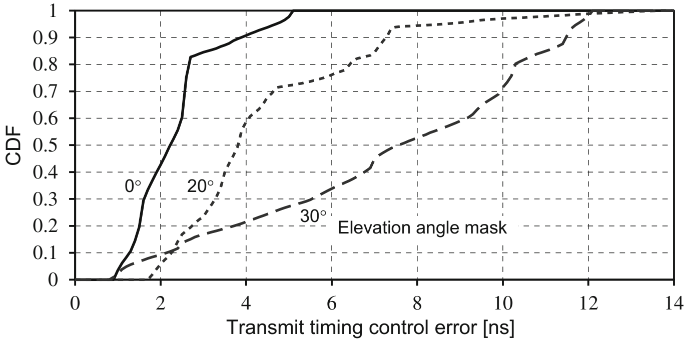


Fig. 9.38 CDF of the transmission timing control error

Table 9.1 Receive timing error in the receivers

Elevation angle mask	$\theta = 0°$	$\theta = 20°$	$\theta = 30°$
Sky view factor (%)	100	60	40
Timing error among terminals (T_{j1}) (ns)	10.0	19.0	26.5
Transmission timing error due to positioning error (T_{j2}) (ns)	5.1	12.1	13.7
Receive timing error in receiver ($T_{j1} + T_{j2}$) (ns)	15.1	31.1	40.2

using QZSS written in Sect. 9.4.3.1 (see Sect. 23.2 and Ref. [29] for details). The evaluations described above thus provides the basic proof of the concept, that the highly accurate positioning signal from GNSS can be used for the synchronized SS-CDMA. More detailed discussions of the concept and accuracy of SS-CDMA using GNSS are underway.

9.4.3 Timing Dependability for Global Network and Computing Systems

Since the nanosecond (ns) order clock synchronization using QZSS and GPS can be realized as shown in Sect. 9.4.2, the next-generation global network and computing systems will be able to upgrade by using a high-accuracy clock synchronization with GNSS. Figure 9.39 shows an overview of global network and computing systems with highly accurate clock synchronization with GNSS. In this subsection, three possibilities of applications using a high-accuracy clock synchronization will be explained.

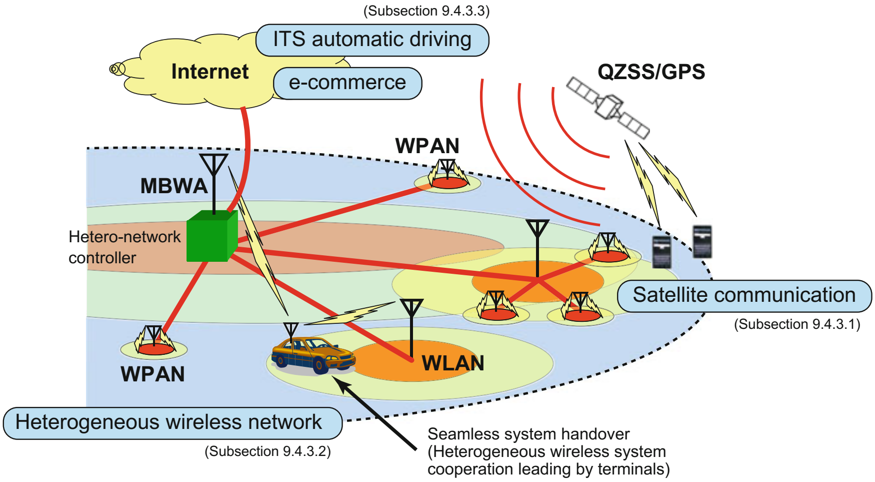


Fig. 9.39 Overview of global network and computing systems with highly accurate clock synchronization with GNSS

9.4.3.1 Large Capacity Satellite Communication System Using QZSS

By using ns-order clock synchronization, high-efficiency wireless communication can be realized. For example, the large capacity satellite communication using QZSS will be discussed in Chap. 23 of this book.

When a great disaster occurs, terrestrial infrastructure could be seriously damaged. Thus, satellite communication has an important role to keep a minimum reliable connection. QZSS is expected to provide a high-accuracy positioning service and allows two-way communication which includes the terminal location and short messages. We propose the SS-CDMA scheme which realizes direct access from terminals to the satellite, and simultaneous multiuser transmission using large spreading factor SS codes. In this system, keeping orthogonality among users in the time and frequency domain is the most important issue. The detail of this system will be explained in Sect. 23.2.

9.4.3.2 Heterogeneous Wireless System with Network Selection Scheme Using Positioning Information

It is self-evident that the next-generation wireless network will evolve to the heterogeneous wireless network as shown in Sect. 9.4.1. The main issue of heterogeneous wireless networks is seamless system handover. In Fig. 9.39, an example of the seamless system handover method is drawn.

By using location information with clock synchronization, we proposed a high-reliability and high-efficiency network selection scheme. In the proposed scheme, users select a cell using their location and the channel quality information. The channel quality information at each location is provided for the cell selection. User terminals can guess the channel quality information by measuring only their locations. In other words, the best connection is automatically identified by using the location information. Furthermore, this channel quality information is the average of the signal strength and the traffic load information. Therefore, users can suppress the cell selection error and select a cell in response to the real-time traffic load variation. The details of this scheme will be explained in Sect. 23.3.

9.4.3.3 Computer Coordination Using ns-Order Clock Synchronization

It is important for a number of applications on the Internet to be able to have and share highly accurate clock signals. Although the accuracy of clocks of network nodes is now millisecond (ms) order, high-accuracy clocks such as microsecond (μs) or ns-order will be needed in the near future.

By using ns-order clock synchronization with GNSS, all network nodes (computers), including small size mobile terminals, will be able to synchronize with universal clock such as the UTC. Coordination between computers will be able to upgrade by using universal clock synchronization. For example, worldwide synchronized transaction and distributed computing will be realized by using high-accuracy positioning signals provided from QZSS and GPS.

As a result, the applications of computer coordination using clock synchronization will be widely used in the near future. In Fig. 9.39, examples of computer coordination using ns-order clock synchronization are depicted; (1) e-commerce with ns-order timing control high-speed transaction, and (2) automatic driving with ns-order timing control and highly accurate location control.

References

1. IEC 61508 ed2.0, Functional safety of electrical/electronic/programmable electronic safety-related systems (2010)
2. H. Kopetz, *Real-Time Systems*, 2nd edn. (Springer, 2011)
3. A. Namiki, Y. Nakabo, I. Ishii, M. Ishikawa, 1 ms Sensory-motor fusion system. IEEE Trans. Mechatron. **5**(3), 244–252 (2000)
4. Y. Nakabo, I. Ishii, M. Ishikawa, 1 ms target tracking system using a massively parallel processing vision. J. Robot. Soc. Japan **15**(3), 105–109 (1997)
5. G.C. Buttazzo, *Hard Real-Time Computing Systems: Predictable Scheduling Algorithms and Applications* (Springer, 2004)
6. K. Suito, R. Ueda, K. Fujii, T. Kogo, H. Matsutani, N. Yamasaki, Dependable responsive multithreaded processor for distributed real-time systems. IEEE Micro. **32**(6), 52–61 (2012)
7. N. Yamasaki, Responsive link for distributed real-time processing, in *Proceedings of the 10th International Workshop on Innovative Architecture for Future Generation High-Performance Processors and Systems* (2007), pp. 20–29

8. J. Urata, Y. Nakanishi, K. Okada, M. Inaba, Design of high torque and high speed leg module for high power humanoid, in *Proceedings of the 2010 IEEE/RSJ International Conference on Intelligent Robots and Systems* (2010), pp. 4497–4502
9. H. Takada, μITRON 4.0 Specification (TRON Institute, 2004)
10. C.L. Liu, J.W. Layland, Scheduling algorithms for multiprogramming in a hard real-time environment. J. ACM **20**(1), 46–61 (1973)
11. N. Yamasaki, Responsive multithreaded processor for distributed real-time systems. J. Robot. Mechatron. **17**(2), 130–141 (2005)
12. J.W.S. Liu, *Real-Time Systems* (Prentice Hall, 2000)
13. N. Yamasaki, I. Magaki, T. Itou, Prioritized SMT architecture with IPC control method for real-time processing, in *Proceedings of the 13th IEEE Real-Time and Embedded Technology and Applications Symposium* (IEEE, 2007), pp. 12–21
14. J.G. Ziegler, N.B. Nichols, Optimum settings for automatic controlles. ASME Trans. **64**(11), 759–768 (1942)
15. T. Itou, N. Yamasaki, Design and implementation of the multimedia operation mechanism for responsive multithreaded processor. J. Robot. Mechatron. **17**(4), 456–462 (2005)
16. M. Dean, T. Williams, D. Dill, Efficient self-timing with level-encoded 2-phase dual-rail (LEDR), in *Advanced Research in VLSI*, ed. by C.H. Séquin (MIT Press, 1991), pp. 55–70
17. M. Imai, T. Yoneda, Improving dependability and performance of fully asynchronous on-chip networks, in *Proceedings of ASYNC2011* (2011), pp. 65–76
18. R. Dobkin, R. Ginosar, A. Kolodny, Qnoc synchronous router. integration. VLSI J. **42**(2), 103–115 (2009)
19. Y. Thonnart, P. Vivet, F. Clermidy, A fully-asynchornous low-power framework for gals NOC integration, in *Proceedings of DATE* (2010), pp. 33–38
20. M.N. Horak, S.M. Nowick, M. Carlberg, U. Vishkin, A low-overhead asynchronous interconnection network for gals chip multiprocessors, in *Proceedings of NOCS* (2010), pp. 43–50
21. T. Yoneda, M. Imai, N. Onizawa, A. Matsumoto, T. Hanyu, Multi-chip NoCs for automotive applications, in *Proceedings of PRDC* (2012), pp. 105–110
22. M. Singh, S.M. Nowick, MOUSETRAP: ultra-high-speed transition-signaling asynchronous pipelines, in *Proceedings International Conference Computer Design (ICCD)* (Nov 2001), pp. 9–17
23. A.J. Martin, Programming in VLSI: from communicating processes to delay-insensitive circuits, in *Developments in Concurrency and Communication*, UT Year of Programming Series, ed. by C.A.R. Hoare (Addison-Wesley, 1990), pp. 1–64
24. C. Myers, *Asynchronous Circuit Design* (Wiley, 2001)
25. M. Imai, T. Yoneda, T. Nanya, N-way ring and square arbiters. in *Proceedings of the ICCD'09* (2009), pp. 125–130
26. G. Miorandi, D. Bertozzi, S.M. Nowick, Increasing impartiality and robustness in high-performance n-way asynchronous arbiters, in *Proceedings of ASYNC* (2015), pp. 108–115
27. K. Tsubouchi, Extended dependable air: heterogeneous wireless network for surface, space and sea, in *Asia-Pacific Microwave Conference 2014 (APMC2014)* (Nov 2014 (invited))
28. T. Takahashi, Y. Miyake, F. Yamagata, H. Oguma, S. Kameda, N. Suematsu, T. Takagi, K. Tsubouchi, Large-capacity QZSS location and short message system using frame slotted ALOHA with flag method, in *IEEE 24rd International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC2013)* (London, U.K., Sept 2013), pp. 3280–3285
29. A. Taira, Y. Miyake, S. Kameda, N. Suematsu, T. Takagi, K. Tsubouchi, QZSS location and short message communication system against big disasters, in *Vietnam-Japan International Symposium on Antennas and Propagation (VJISAP2013)* (Jan 2014 (invited)), pp. 229–234
30. A. Taira, Y. Miyake, S. Kameda, N. Suematsu, T. Takagi, K. Tsubouchi, System stability of SS-CDMA location and short message communication using QZSS, in *Asia-Pacific Microwave Conference 2014 (APMC2014)* (Nov 2014)

31. Y. Miyake, S. Kameda, A. Taira, K. Norishima, H. Oguma, N. Suematsu, T. Takagi, K. Tsubouchi, Experimental evaluation of timing synchronization accuracy consider elevation angle mask for QZSS SS-CDMA short message communication, in *IEICE Technical Report*, vol. 115, no. 2, RCS2015-10 (April 2015), pp. 47–52 (in Japanese)
32. N. Suematsu, S. Kameda, Y. Miyake, T. Takahashi, A. Taira, T. Takagi, K. Tsubouchi, QZSS SS-CDMA location and short message communication system, in *2015 Vietnam-Japan MicroWave 2015 (VJMW2015)* (Ho Chi Minh City, Vietnum, Aug 2015 (invited))
33. K. Ohya, S. Kameda, H. Oguma, A. Taira, N. Suematsu, T. Takagi, K. Tsubouchi, Experimental evaluation of timing synchronization accuracy for QZSS short message synchronized SS-CDMA communication, in *2016 IEEE 27th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 2016)* (Sept 2016)
34. FURUNO ELECTRIC CO., LTD., GF-180TC, http://www.furuno.com/en/products/gnss-module/GF-180TC
35. CORE CORPORATION, CD311, http://www.core.co.jp/product/gnss/outline/qzs_gps.html

Chapter 10
Malicious Attacks on Electronic Systems and VLSIs for Security

Takeshi Fujino, Daisuke Suzuki, Yohei Hori, Mitsuru Shiozaki, Masaya Yoshikawa, Toshiya Asai and Masayoshi Yoshimura

Abstract In this chapter, we briefly review malicious attacks that have been attempted on security-critical systems employing a variety of methods, and discuss cryptographic functions embedded in VLSIs to be used in systems which require dependability in terms of protection against attackers. Recent cryptographic algorithms such as AES or RSA are computationally safe in the sense that it is practically impossible to reveal the key information from a pair of plain and cipher texts if a key with a sufficient length is used. An attacker would therefore try to reveal the cryptographic keys by exploiting possible implementation flaws in the security LSIs. For example, attempts have been made to modify the control flow of a program and read out the key data. Other types of attacks have used side-channel information such as power traces or electromagnetic emission from the LSIs. Therefore, of the utmost importance in security LSIs is "tamper resistance" or robust key-protection mechanisms. In Sect. 10.1, the role of LSIs in the integrity of security-critical systems is presented and a review is given over reported incidents

T. Fujino (✉) · M. Shiozaki
Ritsumeikan University, Kusatsu, Japan
e-mail: fujino@se.ritsumei.ac.jp

M. Shiozaki
e-mail: mshio@fc.ritsumei.ac.jp

D. Suzuki
Mitsubishi Electric Corporation, Kamakura, Japan
e-mail: Suzuki.Daisuke@bx.MitsubishiElectric.co.jp

Y. Hori
National Institute of Advanced Industrial Science and Technology (AIST), Tsukuba, Japan
e-mail: hori.y@aist.go.jp

M. Yoshikawa · T. Asai
Meijo University, Nagoya, Japan
e-mail: masay@meijo-u.ac.jp

M. Yoshimura
Kyoto Sangyo University, Kyoto, Japan
e-mail: yoshimura.masayoshi@cc.kyoto-su.ac.jp

S. Asai (ed.), *VLSI Design and Test for Systems Dependability*,
https://doi.org/10.1007/978-4-431-56594-9_10

of malicious attacks. Section 10.2 discusses typical tampering methods against cryptographic circuits in more detail. Tamper-resistant security hardware design and verification methods are introduced in Sects. 10.3 and 10.4. The vulnerability of scan-based test scheme is discussed in Sect. 10.5. A testing environment called SASEBO (http://www.toptdc.com/product/sasebo/) for evaluation of security LSIs is introduced in Sect. 10.6.

Keywords Cryptographic circuits • Fault analysis attacks • Side-channel attacks
Tamper resistance

10.1 The Role of Security LSI and the Example of Malicious Attacks

Takeshi Fujino, Ritsumeikan University
Daisuke Suzuki, Mitsubishi Electric Corporation

10.1.1 The Role of Security Function and System Example

The five functions: Confidentiality, Integrity, Availability, Authenticity, and Accountability are essential components in computer security [1]. These components except availability are depicted in Fig. 10.1. Confidentiality is the function that protects the system from having its data stolen (e.g., by eavesdropping). Authenticity is the function that permits authorized access, while rejecting unauthorized (and thereby preventing spoofing). Integrity prohibits attempts to alter the system and/or the data stored in the system. Accountability validates or justifies the behavior of the system (so that repudiation, for example, is invalidated). Availability is the function that enables the use of the system at any time.

An example of systems, as in the bank-card, credit-card, or corporate work environment, where smart cards are used for controlling access to a central server is illustrated in Fig. 10.2. A user enters into the system through an authentication process (1) using the card, a client computer to the server computer, and a key, KA, which is kept secret between user and the owner of the system. The data on the central storage is encrypted by the user's encryption keys, KE, and a user has an access to it within the limitations of authorization the owner give him/her.

The secret key information is not directly exchanged to avoid the risks of eavesdropping. The challenge–response authentication protocol is used instead as indicated by step (1) in Fig. 10.2. When the client requests authentication to the server, a "challenge," which is a random number generated on the server, is delivered to the client. The client then encrypts the "challenge" with the authentication key, KA, and sends it back to the server as the "response." The server, upon

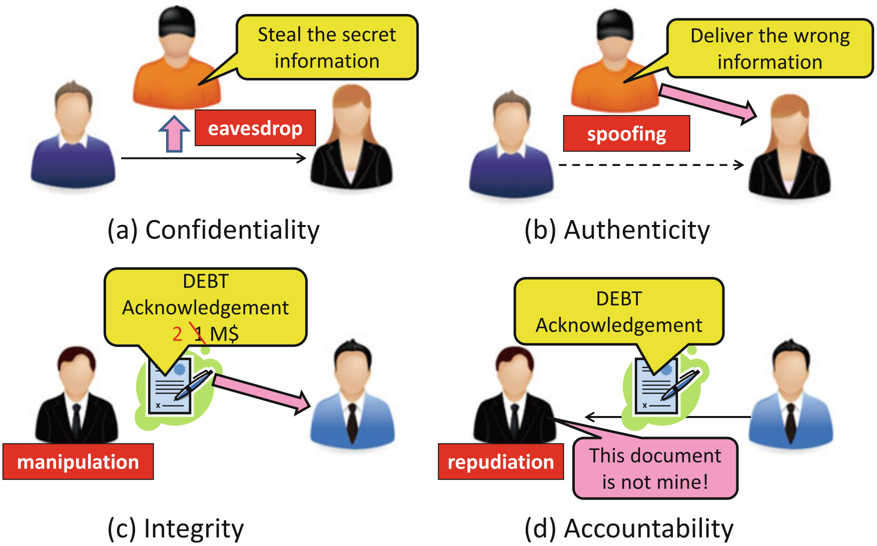


Fig. 10.1 The roles of computer security

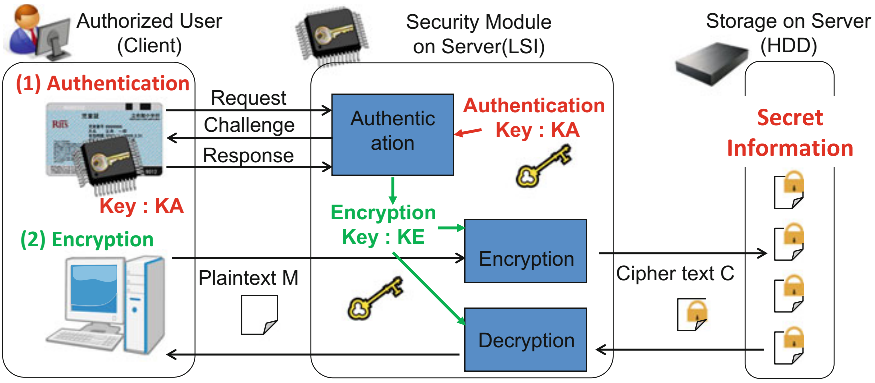


Fig. 10.2 The system example using computer security functions

confirmation that the "challenge" encrypted by the server by the same key KA it possesses proves identical to the "response", the client, or the user, is authenticated.

Going further to use the system, the user accesses the data on the server he/she has been authorized to access by using another encryption key, KE, as indicated by step (2) in Fig. 10.2. The data he/she wants to store on the central storage is encrypted by the client before being transmitted. Conversely, the encrypted data on the storage is downloaded from the server and decrypted by the client when the user wants to read it out.

10.1.2 Attack Incidents to Security LSIs

Attack incidents reported to date on commercial security LSIs can be categorized into two groups. In the first group, it was the vulnerabilities of cryptographic algorithms or protocols embedded in the security LSI that have been exploited by attackers. The attack on the MIFARE classic [2] that is shown here. MIFARE classic that is a contact-less smart card supplied from NXP Semiconductors, is a well-known example. A proprietary encryption algorithm Crypto-1 created by NXP was used on the card. Though the security of Crypto-1 partly relied on the secrecy of the algorithm, however, the confidential algorithm was exposed by reverse engineering. Possibilities of theft and cloning of the card information have been reported in a subsequent research [3]. A similar incident was reported on the remote keyless entry system on automobiles supplied from Microchip Technology [4].

The second category of attack incidents has to do with improper "implementations" of cryptographic algorithms. In such cases, the security functions can be vulnerable even if the cryptographic algorithms and protocols are secure. An "implementation" attack was reported on PlayStation 3 (PS3) supplied from Sony Computer Entertainment [5]. The ECDSA (Elliptic Curve Digital Signature Algorithm) used in PS3 was considered sufficiently strong against cryptanalysis, and thus it was listed in 2013 among the Japanese E-Government recommended ciphers [6]. The key extraction attack succeeded because a parameter, which should have been different for each operation, was fixed in the implementation of PS3.

The "side-channel attacks" that also exploit vulnerabilities in implementation, can be successful even when there is no such flaw in algorithm implementation. The incidents of the attacks are listed in Table 10.1. In order to counteract "side-channel attacks", therefore, sufficient care has to be taken in the design and verification of cryptographic circuits.

10.1.3 Cryptographic Circuits and Other Components

When attackers try to reveal a secret key, the main target on the security LSI would be the cryptographic circuit. In addition, the bus and memory circuits can be alternative targets because the key data is transferred or stored in these circuits.

(a) The symmetric-key cryptography and its operation

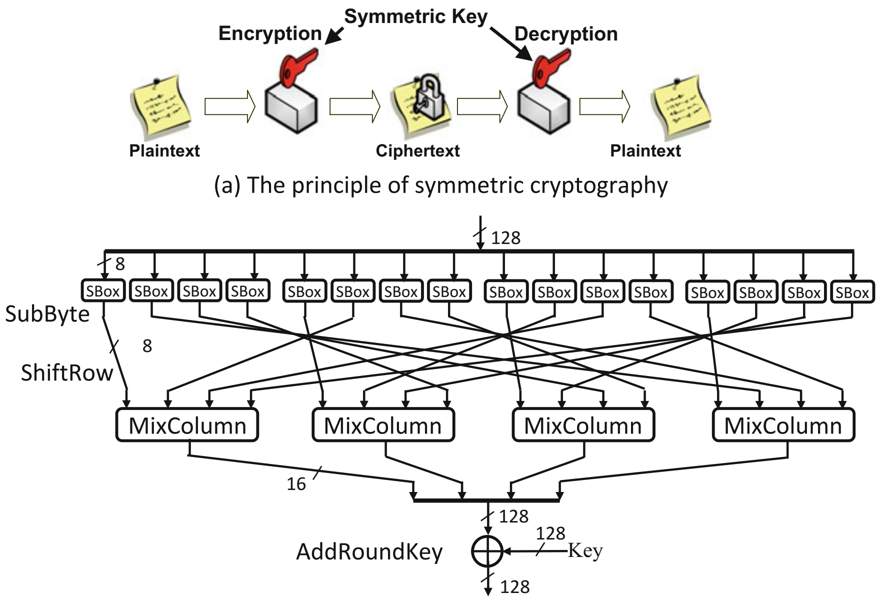
The symmetric-key cryptography scheme is one of the most popular algorithms to keep the data secret. The ancient Caesar cipher falls in this category. The sender and the receiver share a common secret data called the symmetric key before exchanging data. The sender encrypts a plaintext with the symmetric key and produce a ciphertext. On the other hand, the receiver decrypts the ciphertext with the same symmetric key. As a result, the original plaintext is recovered as shown in Fig. 10.3a. In order to protect data from a third party, the symmetric key must be kept secret to others.

Table 10.1 The attack incidents on the security LSI

Conference	The title of the paper	Abstract
CRYPTO 2008	On the power of power analysis in the real world: a complete break of the KeeLoq code hopping scheme [7]	The side-channel attack was realized against the security LSI used in the commercial key-less entry system. The key-cloning was also successful because both the secret key of a remote transmitter and the manufacturer key stored in a receiver were revealed
BlackHat 2010	Deconstructing a 'secure' processor [8]	The infineon security LSI used in the TPM (trusted platform module) was cracked by the micro-probing of the chip. In general, this invasive reverse-engineering technique requires the high level skill and costs
CHES 2011	Breaking Mifare DESFire MF3ICD40: power analysis and templates in the real world [9]	The NXP contact-less smart card was cracked by the non-invasive side-channel attack. As a results, 112-bit secret key on 3DES algorithm was completely recovered. This attack can be realized at a low cost standard equipment
CT-RSA 2012	On the portability of side-channel attacks—an analysis of the Xilinx Virtex 4, Virtex 5, and Spartan 6 bitstream encryption mechanism [10]	The bitstream encryption mechanism on Xilinx FPGA was cracked by the basic side-channel attack utilizing power consumption analysis. Access to the key allows cloning and manipulating a FPGA design, which has been encrypted to protect the intellectual property and to prevent fraud
CHES 2012	Breakthrough silicon scanning discovers backdoor in military chip [11]	The Actel/Microsemi ProASIC3 Flash FPGA was cracked by analyzing the JTAG controller. This work revealed that a backdoor was inserted to the chips for accessing FPGA configuration

The symmetric-key cryptography is categorized into block ciphers and stream ciphers. In the stream cipher, the plaintext is encrypted bit by bit by EXORing it with a key stream. On the other hand, a data block of 64–256 bits is encrypted at a time in the block ciphers. In general, the stream ciphers require fewer calculation resources so it is favorable in encrypting large data with high speed. However, block ciphers are used in most applications, because research of the security analysis is well studied compared to the stream cipher.

The DES (Data Encryption Standard) algorithm [12] standardized in 1977 had been widely used until the mid-2000s. In the early 1990s, some cryptanalytical attacks such as "differential cryptanalysis" and "linear cryptanalysis" are developed. In addition, the 56-bits key of DES became too short to resist the brute-force key search owing to the progress of computer hardware in 1990s. Consequently, 3DES (triple DES) algorithm, which utilizes 3 different keys in the DES algorithm, was temporally used instead of DES. In 2001, AES (Advanced Encryption Standard)



(a) The principle of symmetric cryptography

(b) The configuration of 128bit AES cryptographic circuit

Fig. 10.3 The symmetric cryptography and the circuit configuration

algorithm [13] was formally approved as a US federal standard as a result of an open competition. At present, AES is widely used in many applications.

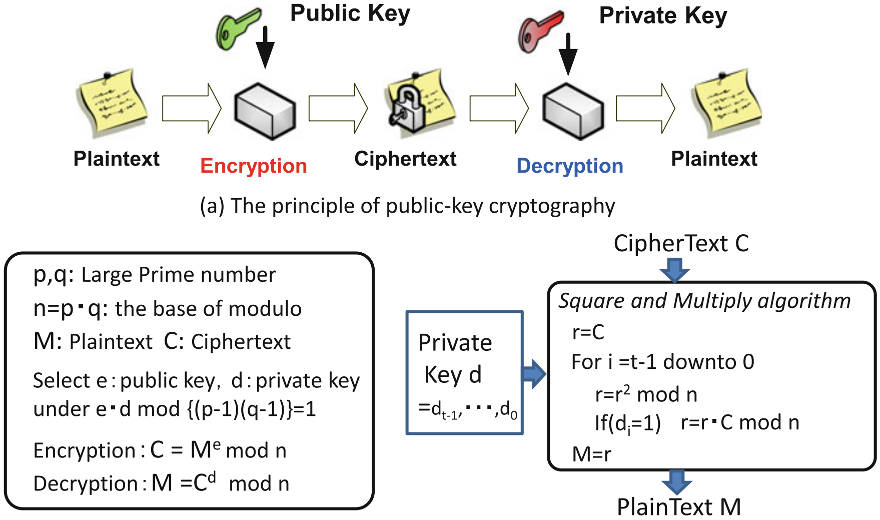
AES is the 128-bit block cipher algorithm that is operated on a sequence of 128-bit plain text blocks with the key size of 128, 192 or 256 bits. The input block undergoes 10-round encrypting operation using 10 different round keys generated by an initial key. Each round except the last round consists of 4 different layers as shown in Fig. 10.3b: SubByte, ShiftRow, MixColumn, and AddRoundKey operations. In the SubByte operation, each byte is substituted with another byte using a nonlinear substitution table called SBox (substitution box). The substitution is determined by a modular arithmetic over the Galois field, and is implemented in a nonlinear circuit composed of AND or OR gates. It has been known that power consumption of nonlinear circuits have input data dependency. Hence the SBox is the main target on the side-channel attack which exploits power consumption. The input 16 bytes are cyclically shifted in the ShiftRow transformation. The Mix-Column step is a liner transformation on 4 bytes using multiplication over the Galois field. The complete descriptions of the AES encryption processes including mathematical preliminaries are shown in FIPS-197 [13].

(b) The public-key cryptography and its operation

As shown in the sample security system in Fig. 10.2, the confidentiality and the authenticity can be realized using the symmetric-key algorithm. However, the accountability and the secure symmetric key exchange require other kinds of cryptography. In 1976, the principle of public-key cryptography which uses two separate keys was introduced. One of the keys is publicly distributed while another is kept private. As illustrated in Fig. 10.4a, the data encrypted with the public key can be decrypted with the private key. That is why this cryptography is called the "asymmetric cryptography". While the public and private keys are mathematically linked, an attacker who knows the public key cannot guess the private key.

The key distribution problem of the symmetric-key cryptography was solved by using the above-mentioned public-key cryptography. The symmetric key encrypted with the receiver's public key can be securely delivered to the receiver. Then the encrypted key can be decrypted with the private key of the receiver. Even if a third party gets the encrypted symmetric key, they cannot decrypt the key without the private key of the receiver. The public-key cryptography is used in the "digital signature", which authenticates the identity of the sender's message or document, to avoid spoofing or repudiation as depicted in Fig. 10.1.

The public-key cryptography algorithm most widely used today is the RSA algorithm [14] which was first presented in 1977 by Rivest, Shamir, and Adleman and later adopted as the world standard [15]. The three inventors of the algorithm, used the well-known fact that it is difficult to factor large integers. The RSA algorithm works as shown in Fig. 10.4b with *e* as the public key and *d* as the private key. Vulnerability for SCA could be introduced by the square-and-multiply algorithm used for exponentiation of large integers that is necessary for encryption and decryption process as in Fig. 10.4c. Assume the exponent is a key *d*. In the square-and-multiply algorithm, a bit in the key namely d_i is scanned in the loop. When $d_i = 1$, the square and multiply is carried out. In another case when



(a) The principle of public-key cryptography

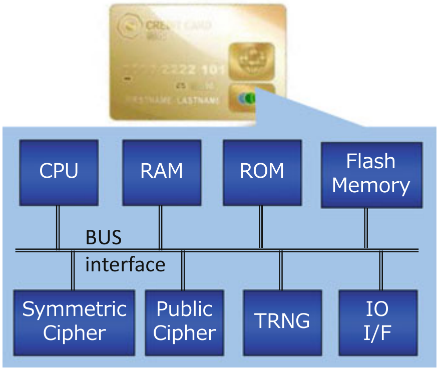
p,q: Large Prime number
n=p・q: the base of modulo
M: Plaintext C: Ciphertext
Select e : public key, d : private key under e・d mod {(p-1)(q-1)}=1
Encryption : C = M^e mod n
Decryption : M = C^d mod n

(b) The algorithm of RSA cryptography

```
Square and Multiply algorithm
  r=C
  For i =t-1 downto 0
     r=$r^2$ mod n
     If($d_i$=1)   r=r・C mod n
  M=r
```

(c) The calculation of exponentiation

Fig. 10.4 The public-key cryptography and the operation



Component	The role on the cryptography
CPU	System control and some operation and error sequence
RAM	Store the temporal value
ROM	Store the program
Flash Memory	Store the key value
Symmetric Key Cipher	High speed operation of AES and DES symmetric key cipher
Public-Key Cipher	High speed operation of RSA and EC public-key cipher
TRNG	Generate True Random Number
IO I/F	Communicate with IO interface

Fig. 10.5 The components implemented in the security LSI

$d_i = 0$, then only the square is carried out. Therefore, the operation time or operation power reflect the binary key d. Such a property has been exploited in the simple power analysis, which is one of the side-channel attacks, or the fault injection attack.

(c) Other components embedded in security LSI

In order to implement a security LSI, we need other components such as CPU, non-volatile memory, program ROM and data RAM in addition to the cryptographic circuits. A true random number generator (TRNG) is also indispensable to many cryptographic protocols. These components are connected together by an internal bus interface as shown in Fig. 10.5.

All components of a security LSI have to be designed against tampering, because the security level of the chip is determined by the weakest component. Top-down design on the whole security system is needed in addition to develop secure components.

10.1.4 Certification of the Security Module

Any security LSI needs to be certified with respect to a certain security standard to let the chip users know what security characteristics it is guaranteed to exhibit. The current certification system is described in this section.

ISO/IEC 15408 [16], which is called CC (Common Criteria), is an international standard for computer security certification. Several security certification systems had been employed in the US and Europe from early 1990s, CC was established by unifying these old standards, so that security product venders would only need to have their modules evaluated in one standard. By evaluation, the confidentiality, integrity and availability are tested if they are protected against accidental faults and malicious attacks. In certification, a vender claims a protection profile (PP) for a product. A certified testing laboratory evaluates the products to check if it actually meets the claim.

Another security standard is FIPS-140-2 (Federal Information Processing Standard Publication 140-2) [17] which is an U.S. government computer security standard. The FIPS 140-2 standard provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. Security Level 1 provides the basic security requirements such as an approved cryptographic algorithm, and no specific physical security mechanisms are required. The physical security such as tamper-evident coating and seals are required in the Security Level 2. Further physical security mechanisms such as tamper detection and response are required at Security Level 3. Level 4 provides the highest level of security including the robustness against environmental conditions or fluctuations.

Its security requirements cover areas related to the secure design and implementation of a cryptographic module. These areas include (1) cryptographic module specification; (2) cryptographic module ports and interfaces; (3) roles, services, and authentication; (4) finite state model; (5) physical security; (6) operational environment; (7) cryptographic key management; (8) electromagnetic interference/electromagnetic compatibility (EMI/EMC); (9) self-tests; (10) design assurance; and (11) mitigation of other attacks. The Cryptographic Module Validation Program (CMVP) validates cryptographic modules according to FIPS-140-2.

The next FIPS 140-3 was proposed and drafted as the revision of FIPS 140-2 during 2007–2012. In the FIPS 140-3 draft, the mitigation of non-invasive attack including side-channel attack was required. For the most recent updates in FIPS-140-3, readers are referred to the websites of NIST [18].

10.2 Methods for Tampering Cryptographic VLSIs

Yohei Hori, National Institute of Advanced Industrial Science and Technology (AIST)

10.2.1 Categories of Attacks

In the previous section, we introduced examples of attacks in which secret data inside a cryptographic large-scale integrated circuit (LSI) were extracted by tampering with the physical chip. These examples show that secret information can leak even from a system that uses seemingly secure standard cipher algorithm, if it is not properly implemented on a physical device.

To better understand the methods of attacks against cryptographic hardware, it is useful to consider the four attack categories suggested by Anderson: *remote attacks*, *invasive attacks*, *semi-invasive attacks*, and *local non-invasive attacks* [19].

In this section, we briefly outline remote and invasive attacks, and then explain fault analysis attacks and side-channel attacks.

10.2.2 Remote Attacks

Typical remote attacks include cryptanalysis of cipher algorithms and protocol attacks. Cryptanalysis attacks aim at discovering algorithmic design flaws that can be exploited to extract secret information. Such attacks have proven successful in the past; the standard cryptographic algorithm Data Encryption Standard [20] (DES) has been broken by both differential cryptanalysis [21, 22], and linear cryptanalysis [23].

Protocol attacks, in contrast, inspect the transactions of a cryptographic system to find flaws in the encryption procedure, hash function, authentication, or other such things. Because such attacks do not require direct access to the cryptographic device, they can be launched via the Internet, and thus the attacker may not need to directly access the cryptographic device. Remote attacks are outside the scope of this paper, so we omit a detailed description of them, but interested readers are referred to [19].

10.2.3 Invasive Attacks

An invasive attack [19] physically accesses the internal circuitry of a cryptographic module to extract the secret information. This kind of attack typically requires direct wire-tapping of the signal wires by using a microprobe station or observing the state of memory cells with an electron microscope. An invasive attack is usually accompanied by some physical destruction of hardware, such as drilling of the passivation layers of the chip using a focused ion beam. Note that invasive attacks can be far more powerful than other methods of attack, but the attack cost is usually prohibitively high.

Invasive attacks can be prevented by using sensors that detect attempts to physically destroy the chip. For example, the secret information in the memory can be erased in the event that the top cover of the chip is removed or when a set of dummy mesh wires is removed.

10.2.4 Semi-invasive Attacks and Fault Analysis Attacks

Unlike invasive attacks, a semi-invasive attack accesses only the chip surface and does not destroy the chip layers. A semi-invasive attack is accompanied by moderate physical destruction, such as removal of the outer covering of the chip. For example, with the top cover of a chip removed, Skorobogatov and Anderson were able to perform a so-called optical attack [24] in which they irradiated the exposed chip surface with a camera flash and laser pointer and successfully flipped a bit in an SRAM cell. This demonstrates that the intended control flow of a cryptographic module, such as conditional branching to exclude an incorrect input, could be altered, allowing wrongful authentication of an attacker.

A fault analysis attack exploits the erroneous values of a cryptographic module to guess the secret key. The error is intentionally caused by injecting a clock glitch [25], by supplying abnormal voltage [26], or irradiating key surfaces with a laser [24]. Some fault analysis attacks require depackaging of the chip to irradiate its surface with a laser or electromagnetic beam. Such attacks are categorized as semi-invasive attacks. Other fault analysis attacks that use clock glitches or an abnormal supply voltage do not require depackaging, and they can be considered as non-invasive attacks.

10.2.5 Side-Channel Attacks

The main concern of this literature is non-invasive attacks, and particularly side-channel attacks (SCAs) [27], which are a growing threat to a wide range of cryptographic systems.

SCA is a collective term for various non-invasive attacks that exploit side-channel information such as the power consumption, electromagnetic radiation, and processing time of a cryptographic module. Even when the implementation of a cryptographic algorithm is certified to be computationally secure, the secret information (e.g., a secret key) inside the cryptographic module may be vulnerable to extraction by SCA. Note that SCA can be quite powerful, yet it can be carried out with inexpensive equipment, such as a digital storage oscilloscope and a personal computer. For this reason, SCA has been recognized as a serious problem by researchers in both industry and academia.

SCAs that exploit power, electromagnetic radiation, or computation time are known, respectively, as power analysis (PA), electromagnetic analysis (EMA) [28, 29], and timing analysis attacks. PA can be further subcategorized according to the analysis algorithm into types such as simple power analysis (SPA) [30], differential power analysis (DPA) [30], correlation power analysis (CPA) [31], and mutual information analysis (MIA) [32]. Similarly, EMA can be subcategorized into differential electromagnetic analysis (DEMA), correlation electromagnetic analysis (CEMA), and so on.

Several of these subcategories are detailed in the sections that follow.

10.2.5.1 Timing Analysis Attack

Timing analysis attack (TA) was the first side-channel analysis attack proposed by Kocher in 1996 [33]. TA can be applicable to cryptographic algorithms whose computational time varies depending on the secret. Suppose there is an algorithm where a subroutine A is executed when a certain secret bit is 0 and B is executed when the bit is 1. If the computation time of A and B are different, we can know if the secret bit is 0 or 1 by observing the computation time.

10.2.5.2 SPA

SPA is an attack that interprets the shape of a power trace of the cryptographic module to obtain the secret information. If a computation causes power consumption different according to the state of a specific secret bit, then the shape of the power trace visually represents the value of the secret bit. One computation of the type vulnerable to SPA is modular exponentiation, which is performed in many cryptographic algorithms.

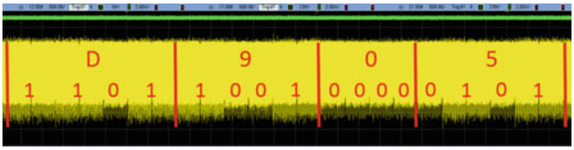
RSA [34], one of the most popular public-key cryptography systems, uses modular exponentiation for encryption and decryption. Algorithm 1 shows the procedure for performing modular exponentiation, $Z = X^E \bmod N$, in RSA using the left-to-right method. Note that Z is multiplied by X only if the key bit e_i is 1, and that Z is always squared independently of the key bit. Consequently the power consumption of the chip for $e_i = 1$ and $e_i = 0$ will be clearly distinguishable from a power trace, allowing an attacker to deduce the secret key.

Algorithm 1: Modular exponentiation calculation using the left-to-right binary method.

```
input : $X, N, E$
output: $Z = X^E \bmod N$
$Z \leftarrow 1$;
for $i = k - 1$ downto 0 do
    $Z \leftarrow Z \times Z \bmod N$;
    if ($e_i = 1$) then
        $Z \leftarrow Z \times X \bmod N$;
    end
end
return $Z$;
```

Figure 10.6 shows an example of SPA used against an RSA cipher, where the shape of the power trace clearly indicates the secret key. The voltage fluctuation was observed during a 1024-bit RSA calculation using the experimental setup shown in Fig. 10.7. The RSA algorithm was implemented on a cryptographic LSI manufactured for test purposes using TSMC 130-nm cell libraries. The LSI was mounted on a board *SASEBO-RII* [35], which was controlled by a ZUIHO board equipped with

Fig. 10.6 Secret key extraction using SPA against RSA



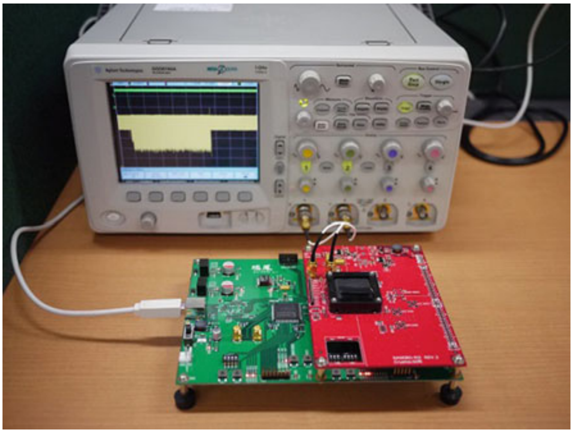


Fig. 10.7 Experimental setup for SPA

field-programmable gate array [36]. The voltage of the LSI was measured with an Agilent DSO 6104A oscilloscope and SMA cables. Figure 10.6 was obtained by using a low-pass filter with a cut-off frequency of 80 MHz. From the trace shown in Fig. 10.6, we can easily deduce (a part of) the secret key, "0xD905."

10.2.5.3 DPA

DPA was the first differential side-channel analysis attack, developed by Kocher et al. [30]. For many symmetric block cipher algorithms, a single power wave trace will not reveal any sensitive information, but DPA collects a large number of such traces during encryption and statistically analyzes them to guess the secret key. DPA uses the mean difference of the two groups of measured power traces as a statistic.

More specifically, an attacker uses an oscilloscope to collect the power traces of the cryptographic module as it encrypts large amounts of plaintext. The power traces are then divided into two groups according to the intermediate computational value of the specific encryption/decryption operation. Although this value is bound to the key, the attacker can never obtain it directly. Instead, the attacker tries all possible key values and calculates backward to the corresponding intermediate values. If the value is 0 under the hypothetical key $\hat{k}$, then the corresponding power trace is grouped under $W_{\hat{k}}^{0}$; if the value is 1, the power trace is grouped under $W_{\hat{k}}^{1}$.

Next, the mean difference $\Delta_{\hat{k}}$ of the two groups of wave traces under the hypothetical key $\hat{k}$ is calculated as follows:

$$\Delta_{\hat{k}_i} = \overline{W_{\hat{k}_i}^{0}} - \overline{W_{\hat{k}_i}^{1}} \tag{10.1}$$

where $\overline{W^0_{\hat{k}_i}}$ and $\overline{W^1_{\hat{k}_i}}$ are the mean of power traces in $W^0_{\hat{k}}$ and $W^1_{\hat{k}}$, respectively. The attacker then guesses that the actual key k is the hypothetical key $\hat{k}_i$ that makes $\Delta_{\hat{k}_i}$ largest:

$$k = \underset{\hat{k}_i}{\operatorname{argmax}} |\Delta_{\hat{k}_i}|. \tag{10.2}$$

For example, in 128-bit key AES, the number of the possible key values is 256 (=2^8) and not 2^{128}, even though the key length is 128 bits. This reduction is possible because power consumption is correlated with the partial intermediate value, allowing the attack to focus on the 8-bit partial key instead of the full-length key.

10.2.5.4 CPA

CPA exploits the correlation between the intermediate values of a cryptographic module and its power traces. In particular, CPA uses Pearson's correlation coefficient, a statistic representing the strength of the linear correlation between two random variables.

As with DPA, an attacker collects power traces W of the cryptographic module during the encryption process. The attacker also calculates hypothetical power consumption $H_{\hat{k}}$ under a hypothetical key $\hat{k}$. $H_{\hat{k}}$ can be the Hamming weight or Hamming distance of the intermediate value, and may, in some cases, be the intermediate value itself. The correlation coefficient $\rho_{\hat{k}}$ under the hypothetical key $\hat{k}$ is obtained as follows.

$$\rho_{\hat{k}} = \frac{\sum_n (W_n - \overline{W})(H_{n,\hat{k}} - \overline{H_{\hat{k}}})}{\sqrt{\sum_n (W_n - \overline{W})^2}\sqrt{\sum_n (H_{n,\hat{k}} - \overline{H_{\hat{k}}})^2}} \tag{10.3}$$

The attacker then guesses that the actual key k is the hypothetical key $\hat{k}_i$ that makes $\rho_{\hat{k}_i}$ largest:

$$k = \underset{\hat{k}_i}{\operatorname{argmax}} |\rho_{\hat{k}_i}|. \tag{10.4}$$

10.2.5.5 MIA

Mutual information indicates linear and nonlinear correlation of two random variables, whereas Pearson's correlation coefficient indicates only the linear correlation. Therefore, MIA yields a more powerful attack against certain kinds of cryptographic modules.

MIA exploits the mutual information of the hypothetical intermediate values and the power (or electromagnetic) traces of the cryptographic module. Let W_j and $H_{\hat{k}}$ be the power traces and intermediate values, respectively, under a hypothetical key $\hat{k}$, the mutual information $I(W; H_k)$ can be calculated as follows:

$$\begin{aligned} I(W; H_{\hat{k}}) &= H(W) - H(W|H_{\hat{k}}) \\ &= -\sum_n \Pr(W_n) \log_2 Pr(W_n) + \sum_{H_{\hat{k}}} \Pr(H_{\hat{k}}) \sum_n \Pr(W_n|H_{\hat{k}}) \log_2 \Pr(W_n|H_{\hat{k}}). \end{aligned} \tag{10.5}$$

The attacker then guesses that the actual key k is the hypothetical key $\hat{k}_i$ that makes $I(W; H_{\hat{k}})$ largest:

$$k = \underset{\hat{k}_i}{\operatorname{argmax}}\, I(W; H_{\hat{k}}). \tag{10.6}$$

Since $H(W)$ is constant for any $H_{\hat{k}}$,

$$\begin{aligned} k &= \underset{\hat{k}_i}{\operatorname{argmin}}\, H(W|H_{\hat{k}}) \\ &= \underset{\hat{k}_i}{\operatorname{argmax}} \sum_{H_{\hat{k}}} \Pr(H_{\hat{k}}) \sum_n \Pr(W_n|H_{\hat{k}}) \log_2 \Pr(W_n|H_{\hat{k}}). \end{aligned} \tag{10.7}$$

10.2.5.6 Scan-Based Attacks

Many newer LSIs have an internal boundary scan chain for testing and debugging of the chip at fabrication and in the field. By using this scan chain, a manufacturer or user can easily monitor flip-flops that encode various types of information, such as the status of the control flags and the intermediate computational values. The monitored flip-flops are sequentially connected and shifted in/out for writing/reading through a JTAG[1] interface.

A scan-based attack [37] exploits the scan chain to analyze confidential information inside the cryptographic chip. Even if the scan chain is not directly connected to the secret, that information can be guessed from the monitored intermediate values. The detailed attack methods are discussed in Sect. 10.5 and the literature [38].

[1] Joint Test Action Group

10.3 Tamper-Resistant Symmetric-Key Cryptographic Circuits

Mitsuru Shiozaki, Ritsumeikan University

Takeshi Fujino, Ritsumeikan University

Masaya Yoshikawa, Meijo University

10.3.1 Side-Channel Attacks on Symmetric Cipher Circuit

In recent years, cryptographic circuits have become essential to the security of embedded systems. The designer of the cryptographic circuits therefore needs to pay enough attention to the threat of possible leakage of information relating to the secret key due to side-channel attacks, which attempt to reveal it by measuring power consumption or electromagnetic radiation during the circuit operation. This section begins with a quick review of the side-channel attacks (SCAs) as illustrated in an experimental setup of Fig. 10.8, and then elaborates on a few effective ways of reducing the risks of SCAs.

The power analysis (PA) attack that exploits the power consumption characteristics of devices is well-known among the SCAs. The famous PA attacks are the differential power analysis (DPA) attack described by Kocher et al. in 1999 [30] and the correlation power analysis (CPA) attack described by Brier et al. in 2004 [31]. In a CPA attack, the correlation coefficients between the intermediate values of the cryptographic circuit and measured power traces are calculated to reveal the secret key. The CPA attack requires fewer traces than the DPA attacks to reveal the secret key, and thus the CPA attack is regarded as more significant. Other than the above,

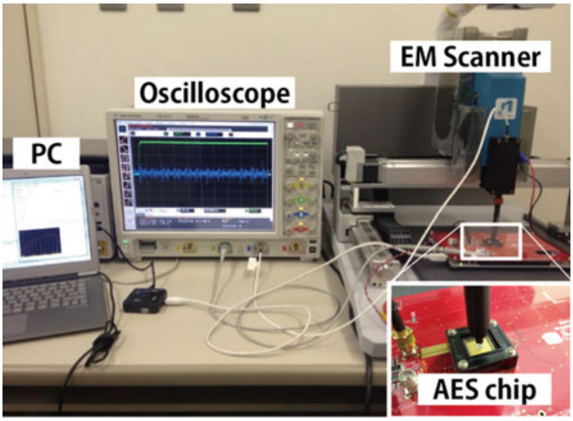


Fig. 10.8 The side-channel attack equipment utilizing electromagnetic analysis

Zero-Value DPA [39], Zero-Offset DPA [40], Mutual Information Analysis (MIA) [41], Template Attack [42] are also well-known.

Electromagnetic analysis (EMA) attacks [29, 43] have also begun attracting more attention. The EMA attacks are side-channel attacks that exploit the electromagnetic radiation of devices. Like CPA attacks, the correlation electromagnetic analysis (CEMA) attacks calculate the correlation coefficients between intermediate values and electromagnetic traces.

The leak model of these attacks is classified into two main models [44]. The Hamming-weight model looks at the input values of the nonlinear logic gate (such as AND/OR gate) as an indication of the secret key, since the output transition of the nonlinear logic gate is biased by the inputs. The Hamming-distance model watches the number of transitions between the registers to reveal the secret key. It is noted that the transition of registers between every round in loop architecture are linked to the cryptographic key values. Thus, the designer needs to pay attention to all the combinations of the attack method, the leak source (PA/EMA), the leak model.

10.3.2 The Effect of Decoupling Capacitor on Side-Channel Attacks

A simple way of reducing PA leaks is inserting decoupling capacitors into the printed board [45], but exactly effective it is for improving the vulnerability to EMA leaks has never been unknown. Thus, we fabricated advanced encryption standard (AES) [46] cryptographic chips with and without on-chip decoupling capacitors. Each was subjected to a test for resistance against PA and EMA attack, and the results were compared for the first time [47].

Firstly, the results of the CPA attack on the AES cryptographic chip without on-chip decoupling capacitors are shown in Fig. 10.9a. These results indicate the relationship between the number of revealed key bytes (max 16 bytes) and the number of the measured power traces. All secret keys (16 bytes) of AES without on-chip decoupling capacitors were easily revealed within 1,000 traces by HD (Hamming Distance)-CPA attack (solid line in Fig. 10.9a). HW (Hamming Weight)-CPA attack revealed all secret keys with approximately 10,000 traces (dashed line in Fig. 10.9a). Meanwhile, inserting decoupling capacitors increased the number of traces needed to reveal the secret key and reduced the risk of PA leakage. Figure 10.9b shows CPA attack results on the AES with on-chip decoupling capacitors. The number of secret keys revealed with 10,000 traces by CPA attacks in either HD or HW methods was reduced below half compared to the case of chips without decoupling capacitors. The on-chip decoupling capacitors have thus proven to enhance PA resistance since the voltage spike is averaged owing to its capacitors.

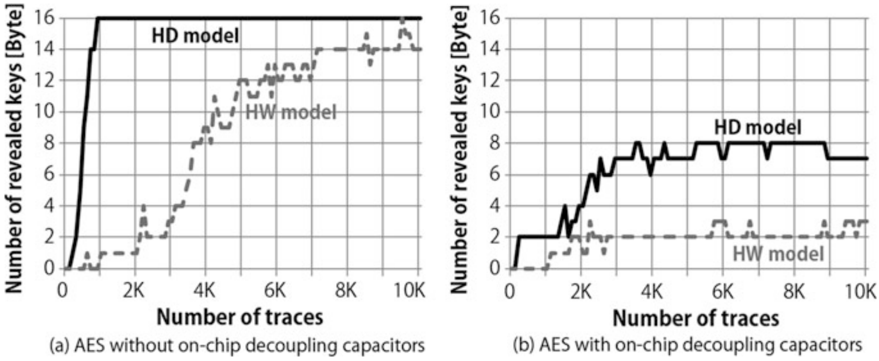


Fig. 10.9 CPA results on AES with/without on-chip decoupling capacitors

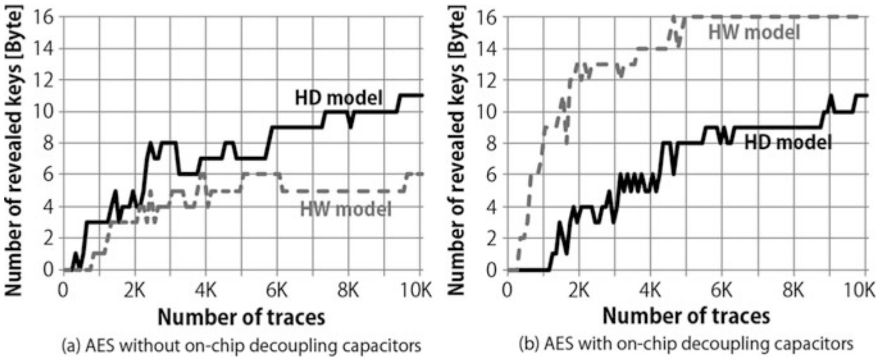


Fig. 10.10 CEMA results on AES with on-chip decoupling capacitors

Next, EMA attack results on AES with/without on-chip decoupling capacitors are shown in Fig. 10.10. In the measurement, a horizontal magnetic-field probe was placed in the center of the chip and placed as close as possible to the chip surface. Figure 10.10a shows CEMA attack results on the AES without on-chip decoupling capacitors. HD-CEMA and HW-CEMA attacks revealed 11 and 6 bytes of secret key, respectively. When decoupling capacitors are inserted into the AES cryptographic circuit, the revealed secret key increased, as shown in Fig. 10.10b. All secret keys were revealed within 5,000 traces by HW-CEMA attack. The insertion of the on-chip decoupling capacitor emphasizes the signal transition and makes ineffective against EMA attacks. Thus, an LSI designer has to pay attention to inserting the decoupling capacitors.

10.3.3 Typical Countermeasure Schemes

Various countermeasures have been studied so far to tighten the security circuit against leakage of keys (Table 10.2). They are classified into the hiding technique and the masking technique, and are implemented either at the algorithm level, cell level or gate level. The famous countermeasures are Wave Dynamic Differential Logic (WDDL) [48], Masked-AND Operation (MAO) [49], Masked Dual-rail Precharge Logic (MDPL) [50], and Random Switching Logic (RSL) [51], and Threshold Implementation (TI) [52].

10.3.4 Countermeasure Using IO-Masked Dual-Rail ROM

The authors have proposed (and implemented) the IO-Masked Dual-Rail ROM (MDR-ROM) circuit [54] in order to achieve a small-area and low-power symmetric cipher circuit against side-channel attacks. A block diagram of AES encryption with MDR-ROM is shown in Fig. 10.11. The random numbers, generated for every new loop, are used as an additive mask to the intermediate value. ShiftRows, MixColumns, and AddRoundKey operations are performed using the

Table 10.2 Typical countermeasure schemes

Name	
WDDL	WDDL is a cell-level countermeasure using hiding technique. A dual-rail precharge logic, which consists of a pair of positive and negative gates, is applied to make total gate switching constant. However, a small difference of power consumptions between the positive and negative gates leaks secret information, because it is very difficult to eliminate the output-load imbalance in the standard CAD tools
MAO	MAO is a gate-level countermeasure using masking technique. Intermediate values are randomized using combination logic blocks. The leakage of secret information is caused by the signal delay variations in combination logic gates
MDPL	MDPL is a cell-level countermeasure using both hiding and masking techniques, and combines the idea of WDDL and random switching logic to randomize power consumption on a cryptographic device. However, it has been reported that the leakage of secret information on the MDPL occurs because of the "early propagation effect [53]"
RSL	RSL is a cell-level countermeasure using the masking technique, and applies majority decision logic gates with switching transistor in order to adjust operation timing. A cryptographic circuit using RSL scheme has sufficient side-channel resistance. However, the asynchronous clock timing design is required to eliminate information leakages
TI	TI is an algorithm-level countermeasure using the masking technique based on Shamir's secret sharing. The circuit area and power consumption of TI increases several times larger than that of non-countermeasure circuit

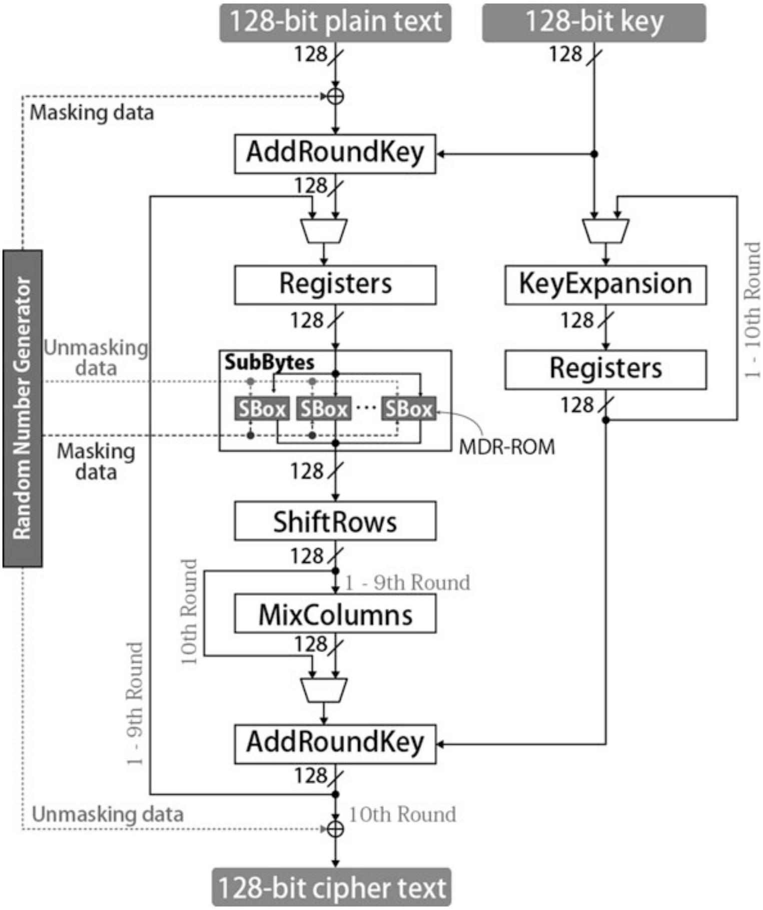


Fig. 10.11 Block diagram of AES encryption with MDR-ROM countermeasure

masked data, to have the intermediate values protected against side-channel attack. The SubByte transformation cannot be performed on the additive masked data, because the data requires non-liner calculations. In this proposal, the SubByte transformation is performed using MDR-ROM, on which the masked intermediate data is un-masked at the entrance of the ROM and the data is re-masked again at the exit.

A dual-rail precharge logic is applied in the ROM in order to protect SubByte transformation against PA/EMA attacks. Figure 10.12 shows the circuit diagram of the MDR-ROM. The masked input data is converted into dual-rail logic by a domino XOR gate pair. Because the dual-rail logic consumes constant power regardless of input values, the dual-rail logic can hide intermediate values from PA/EMA attacks using an HW model. In addition, the domino XOR gate is the precharge logic and is precharged by the clock signal, so that the data correlations

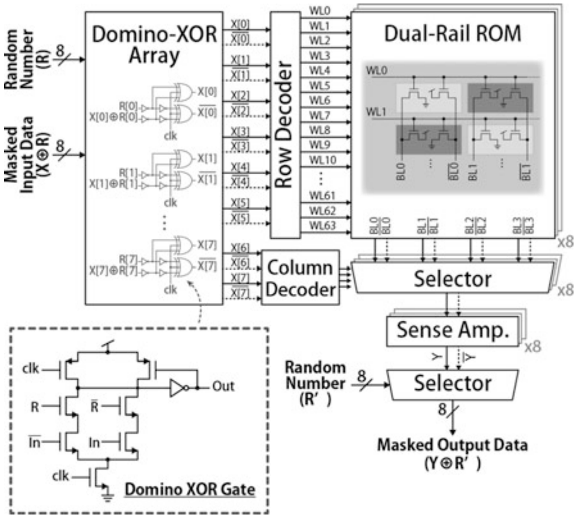


Fig. 10.12 Basic circuit diagram of MDR-ROM

between AES round operations are separated during the precharge phase. Thus, intermediate values are better protected from PA/EMA attacks using an HD model. The row and column addresses are decoded to drive only one word-line selected by dual logic values. It is to be noted that the power consumption of decoders is independent of the input value. Single-end read bit-lines are widely used in the ROM. Here, however, the double-end bit-lines are adopted in order to avoid PA/EMA attacks. Thus, the transformed data is derived from the dual-rail ROM with NMOS transistor pairs. The column decoder selects the bit-line pairs, and connects the ROM cell to the sense amplifier circuit. The output data is selected by output random number in order to randomize the side-channel information.

10.3.5 Countermeasure Using Spreading Clock Scheme

A clock-based countermeasure using the spreading clock scheme has been proposed by the authors [55], in which the clock frequency and skew are continuously varied. Since the side-channel attacks are a statistical analysis, an attacker needs to know the timing of information leakage, such as transition timing of registers. The proposed spreading clock scheme hides time information of cryptographic processing. The circuit with proposed scheme consists of a variable frequency oscillator and a variable skew generator, as shown in Fig. 10.13. The variable frequency oscillator can be switched among clocks with various frequencies. The variable skew generator changes the clock skew of respective registers. Figure 10.14a shows the correlation between cipher texts and power traces on the non-countermeasure AES.

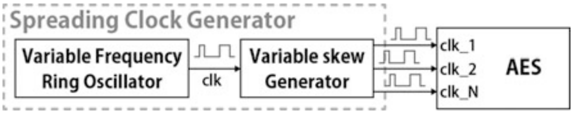


Fig. 10.13 A countermeasure circuit using the spreading clock scheme

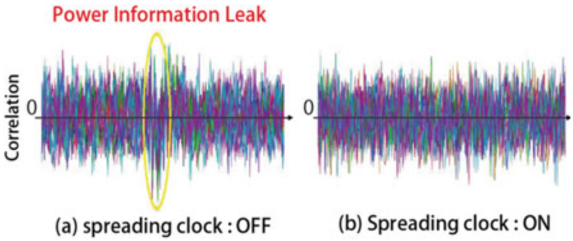


Fig. 10.14 Effectiveness of the spreading clock scheme

The correlation peak appears at the leak position of secret information. On the other hand, the AES circuit built with the spread clock of Fig. 10.13 showed no apparent correlation peaks as demonstrated in Fig. 10.14b, and proved to be more robust against PA attacks.

10.3.6 Comparison of Countermeasures

Figure 10.15 compares the circuit area and power consumption for various circuits with and without countermeasures against PA attacks: (non-countermeasure AES using an S-Box look-up table (TBL AES), WDDL AES, MAO AES, MDPL AES, TI AES and MDR-ROM AES). These results are normalized by the circuit area and power consumption of the non-countermeasure AES. The increase of the circuit

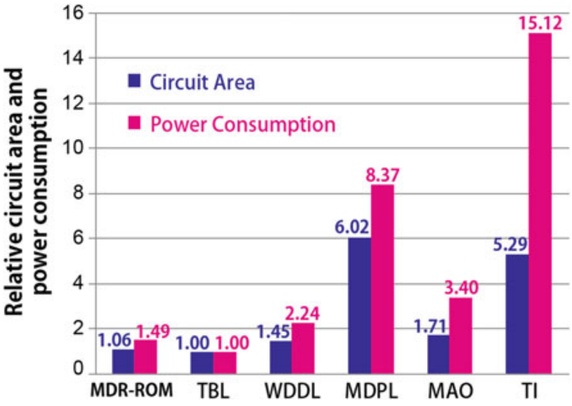
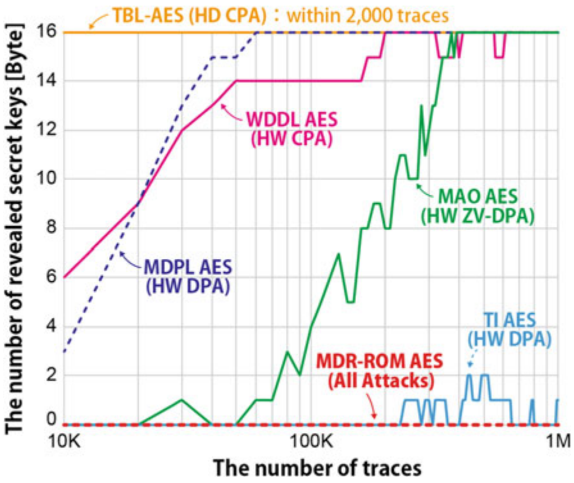


Fig. 10.15 Comparison of the power consumption and circuit area for various AES circuits

Fig. 10.16 PA/EMA attack results



area and power consumption is very large in the MDPL and TI schemes. Smaller circuit area and lower power consumption have been achieved in the MDR-ROM AES compared with other countermeasures.

Evaluation results on the resistance against HW-/HD-CPA, HW-/HD-CEMA, HW-/HD-DPA, Zero-Value (ZV) DPA, and Zero-Offset (ZO) DPA attacks are summarized in Fig. 10.16. The revealed key curves are plotted by the most powerful attacking method, by which the largest number of keys are revealed with the fewest traces. All the secret keys on the WDDL AES, MAO AES and MDPL AES were revealed within a half million traces. It is noted that the dedicated layout techniques for dual-rail wiring are not applied with WDDL and MDPL. The MDR-ROM AES and TI AES required over 1 million traces to disclose secret key, and had sufficient resistance against side-channel attacks. These results have demonstrated that the MDR-ROM AES can be implemented in a small chip area and low power consumption, with strong resistance against side-channel attacks. The countermeasure using spreading clock scheme can be combined with MDR-ROM scheme for additional side-channel resistance.

10.4 Verification Method for Tamper-Resistant VLSI Design

Masaya Yoshikawa, Meijo University
Toshiya Asai, Meijo University

10.4.1 Problems in the Flow for Designing a Tamper-Resistant Large-Scale Integrated Circuit

It is very important to verify the design of a security LSI for tamper resistance before it is put into production. Circuit simulation is an indispensable tool for analyzing the vulnerability of the chip for power analysis (PA) attacks, and assessing fault injection due to fault attacks as well. In this section, we will discuss the accuracy and computation time of such simulations, factors that are critical for effective analysis of tamper resistance. It is attempted to build a platform for tamper-resistance verification based on circuit simulations at the physical level and vulnerability analyses at a higher level.

Table 10.3 shows the problems encountered in tamper-resistance verification during the design of an LSI and the solutions to these problems. These measures feature the use of a platform for tamper-resistance verification. Power consumption waveforms must be scrutinized for possible exploitation for secret keys and the relationship between the obtained fault patterns and the possibility of fault attacks must be effectively determined.

10.4.2 Platform for Tamper-Resistance Verification

10.4.2.1 High-Speed Power Consumption Simulator

Previously, power consumption waveforms were acquired by performing multiple encryption simulations that use an LSI design tool from an EDA vendor. It enabled, in principle, designers to verify the tamper resistance of an LSI against power analysis attacks at the design stage. However, the computation time needed to obtain accurate power traces in the conventional method was too long, making it difficult to complete verification within a realistic timeframe. As a high-precision

Table 10.3 Problems and solutions in tamper resistance verification

	Problem	Countermeasure
Power analysis attack	The simulation of power consumption waveforms is encumbered by a slow processing time and is inaccurate	High-precision and high-speed simulation should be implemented using event models [56, 57]
	The cause of vulnerability that facilitates successful attacks is difficult to be revealed	Vulnerability should be evaluated by multiple linear regression [58] or clustering [59]
Fault attack	The relationship between fault patterns and the possibility of attacks is uncertain	A fault simulator that can handle multiple errors should be developed [60]

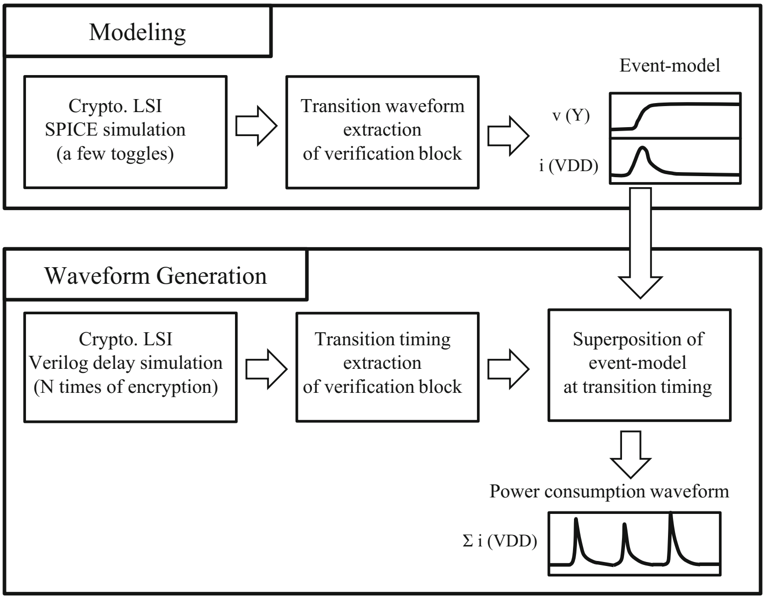

Modeling
Crypto. LSI SPICE simulation (a few toggles)
Transition waveform extraction of verification block
Event-model
v (Y)
i (VDD)
Waveform Generation
Crypto. LSI Verilog delay simulation (N times of encryption)
Transition timing extraction of verification block
Superposition of event-model at transition timing
Power consumption waveform
Σ i (VDD)

Fig. 10.17 Procedure of event-model simulation

and high-speed approach to acquiring power consumption waveforms, event-model-simulation, that is specifically designed to acquire encrypted waveforms, has been proposed by the authors [56, 57]. This method features (1) a modeling process and (2) a process of generating encrypted waveforms. Figure 10.17 illustrates these processes.

In the modeling process, the output transition waveform and the current consumption waveform (i.e., a waveform pair) in each cell of the circuit to be verified are extracted using SPICE. Current consumption waveforms that occur upon rise transition and fall transition are prepared as event models. In the process of generating encrypted waveforms, the transition time of each cell of the circuit is obtained using a delay simulation of Verilog. With the information about the transition time and the above-mentioned event models, the event models are superposed at each transition time and current consumption waveforms are generated. The advantages of the event model simulation are as follows:

- Compared with SPICE simulation, the event model simulation features a considerably higher processing speed but slightly lower accuracy.
- The switching conditions of each cell in the circuit to be verified can be obtained.
- Through the selective generation of waveforms near the attack time, high-speed processing can be achieved and data volume can be reduced.

A method that shortens the processing time spent in power consumption simulation has been proposed [61]. In this method, the power consumption simulations

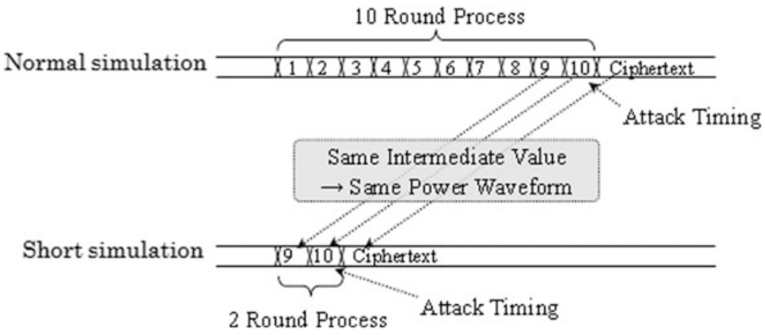


Fig. 10.18 Shortened simulation of AES encryption

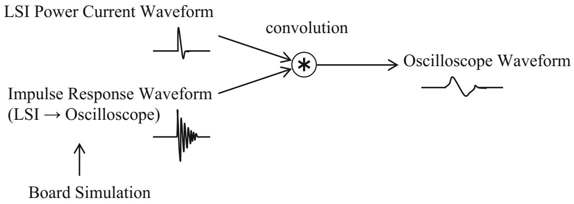
at rounds that are unnecessary for attacks are eliminated, and only the power consumption waveforms at rounds to be attacked are reproduced. This method is called a short simulation. By slightly changing the net list generated during LSI development, the short simulation can be performed (Fig. 10.18).

In the short simulation, the cryptographic intermediate value when the circuit is activated with short operations becomes identical to that when the circuit is activated with normal operations. For both cases, therefore, the power consumption waveforms at the attack time are the same.

In the evaluation of the resistance against power analysis attacks, the circuit elements in the power supply system-related elements, which are indispensable for observation of the waveforms, must be included for analysis. For this purpose, a method of modeling a board and a power supply system located between the LSI under test and the observation system has been proposed [62]. Figure 10.19 shows the outline of the modeling method.

In the method, the impulse response waveform that carries out transmission from an LSI to an observation system is obtained by conducting a circuit simulation at the board level. The waveform actually observed is then estimated by convoluting the impulse response waveform and the LSI's current consumption waveform simulated separately. In this method, the accuracy of the observation waveform depends on the accuracy of the board simulation in obtaining the impulse response waveform. The board simulation uses a model, into which the power source patterns of boards and elements such as capacitors for power supply systems are

Fig. 10.19 Estimation of observed waveform

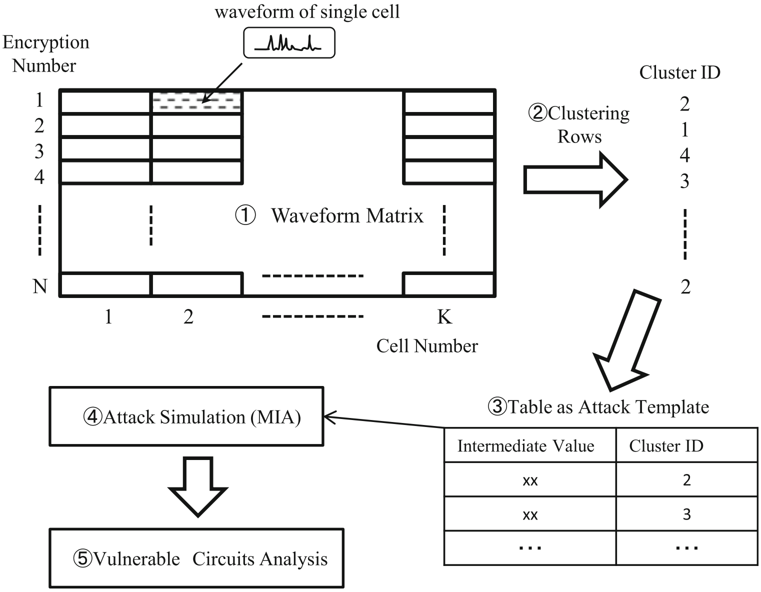


incorporated. If boards that possess similar power supply system exist, the transmission characteristics can be obtained using a network analyzer.

10.4.2.2 Quantitative Evaluation of Tamper Resistance

Previously, the results of simulations as described in the previous subsection were used to produce only a qualitative judgment with regard to the vulnerability of the circuit under verification. More recent trend is trying to come up with more quantitative evaluation regarding the amount of information the chip would release under an attack and the identification of the exact part of the circuit that is responsible for the leakage (vulnerable point). The authors have introduced, (1) clustering method for semi-custom designs [59], and (2) multiple linear regression analysis is used for intellectual property (IP)-based designs [58].

Figure 10.20 outlines the clustering method. (1) First, the current waveform data of all cells are summarized in the form of a waveform matrix. (2) With nonnegative matrix factorization, clustering is then performed for the patterns of each row in the cell waveform matrix. (3) As the result of clustering, one cluster ID is assigned to each row at every round of encryption processing. That is, all the obtained current waveforms are classified into several clusters. Here, clustering uses the current waveform of each cell instead of the current waveform of the entire verification circuit. The location of the used cell is therefore reflected in the clustering results. (4) On the basis of the clustering results and the cryptographic intermediate value, a



Intermediate Value	Cluster ID
xx	2
xx	3
…	…

Fig. 10.20 Clustering method

correspondence table is created. Mutual information analysis [32] is performed using this table. If the period at which an attack succeeded is recorded, a circuit that operated at the time can be identified using the data of the cell waveform matrix, and the cause of vulnerability can be analyzed.

Evaluating vulnerability by multiple linear regression analysis involves the use of power consumption as the objective variable and the intermediate values in the verification module as the explanatory variables. Although the value used as the intermediate value can be arbitrarily determined, Hamming distance or weight is generally used. Figure 10.21 illustrates multiple linear regression analysis. As shown in the figure, the partial regression coefficient in the regression equation is the numerical value that expresses the correlation between each explanatory variable and the objective variable.

With the coefficient of determination and the partial regression coefficient in the regression analysis, the resistance against power analysis attacks is evaluated. The time at which the partial regression coefficient of a certain explanatory variable increases can be used to identify a vulnerable block. Evaluating the reliability of a coefficient by a t-test enables researchers to assess whether the number of waveforms used in evaluating vulnerability is sufficient.

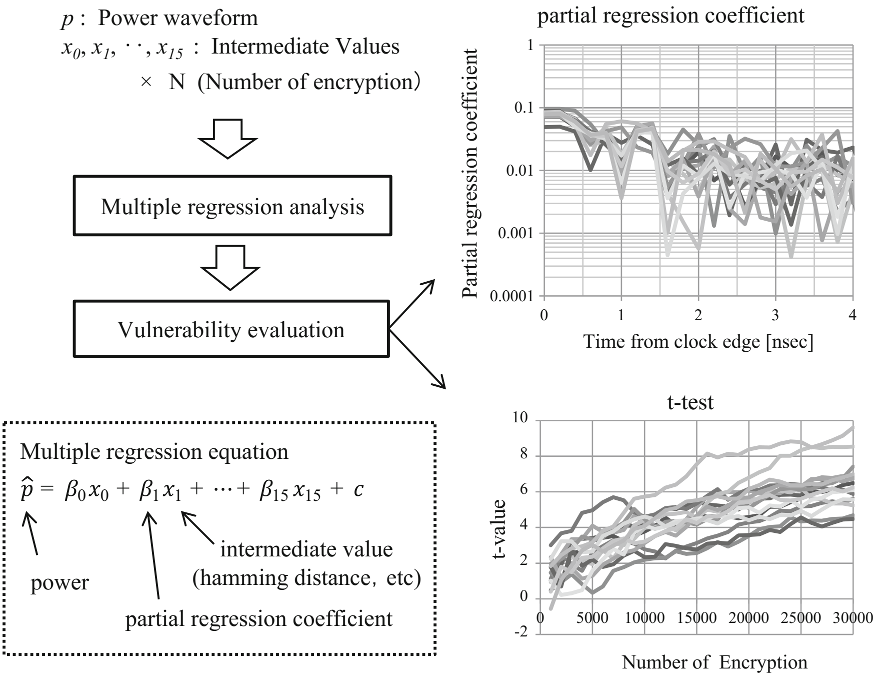

p : Power waveform
$x_0, x_1, \cdot\cdot, x_{15}$: Intermediate Values
× N (Number of encryption)
Multiple regression analysis
Vulnerability evaluation
Multiple regression equation
$\hat{p} = \beta_0 x_0 + \beta_1 x_1 + \cdots + \beta_{15} x_{15} + c$
power
partial regression coefficient
intermediate value
(hamming distance, etc)
partial regression coefficient
Partial regression coefficient
1
0.1
0.01
0.001
0.0001
0
1
2
3
4
Time from clock edge [nsec]
t-test
t-value
10
8
6
4
2
0
-2
0
5000
10000
15000
20000
25000
30000
Number of Encryption

Fig. 10.21 Multiple linear regression analysis

10.4.2.3 Methods for Verifying Resistance Against Fault Attacks

In earlier analyses of fault attacks, simplest fault models have been applied to the particular circuit block under attention. In real fault attacks, voltage spikes or illegal clocks applied to the cryptographic circuit could result in multiple errors in multiple locations are difficult to predict because the entire current-supply circuit is being subject to fault generation. Therefore, analyzing the security of a secret key is not straightforward.

A method that performs analysis even when multiple errors simultaneously occur has recently been proposed by authors [60]. In the AES, many processes are performed every state, and the processing time of each state differs from each other due to signal propagation delay. In each state, the delay time differs from each other in bit unit due to wiring delay. The delay characterization was utilized for the fault analysis. This method estimates the types of errors from the results obtained by encryption processing when errors occur. On the basis of the estimation results, this method narrows multiple secret key candidates down to one secret key. Similar to actual attackers, this method can perform analysis even when detailed information about error location (bit position) and a circuit is unavailable.

10.5 A Method for Evaluating Vulnerability to Scan-Based Attacks

Masayoshi Yoshimura, Kyoto Sangyo University

10.5.1 Outline of Scan-Based Attacks

One of the types of malicious attacks on security LSIs is an attack that takes advantage of subsidiary functions. One of such attack type is scan-based attack. This section describes the procedure against scan-based attack, countermeasures of scan-based attack and evaluation methods for the countermeasures.

Scan design [63] is among the frequently used methods of design-for-testability that help to reduce manufacturing test time and improve manufacturing test quality. It provides the means to directly observe values of all or a part of memory elements in an LSI. It also provides the means to directly control any values of all or a part of memory elements in an LSI.

Scan design is realized by replacing flip-flops (FFs) by scan flip-flops (SFFs [63]) and connecting them to form scan registers in test mode. A scan chain consists of SFFs, a scan enable signal, a scan-in pin, and a scan-out pin as shown in Fig. 10.22. In Fig. 10.22, when the scan enable signal is high, the circuit is in the

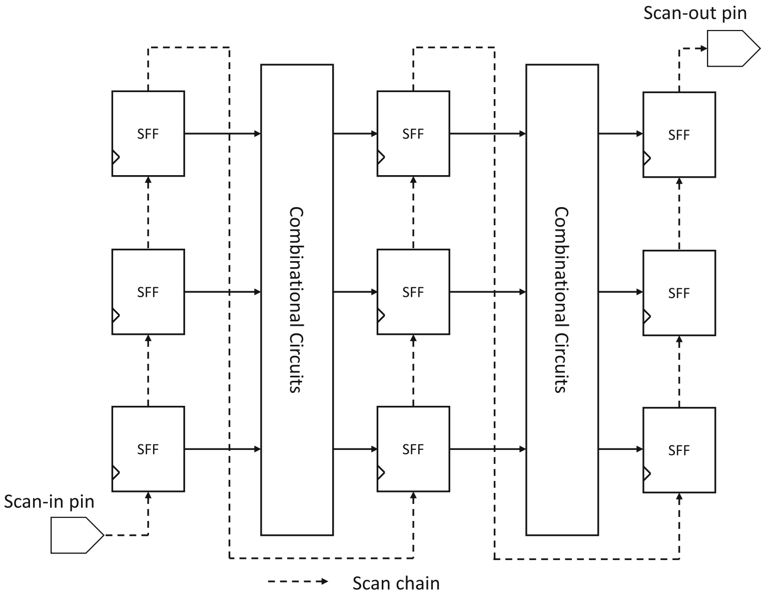


Fig. 10.22 Scan chain structure

test mode. During the test mode or the shift mode, as it is called alternatively, the values of SFFs can be read out and can be modified as well through scan chains.

It should be obvious now that there is a conflict between scan design and security. Attackers can use scan chains as a tool to observe and/or modify the values of SFFs to get a hand on the sensitive data on the security LSI. A simple countermeasure is to eliminate SFFs which contain sensitive data from SFFs and to apply other DFT methods to complement the testability of the security LSI.

Such attack method exploiting the scan design called the scan-based attack. Yang et al. have proposed effective attack methods against a DES hardware implementation [64] and an AES hardware implementation [65]. These attack methods were based on following few assumptions. The first one is that the sensitive data cannot be directly obtained from the values of SFFs. The second one is that the attacker can calculate sensitive data from indirect data. The third one is that the attacker has no information about the structure of scan chains of the security LSI. The attack method consists of three steps. The first step is to determine the structure of scan chains in a security LSI. Intermediate results after the first round are stored in the registers on scan chains. The attacker can obtain the intermediate results through scan chains and identify different values in two intermediate results correspond to the SFFs. The second step is to calculate the first round key from the scan chain structure and the intermediate results. The third step is to identify the secret key by three round keys. It has been reported that the attack method is effective to other ciphers [66, 67].

10.5.2 Countermeasures Against Scan-Based Attacks

Countermeasures against scan-based attacks have been proposed over the years, and can be classified into three types. The first type of countermeasures (type I) is to restricting utilizations of scan chains. Although its security is highest. Type I suffers from the disadvantage in testability [65, 68]. The second type of countermeasures (type II) is to replace the values in scan chains with other, converted, values [69–71]. The attacker can obtain only the converted data and yet have no information about the converting algorithms. Therefore, it is difficult with the attacker to analyze the structure of scan chains and calculate the first round key. In type II, the quantity of information of values in scan chains is equal to information quantity of the secret key. The designer obviously knows how to convert the values in scan chains into other values. The designer can convert the other values back into the values in scan chains. The testability of type II is the same with that of normal scan designs. However, type II also suffers from a disadvantage in security because the attacker can learn that the security LSI includes a circuit to convert values of scan chains into other values. They might motivate the attacker to employ additional means to pry into the chip. The third type of countermeasures (type III) is the values in scan chains in the security LSI. The security and testability of type III countermeasure depend on the number of bits of the output values. When the number of bits of output values is large, security is low, and testability is high. Most typical type III countermeasures utilize MISR (Multiple Input Shift Register) circuits to descramble values in scan chains.

10.5.3 A Method for Evaluating Vulnerability to Scan-Based Attacks

Countermeasures against scan-based attacks have a trade-off between area, power, testability and security, while there are metrics for the area, power, and testability commonly applicable to security LSIs over different types of countermeasures. Quantitative measures of security, on the other hand, have still been debated. Ito et al. have proposed a criterion for security and proposed an evaluation method [72] with a mutual information applicable for all countermeasures against scan-based attacks. In this criterion, mutual information is calculated based on all of the information except for the secret key and values of memory elements in security LSIs. All of the information includes structures of logic gates, scan chains, and circuits to compact values in scan chains. This mutual information is equal to the maximum of the quantity of information which an attacker can obtain when he/she revealed all of the information except for the secret key and values of memory elements in the chip. This evaluation method calculates the mutual information between the secret key and output values of the chip. The designer can thus decide

Table 10.4 Parameters of DES circuits

Secret key (bit)	# of register (bit)	Output bits (m) (bit)	Function of MISR
48	32	m	$\{0,1\}^{32} \rightarrow \{0,1\}^{m}$

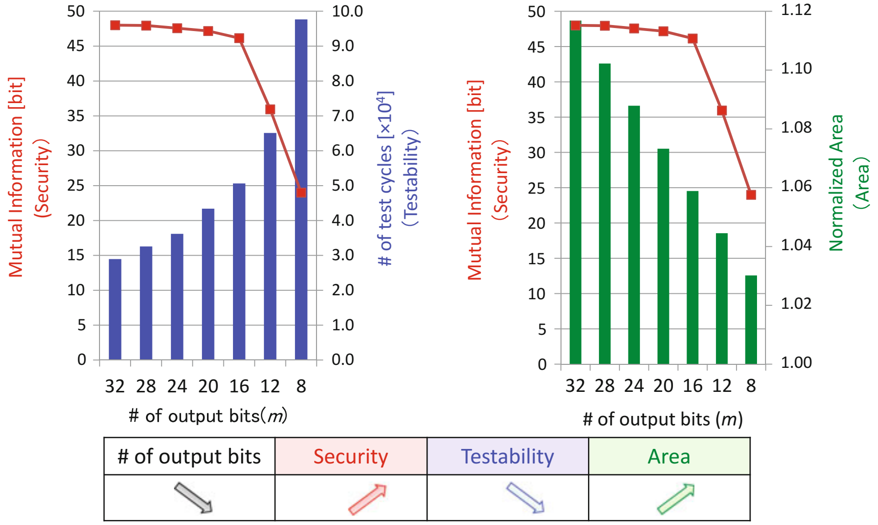


Fig. 10.23 Relation between security, testability and area

whether a countermeasure is applied to a security LSI considering the quantity of leak information calculated by the evaluation method.

In this criterion, it is found that the mutual information of the security LSI of type II countermeasure is equal to the length of the secret key. This result shows that type II countermeasures are not secure. Information of the structures of circuits and scan chains become another secret information in all type II countermeasures. Ito et al. also showed experimental results for circuits of a type III DES security LSI [72] using a MISR (Multiple Input Shift Register) circuit to compact values in scan chains. Table 10.4 shows the parameters of the DES encryption circuit applied in this chip. Figure 10.23 shows the mutual information, number of test cycles and normalized area for each the output bit of MISR. In Fig. 10.23, that the mutual information and testability increase with the number of output bits m. However, the area decreases with m. These results show an example of trade-off between security and testability by using mutual information. These experimental result shows the mutual information of security LSIs applied to countermeasure of the third type depends on the number of outputs bits m. Designers can select suitable countermeasure against scan-based attack by using the evaluation method.

10.6 Evaluation of Tamper Resistance of VLSIs

Yohei Hori, Advanced Industrial Science and Technology (AIST)

10.6.1 SASEBO: An Environment for Evaluating Resistance Against SCA

Side-Channel Attacks (SCAs) have become widely recognized as a serious problem in industry, since Kocher et al. reported timing attacks [73], simple power analysis attacks, and differential power attacks [74]. Until recently, however, there was no common environment for testing devices against SCAs. To address this lack and to facilitate the study of SCAs, we initiated the *SASEBO* project [75] in 2006. We developed several boards to provide a common evaluation environment suitable for academia, industry, and governmental offices globally.

SASEBO (Side-channel Attack Standard Evaluation Board), is the name given to our SCA research project and also a collective term for a series of boards that we developed: SASEBO and SASEBO-G, -B, -R, -GII, -W, -RII, and -GIII [76–78].[2] SASEBO boards are now the most popular SCA evaluation boards worldwide. After the SASEBO project finished, we continued to develop the *ZUIHO* board for educational purposes and the *Miniature Measurement Integrated Circuit Card (MiMICC)* [79] for smartcard evaluation.[3] A summary of our SCA evaluation boards is shown in Table 10.5.

In this section, we introduce the evaluation boards most recently developed under the CREST project, namely, SASEBO-GIII, SASEBO-RII, ZUIHO, and MiMICC.

10.6.1.1 SASEBO-RII

SASEBO-RII (Fig. 10.24) is designed to evaluate custom LSI chips. The board is equipped with a socket for mounting an LSI during cryptographic testing, but not with a field-programmable gate array (FPGA). To simplify the board structure, the control logic is implemented on an external board, such as a SASEBO-W or ZUIHO. Consequently, the size of the SASEBO-RII is only half that of other

[2] The boards SASEBO through SASEBO-GII were developed as a part of the main project, which was funded by the Ministry of Economy, Trade and Industry, Japan. SASEBO-W was developed as part of the Strategic International Research Cooperative Program (SCIP) project funded by the Japan Science and Technology Agency (JST). SASEBO-RII and SASEBO-GIII were developed under the Core Research for Evolutional Science and Technology (CREST) project funded by JST.

[3] ZUIHO and MiMICC were developed as part of the CREST project funded by JST. ZUIHO is named after a Japanese word meaning a *blissful phoenix*.

Table 10.5 Summary of SCA evaluation boards

Name	Year	Cryptographic device	Control device
SASEBO	2007	Virtex-II Pro (XC2VP7)	Virtex-II Pro (XC2VP30)
SASEBO-G	2008	Virtex-II Pro (XC2VP7)	Virtex-II Pro (XC2VP30)
SASEBO-B	2008	Stratix-II (EP2S15)	Stratix-II (EP2S30)
SASEBO-R	2008	LSI socket (QFP160)	Virtex-II Pro (XC2VP30)
SASEBO-GII	2009	Virtex-5 (XC5VLX30/50)	Spartan-3A (XC3S400A)
SASEBO-W	2010	Smartcard slot	Spartan-6 (XC6SLX150)
SASEBO-RII	2011	LSI socket (QFP160/QFP80)	SASEBO-W or ZUIHO
SASEBO-GIII	2012	Kintex-7 (XC7K160T)	Spartan-6 (XC6SLX45)
ZUIHO	2013	Spartan-3A (XC3S700A/1400A)	Spartan-3AN (XC3S50AN)
MiMICC	2013	Spartan-6 (XC6SLX45)	SASEBO-W

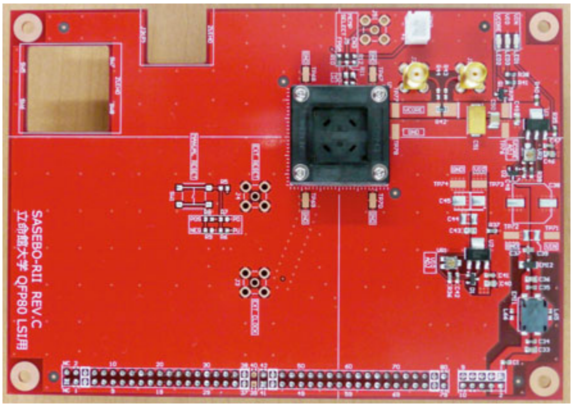


Fig. 10.24 Overview of SASEBO-RII

SASEBO boards. Furthermore, the separation of the control structure greatly improves the board's customizability for LSI evaluation. Because the control logic is not included, a user can easily modify the design of SASEBO-RII to mount a different type of LSI socket.

10.6.1.2 SASEBO-GIII

SASEBO-GIII (Fig. 10.25) is designed for evaluation of SCA effectiveness under state-of-the-art technology scenarios. The board is equipped with a 28-nm process Kintex-7 FPGA for testing cryptographic modules and a Spartan-6 FPGA for implementing control logic. It has two standard FPGA Mezzanine Card (FMC) Low Pin Count connectors, allowing connection of off-the-shelf boards that use an FMC connector, such as HDMI video cards, network cards, and camera boards.

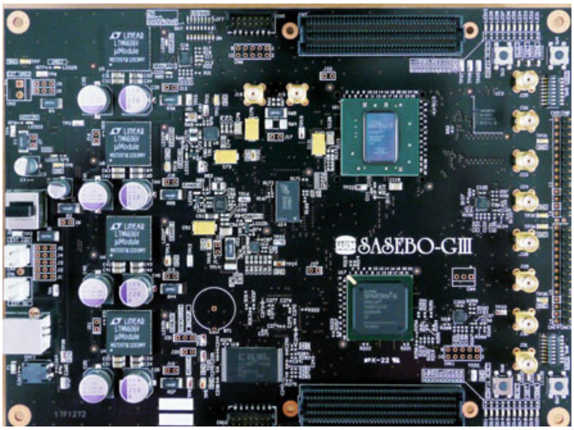


Fig. 10.25 Overview of SASEBO-GIII

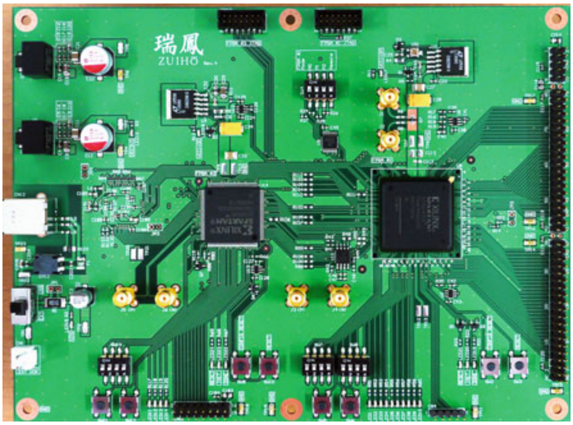


Fig. 10.26 Overview of ZUIHO

10.6.1.3 ZUIHO

ZUIHO (Fig. 10.26) is an FPGA board developed for educational exploration of SCAs and for evaluation of SCA countermeasures. The board is equipped with a 90-nm process FPGA (Spartan-3A) that uses a relatively large process compared with recent FPGAs, such as the 45-nm Spartan-6 used on SASEBO-W and the 28-nm Kintex-7 used on SASEBO-GIII. The power consumption of the Spartan-3A is easier to observe using an oscilloscope, making it more suitable for training and for evaluation of countermeasures.

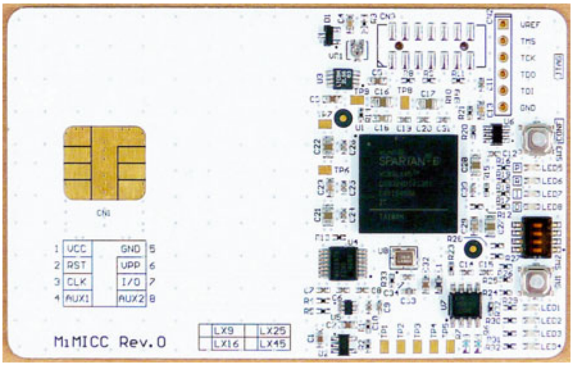


Fig. 10.27 Overview of MiMICC

10.6.1.4 MiMICC

The MiMICC (Fig. 10.27) is a smartcard-shaped FPGA board designed for evaluating the tamper-resistance of a cryptographic module on a smartcard. The board's dimensions are close to those defined by ISO/IEC 7816-2, which are 86.0 × 54.0 mm with 0.8 mm thickness. The parts and devices are mounted on the half plane of the back side of the card to accommodate the card slot. The Spartan-6 LX45 FPGA has adequate logic resources to implement processor IP cores, cryptographic modules, physical unclonable functions, and interface circuits.

10.6.2 Example of Cryptographic Module Evaluation

We here show an example experiment for evaluating tamper-resistance of a cryptographic module. Specifically, We applied Correlation Electromagnetic Analysis (CEMA), a variation of Correlation Power Analysis (CPA) (c.f. Sect. 10.2), to the Advanced Encryption Standard (AES) cryptography [80] on the FPGA of the MiMICC board. For the block diagram of the AES circuit, see Sect. 10.1, Fig. 10.3b [81].

The essence of CEMA is to calculate the correlation between the wave traces (=measured EM strength as a function of time) and the intermediate computation values of encryption/decryption process. If the wave traces (that is, side-channel information) are correlated with the key-related intermediate values, then the cryptographic module is vulnerable to SCAs. If the wave traces are uncorrelated with the key-related data, then the secret key cannot be extracted from the side-channel information. This allows us to evaluate whether the AES module is resistant to EM analysis.

We measured the electromagnetic (EM) radiation from the FPGA using an EM probe and a digital storage oscilloscope. Figure 10.28 shows the experimental setup for the evaluation. The MiMICC is inserted into the card slot of a SASEBO-W,

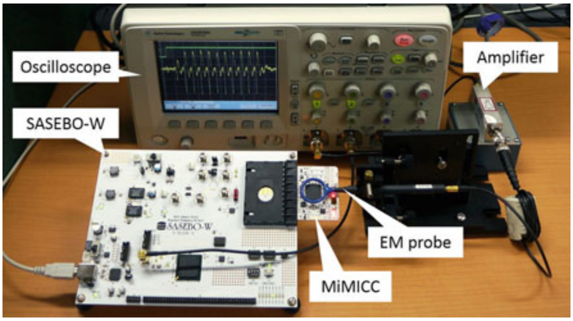


Fig. 10.28 Experimental setup for SCA evaluation using MiMICC and SASEBO-W

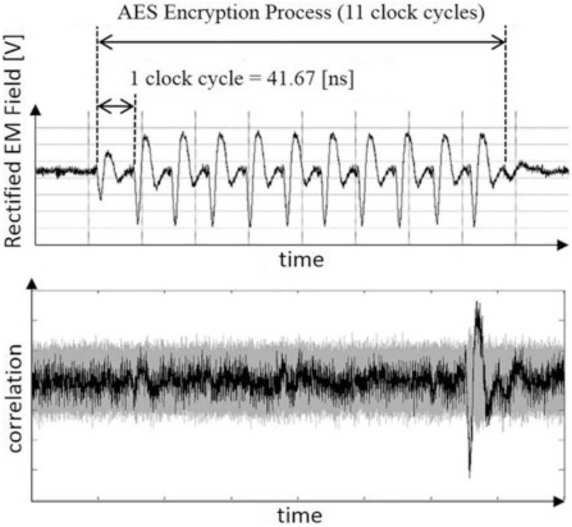


Fig. 10.29 Wave trace during AES encryption and corresponding correlation coefficient

which provides control for the MiMICC. The SASEBO-W is then connected to a host computer, which controls the entire encryption procedure. The EM probe and oscilloscope used are the Agilent[4] DSO 6104A and Langer LF-R 400, respectively. The EM probe is connected to the amplifier Miteq AM-00110 (1–500 MHz, 48 dB).

Figure 10.29 illustrates a wave trace during AES encryption and the correlation coefficient between the wave traces and the key-related intermediate values (c.f. Sect. 12.2). In the experiment, the Hamming distance between the intermediate values of ninth and tenth (final) round state is used for the calculation of correlation coefficient. In this example, 20,000 actual wave traces were collected.

The upper half of Fig. 10.29 shows 11 peaks in the wave trace because AES encryption of one block takes 11 clock cycles. The black line in the lower half of

[4] This oscilloscope is now available from Keysight Technology Inc.

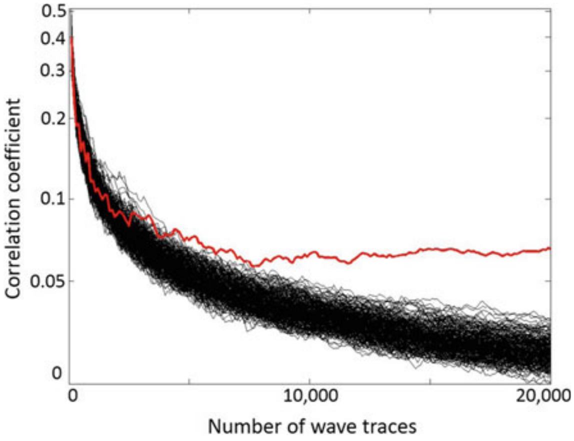


Fig. 10.30 Correlation coefficient calculated under the correct and incorrect keys

the figure is the correlation between the wave traces and the Hamming distance calculated under the correct key hypothesis; gray lines are the correlation calculated under incorrect hypothetical keys. Clearly, the Hamming distance calculated under the correct key hypothesis has a strong correlation with the wave traces during the final round.

Figure 10.30 depicts the variance of the correlation coefficient along with the number of wave traces. The red line shows the transition of the correlation coefficient under the correct key; the black lines show the transitions under incorrect hypothetical keys. The correlation coefficient under the correct key is clearly distinguishable from the others, indicating that we can effectively guess the correct key from the side-channel information.

Figure 10.31 illustrates the relationship between the number of successfully extracted key bytes and the number of wave traces analyzed. The graph shows that the more wave traces we obtain, the higher the success rate for key analysis.

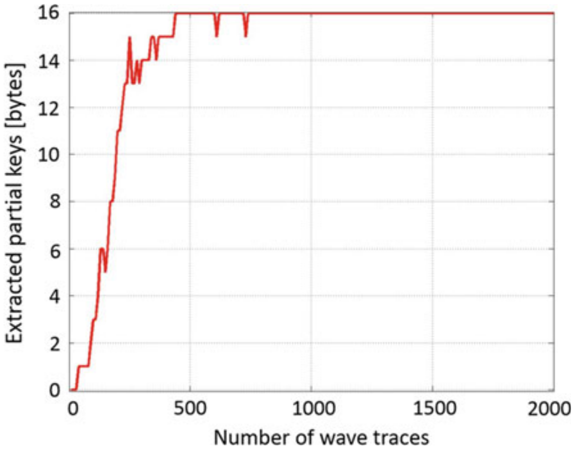


Fig. 10.31 The number of key bytes extracted from AES on MiMICC by CPA

In a real-world evaluation of the tamper-resistance of a cryptographic module, the leakage of side-channel information would be investigated with a greater number of wave traces. Evaluation robustness must strike a balance between the number of wave traces required, the time required to collect and analyze the wave traces, and the cost of conducting the analysis. Clearer metrics for evaluating the tamper resistance of a cryptographic module are currently being discussed for use in Common Criteria, ISO/IEC 17825, and similar. These international standards are introduced in the following section.

10.6.3 International Standards for Evaluating the Tamper-Resistance of Cryptographic Modules

To protect the security of cryptographic modules, the tamper-resistance of those modules should be evaluated on the basis of standardized metrics. Examples of such standards include the Federal Information Processing Standards Publication (FIPS PUB) 140-2 [82] and Common Criteria for Information Technology Security Evaluation (CC) [83–85].

10.6.3.1 FIPS 140-2/-3 and ISO/IEC 19790

FIPS 140-2 was issued in 2001 by the National Institute of Standards and Technology (NIST) in the United States, and subsequently standardized as ISO/IEC 19790. FIPS 140-2 defines four security levels, 1 through 4, and describes the security requirements for cryptographic modules at each of these levels. The evaluation of equipment to see that it satisfies ISO/IEC 19790 is separately defined in ISO/IEC 24759.

Unfortunately, non-invasive attacks, including SCAs, are not yet fully reflected in FIPS 140-2. This has led to support for an update of FIPS 140-3, which is to include a description of SCAs. As of July 2016, the revisions were not yet completed. A revised version of ISO/IEC 19790 was issued in 2014 and includes a description of SCAs. The test methods and evaluation criteria for non-invasive attacks are published as ISO/IEC 17825.

10.6.3.2 Common Criteria and ISO/IEC 15408

CC, also published as ISO/IEC 15408, is an international standard that provides a framework for evaluating the security of various products. CC defines Evaluation Assurance Levels (EAL) 1 through 7 (with 7 representing the most stringent criteria). CC standardizes the procedure to evaluate whether a product surely satisfies the given criteria. The security requirements for the product are provided in another document, the protection profile (PP). The PP is typically created by a product user group or governmental office.

For example, the PP for security IC chips BSI-PP-0035 is provided by the Federal Office for Information Security of Germany (*Bundesamt für Sicherheit in der Informationstechnik*), and PP for smartcards SCSUG-SCPP is provided by the Smart Card Security User Group [86].

Based on CC, in Europe, concrete evaluation methods of hardware-related security have been determined in Joint Interpretation Library (JIL) Hardware-related Attacks Sub-working Group (JHAS). An example of how an attack is numerically scored is given in a document from the JIL [87]. JHAS, however, is a closed working group and therefore the details of the scoring criteria, e.g., what points are given to what degree of attack resistance, have not become open and provided only to member companies.

References

1. W. Stallings, Cryptography and network security, 6th edn. (Pearson education, 2013), p. 10
2. K. Nohl, H. Plötz, Mifare Little Security, Despite Obscurity, 24th Chaos Communication Congress (2007), http://events.ccc.de/congress/2007/Fahrplan/events/2378.en.html
3. F.D. Garcia, G. de Koning Gans, R. Muijrers, P. van Rossum, R. Verdult, R.W. Schreur, B. Jacobs, Dismantling MIFARE Classic, *ESORITICS 2008, LNCS*, vol. 5283 (2008), pp. 97–114
4. E. Biham, O. Dunkelman, S. Indesteege, N. Keller, B. Preneel, *How to Steal Cars—A Practical Attack on KeeLoq, CRYPTO 2007 Rump Session* (2007), http://www.cosic.esat.kuleuven.be/keeloq/keeloq-rump.pdf
5. M. Bushing, S. Segher, *Console Hacking 2010 PS3 Epic Fail, 24th Chaos Communication Congress* (2010), http://events.ccc.de/congress/2010/Fahrplan/events/4087.en.html
6. CRYPTREC, http://www.cryptrec.go.jp/english/list.html
7. T. Eisenbarth, T. Kasper, A. Moradi, C. Paar, M. Salmasizadeh, M.T. Manzuri Shalmani, On the power of power analysis in the real world: a complete break of the KeeLoq code hopping scheme, in *CRYPTO 2008, LNCS*, vol. 5157 (2008), pp. 203–220
8. C. Tarnovsky, Deconstructing a 'Secure' Processor, BlackHat 2010, https://www.blackhat.com/presentations/bh-dc-10/Tarnovsky_Chris/BlackHat-DC-2010-Tarnovsky-DASP-slides.pdf
9. D. Oswald, C. Paar, Breaking Mifare DESFire MF3ICD40: power analysis and templates in the real world, in *CHES 2011, LNCS*, vol. 6917 (2011), pp. 207–222
10. A. Moradi, M. Kasper, C. Paar, On the portability of side-channel attacks—an analysis of the Xilinx Virtex 4, Virtex 5, and Spartan 6 bitstream encryption mechanism (2011), http://eprint.iacr.org/2011/391/20111107:173855
11. S. Skorobogatov, C. Woods, Breakthrough silicon scanning discovers backdoor in military chip, in *CHES 2012, LNCS*, vol. 7428 (2012), pp 23–40
12. DES Standard: FIPS46-3 (1999), http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf
13. AES Standard: FIPS197 (2001), http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
14. R.L. Rivest, A. Shamir, L.M. Adelman, *A Method for Obtaining Digital Signature and Public-key Cryptsystems*, http://web.mit.edu/6.857/OldStuff/Fall03/ref/rivest78method.pdf
15. RSA Standard: PKCS#1 v2.2 (2012), http://www.emc.com/collateral/white-papers/h11300-pkcs-1v2-2-rsa-cryptography-standard-wp.pdf
16. ISO/IEC 15408, http://www.iso.org/iso/catalogue_detail.htm?csnumber=50341

17. FIPS140-2, http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
18. FIPS140-3, http://csrc.nist.gov/groups/ST/FIPS140_3/
19. R. Anderson, M. Bond, J. Clulow, S. Skorobogatov, Cryptographic processors—a survey. Proc. IEEE **94**(2), 357–369 (2006)
20. U.S. Department of Commerce/National Institute of Standards and Technology, Data encryption standard (DES), FIPS PUB 46-3 (1999)
21. E. Biham, A. Shamir, Differential cryptanalysis of DES-like cryptosystems, in *CRYPTO '90* (1990), pp. 2–21
22. E. Biham, A. Shamir, Differential cryptanalysis of DES-like cryptosystems. J. Cryptol. **4**(1), 3–72 (1991)
23. M. Matsui, Linear cryptanalysis method for DES cipher, in *EUROCRYPT '93* (1994), pp. 386–397
24. S.P. Skorobogatov, R.J. Anderson, Optical fault induction attacks, in *CHES '02* (2002), pp. 2–12
25. Y. Li, K. Sakiyama, S. Gomisawa, T. Fukunaga, Fault sensitivity analysis. CHES **2010**, 320–334 (2010)
26. A. Pellegrini, V. Bertacco, T. Austin, Fault-based attack of RSA authentication, in *DATE* (2010), pp. 855–860
27. S. Mangard, E. Oswald, T. Popp, *Power Analysis Attacks* (Springer, 2007)
28. J.J. Quisquater, D. Samyde, Electromagnetic analysis (EMA): measures and countermeasures for smart card, in *e-Smart '01*, *LNCS*, vol. 2140 (2001), pp. 200–210
29. K. Gandolfi, C. Mourtel, F. Olivier, Electromagnetic analysis: Concrete results, in *Proceedings CHES '01*, *LNCS*, vol. 2162 (2001), pp. 251–261
30. P. Kocher, J. Jaffe, B. Jun, Differential power analysis, in *Proceedings Crypto '99, LNCS*, vol. 1109 (1999), pp. 388–397
31. E. Brier, C. Clavier, F. Olivier, Correlation power analysis with a leakage model, in *Proceedings CHES* (2004), pp. 16–29
32. B. Gierlichs, L. Batina, P. Tuyls, B. Preneel, Mutual information analysis, in *Proceedings of CHES 2008, LNCS*, vol. 5154 (2008), pp. 426–442
33. P.C. Kocher, Timing attacks on implementations of diffie-hellman, RSA, DSS, and other systems, in *CRYPTO '96* (1996), pp. 104–113
34. R. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM **21**(2), 120–126 (1978)
35. T. Katashita, A. Sasaki, Y. Hori, M. Shiozaki, and T. Fujino, Development of evaluation environment for physical attacks against embedded devices. In *GCCE* (2012), pp. 598–601
36. Evaluation environment for side-channel attacks. Research Institute for Secure Systems, National Institute of Advanced Industrial Science and Technology (AIST). http://www.toptdc.com/product/sasebo/
37. B. Yang, K. Wu, R. Karri, Scan based side channel attack on dedicated hardware implementations of data encryption standard, in *ITC* (2004), pp. 339–344
38. M. Yoshimura, Malicious attacks on electronic systems and VLSI for security, in *The Book Name of CREST DVLSI*, ed. by S. Asai, chap. 12.6 (Springer)
39. J.D. Golic, C. Tymen, Multiplicative masking and power analysis of AES, in *Proceedings CHES* (2002), pp. 198–212
40. J. Waddle, D. Wagnet, Towards efficient second-order power analysis, in *Proceedings CHES* (2004), pp. 1–15
41. L. Batina, B. Gierlichs, E. Prouff, M. Rivain, F.-X. Standaert, N. Veyrat-Charvillon, Mutual information analysis: a comprehensive study. J. Cryptol. **24**(2), 269–291 (2011)
42. S. Chari, J.R. Rao, P. Rohatgi, Template Attacks, in *Proceedings CHES* (2002), pp. 13–28
43. J. Quisquater, D. Samyde, Electromagnetic analysis (EMA): measures and countermeasures for smart card, E-smart (2001), pp. 200–210
44. S. Mangard, E. Oswald, T. Popp, Power *Analysis Attacks: Revealing the Secrets of Smart Cards* (Springer, 2007)

45. T. Katashita, Experimentation of decoupling capacitance effects of CPA, in *SCIS* (2009) (in Japanese)
46. NIST: Advanced Encryption Standard (AES), FIPS PUB-197, http://www.csrc.nist.gov/publications/fips/index.html
47. T. Nakai, M. Shiozaki, T. Fujino, Evaluation of on-chip decoupling capacitor's effect on AES cryptographic circuit, in *SASIMI, R1-3* (2013)
48. K. Tiri, I. Vebauwhede, A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation, in *Proceedings DATE* (2004)
49. E. Trichina, Combinational logic design for AES SubByte transformation on masked data, in *Cryptology e-Print Archive, 2003/236* (2003)
50. T. Pop, S. Mangard, Masked dual-rail precharge logic: DPA-resistance without routing constrain, in *Proceedings CHES 2006, LNCS*, vol. 4249 (2006), pp. 255–259
51. D. Suzuki, M. Saeki, K. Shimizu, A. Satoh, A design methodology for a DPA resistant cryptographic LSI with RSL techniques, in *Proceedings CHES* (2009), pp. 189–204
52. S. Nikova, C. Rechberger, V. Rijmen, Threshold implementations against side-channel attacks and glitches, in *Proceedings ICICS 2006, LNCS*, vol. 4307 (2006), pp. 529–545
53. D. Suzuki, M. Saeki: Security evaluation of DPA countermeasures using dual-rail precharge logic style, in *Proceedings CHES 2006, LNCS*, ed. by L. Goubin, M. Matsui, vol. 4249 (Springer, 2006), pp. 255–269
54. M. Shibatani, M. Shiozaki, Y. Hashimoto, T. Kubota, T. Fujino, Power analysis resistant IP core using IO-masked dual-rail ROM for easy implementation into low-power area-efficient cryptographic LSIs, in *Proceeding of SASIMI* (2013)
55. T. Asai, M. Shiozaki, T. Kubota, T. Fujino, M. Yoshikawa, A countermeasure against side channel attack on cryptographic LSI using clock variation mechanism (in Japanese). IEEJ Trans. Electron. Inf. Syst. **133**(12), 2134–2142 (2013)
56. M. Yoshikawa, T. Asai, Tamper resistance verification method for consumer security products, in *Proceedings of Computational Science and Computational Intelligence* (2014), pp. 30–33
57. K. Sugioka, T. Asai, M. Yoshikawa, Event modeling method for verification of power analysis attacks, in *Proceedings of the 18th Workshop on Synthesis and System Integration of Mixed Information Technologies* (2013), pp. 280–281
58. T. Asai, M. Shiozaki, T. Fujino, M. Yoshikawa, A vulnerability evaluation method against power analysis attack on gate-level design phase. IEEJ Trans. Electron. Inf. Syst. **133**(5), 947–956 (2013)
59. M. Yoshikawa, T. Asai, Tamper-resistance evaluation for cryptographic side channel leakage at design stage
60. M. Ono, M. Katsube, M. Shiozaki, T. Fujino, M. Yoshikawa, Architecture aware fault analysis based on differential presumption for multiple errors and its evaluation. IEEJ Trans. Electron. Inf. Syst. **132**(12), 1888–1896 (2012)
61. T. Asai, M. Yoshikawa, Efficient acquisition of the side-channel information using event model simulation methods, in *Proceedings of 30th Symposium on Cryptography and Information Security*, vol. 1E1-1 (2013), pp. 1–6
62. T. Asai, M. Yoshikawa, Evaluation for cryptographic side channel leak using FDTD simulation, in *IEICE Technical Report*, vol. 113, no. 217, ISEC2013-51 (2013), pp. 1–7
63. H. Fujiwara, *Logic Testing and Design for Testability* (The MIT Press, 1985)
64. B. Yang, K. Wu, R. Karri, Scan based side channel attack on dedicated hardware implementations of data encryption standard, in *Proceedings of International Test Conference 2004 (ITC 2004)* (2004), pp. 339–344
65. B. Yang, K. Wu, R. Karri, Secure scan: a design-for-test architecture for crypto chips. IEEE Trans. Comput. Aided Des. Integr. Circuits Syst. **25**(10), 2287–2293 (2006)
66. R. Nara, K. Satoh, M. Yanagisawa, T. Ohtsuki, N. Togawa, Scan-based side-channel attack against RSA cryptosystems using scan signatures. IEICE Trans. Fund. Electron. Commun. Comput. Sci. **E93-A**(12), 2481–2489 (2010)

67. R. Nara, N. Togawa, M. Yanagisawa, T. Ohtsuki, Scan-based attack against elliptic curve cryptosystems, in *Proceedings of the 2010 Asia and South Pacific Design Automation Conference (ASP-DAC 2010)* (2010), pp. 407–412
68. M. Yoshimura, Y. Ito, H. Yasuura, An estimation of encryption LSI testability against scan based attack, in *2010 International Symposium on Communications and Information Technologies (ISCIT)* (2010), pp. 727–731
69. R. Nara, H. Atobe, Y. Shi, N. Togawa, M. Yanagisawa, T. Ohtsuki, State-dependent changeable scan architecture against scan-based side channel attacks, in *Proceedings of 2010 IEEE International Symposium on Circuits and Systems (ISCAS)* (2010), pp. 1867–1870
70. M. Inoue, T. Yoneda, M. Hasegawa, H. Fujiwara, Balanced secure scan: partial scan approach for secret information protection. J. Electron. Test. **27**(2), 99–108 (2011)
71. K. Fujiwara, H. Fujiwara, H. Tamamoto, Differential behavior equivalent classes of shift register equivalents for secure and testable scan design. IEICE Trans. Inf. Syst. **E94-D**(7), 1430–1439 (2011)
72. Y. Ito, M. Yoshimura, H. Yasuura, A quantitative evaluation of security for scan-based side channel attack and countermeasures. IEICE Tech. Rep. **109**(316), 73–78 (2009). DC2009-39, 2009 (In Japanese)
73. P.C. Kocher, *CRYPTO '96* (1996), pp. 104–113
74. P. Kocher, J. Jaffe, B. Jun, *CRYPTO '99* (1999), pp. 388–397
75. A. Satoh, T. Katashita, H. Sakane, Synthesiology **3**(1), 56 (2010)
76. T. Katashita, Y. Hori, H. Sakane, A. Satoh, *NIAT* (2011)
77. T. Katashita, A. Sasaki, Y. Hori, M. Shiozaki, T. Fujino, *GCCE* (2012), pp. 598–601
78. Y. Hori, T. Katashita, A. Sasaki, A. Satoh, *GCCE* (2012), pp. 657–660
79. T. Katashita, A. Sasaki, Y. Hori, *GCCE* (2013), pp. 37–39
80. U.S. Department of Commerce/National Institute of Standards and Technology. Announcing the advanced encryption standard (AES). FIPS PUB 197 (2001)
81. T. Fujino, D. Suzuki, *The Book Name of CREST DVLSI*, ed. by S. Asai (Springer), chap. 12.1
82. U.S. Department of Commerce/National Institute of Standards and Technology. Security requirements for cryptographic modules. FIPS PUB 140-2 (2001)
83. C.C. for Information technology security evaluation. Part 1: introduction and general model, version 3.1, revision 4 (2012)
84. C.C. for Information technology security evaluation. Part 2: security functional components, version 3.1, revision 4 (2012)
85. C.C. for Information technology security evaluation. Part 3: security assurance components, version 3.1, revision 4 (2012)
86. S.C.S.U. Group. Smart card protection profile (SCSUG-SCPP), version 3.0 (2001)
87. Joint Interpretation Library. Application of attack potential to smartcards, version 2.9 (2013), http://www.sogisportal.eu/documents/cc/domains/sc/JIL-Application-of-Attack-Potential-to-Smartcards-v2-9.pdf

Chapter 11
Test Coverage

Masahiro Fujita, Koichiro Takayama, Takeshi Matsumoto, Kosuke Oshima, Satoshi Jo, Michiko Inoue, Tomokazu Yoneda and Yuta Yamato

Abstract Verification is a process to prove the correctness of the design of a system referring the design information to requirements specification, and test is a process to prove that a system in its actual embodiment in either prototype or real product performs up to the description of the specification. Whatever functions, performance, or dependability may have been conceived, designed, and built into a system, one can be certain that the actual product exhibits such properties only to the extent that the design has been verified and the product has been tested. In reality, comprehensive coverage of verification and test over ramified combination of functionalities, use cases, and operational conditions becomes increasingly more difficult as systems become more complex. The verification and test are thus very important for assuring system's quality. This chapter addresses some of the key issues of verification and test of electronic systems that use VLSIs as essential components with an emphasis on dependability. Section 11.1 is an overview of the issues and discusses the metrics of verification and test coverage. Section 11.2 addresses two topics: detection of errors in logic design and formal verification, the latter being a method to verify logic design by mathematical reasoning. Section 11.3 introduces the use of Built-in Self-Test (BIST) method to monitor circuit delays in a VLSI precisely enough to be able to predict failures due to device degradation in operation. Section 11.4 proposes a way to accurately measure the delays in the presence of temperature and voltage variation experienced in the field.

M. Fujita (✉) · S. Jo
The University of Tokyo, Tokyo, Japan
e-mail: fujita@ee.t.u-tokyo.ac.jp

K. Takayama
Fujitsu Ltd., Kawasaki, Japan

T. Matsumoto
Ishikawa National College of Technology, Tsubata, Ishikawa, Japan

K. Oshima
Hitachi, Ltd., Tokyo, Japan

M. Inoue · T. Yoneda · Y. Yamato
Nara Institute of Science and Technology, Ikoma, Japan

S. Asai (ed.), *VLSI Design and Test for Systems Dependability*,
https://doi.org/10.1007/978-4-431-56594-9_11

Keywords Test coverage • Formal verification • Debugging
Circuit delay • BIST • Field test

11.1 Verification and Test Coverage

Koichiro Takayama, Fujitsu Ltd.

Coverage metrics are widely used in the verification and validation of both hardware and software to show the progress as well as the goal of the verification and validation process.

Some of the dependable design techniques described in this book are applied to logic circuits in a system. In order to achieve the intended dependability of the system, it is necessary to make sure that the circuits operate correctly.

The objective of the verification is to make a design bug free, but as far as we know, there are no coverage metrics to satisfy this objective such that by achieving 100% coverage it guarantees the design works perfectly.

In this article, topics of coverage metrics in verification and test are described.

11.1.1 Verification Coverage Metrics

In this section, coverage metrics for logic verification are described.

Coverage metrics provide aspects to express if the logic in the design under verification (DUV) is activated in logic simulation or not.

Coverage metrics are categorized into three as follows;

(1) Code coverage

This is one of the most basic metrics to show which parts of the source code of the DUV written in a hardware description language are covered. Most of the logic simulators can measure the coverage automatically during simulation of the DUV. Major code coverage metrics are as follows.

- Line coverage: the fraction of lines of source code which are executed.
- Condition coverage: the fraction of subexpressions of Boolean expressions which are evaluated to true and false.
- FSM coverage: the fraction of the states of a finite state machine (FSM) which are visited.

Code coverage does not guarantee that the DUV is totally correct since code coverage neither uncovers unimplemented features, nor measures concurrent or temporal behaviors of the DUV.

(2) Functional coverage based on the design implementation

This metric is manually derived by a designer by focusing on the implementation-dependent features of the DUV, for example, if the read or write operation took place when a FIFO is empty or full, it is checked whether a pipeline is stalled, or a request is acknowledged within five cycles. It depends very much on the designer's experience and attention how high the resulting verification coverage will be.

(3) Functional coverage based on the design specification

This metric is manually derived from the specification of the DUV by a designer. The derived behavior is concurrent or temporal but independent of the implementation. In many cases, the metric is written in SystemVerilog Assertions (SVA) [1] or PSL [2]. When the derived behavior is too difficult to write in SVA or PSL, a coverage model is written in a hardware description language and the coverage metrics [1] and/or [2] are applied to the model. The coverage will again depend pretty much on the designer's skills.

11.1.1.1 Coverage Metrics with High Correlation to Design Bugs

As described above, coverage metrics are used to define the verification goal. Importantly, it should be noted that more design bugs can be found by achieving 100% of a coverage metric and using better metric. From this point of view, it may be useful to make a new metric by analyzing the design bugs experienced in the past.

In this section, we illustrate an example of metric relating to a bug of incorrect priority of the branch condition. In Fig. 11.1, code A shows a code fragment with an incorrect order of the branch conditions while code B shows the correct one where the condition C should have a higher priority than condition B.

When a set of four vectors (condition A, condition B, condition C) = (true, false, false), (false, true, false), (false, false, true), (false, false, false) is applied to code A and code B, the line coverage for both code is 100%, but the bug is uncovered.

A vector (false, true, true) can uncover the bug. And, in order to verify the priority of all of the combinations of two conditions among three, a set of vector

```
if ( conditionA )
statementA ;
else if ( conditionB )
statementB ;
else if ( conditionC )
statementC ;
else statementD ;
```

(a) codeA : incorrect design

```
if ( conditionA )
statementA ;
else if ( conditionC )
statementC ;
else if ( conditionB )
statementB ;
else statemetnD ;
```

(b) codeB : correct design

Fig. 11.1 Example of a design bug

(condition A, condition B, condition C) = (true, true, false), (true, false, true), (false, true, true), (false, false, true), (false, false, false) is required.

As described in this section, if a pattern in the structure of the source code (design implementation) can be identified by analyzing the bug, a coverage metric can be derived which contributes to the design quality effectively.

11.1.1.2 Cooperation of Logic Simulation and Formal Verification

Formal verification is a technique to prove mathematically whether a design satisfies a property (specification). If a design does not satisfy a property, a counterexample, i.e., an input vector sequence which violates the property, is generated.

If the negation of a coverage metric can be written in a set of properties, by formally verifying the properties against the DUV, part of the coverage space can be eliminated when corresponding property is proved to be redundant, or an input vector sequence for a corner case can be generated as a counterexample. Such cooperation between logic simulation and formal verification has been widely used.

11.1.2 Test Coverage

In this section, issues in manufacturing test to validate dependability of the computer system are discussed. The major causes of malfunction of the system in the field are timing errors by aging and occasional soft error by radiation events such as collision of cosmic rays or alpha particles.

11.1.2.1 Test Coverage for Soft-Error Resilience

Soft-error resilience is one of the main topics of dependability described in Chap. 3. Many existing designs have adopted various techniques in order to recover from the intermittent 1-bit error, for example, error control coding (ECC) for data path, triple modular redundancy for control logic, soft-error tolerant flip-flops, hardware instruction retry. In order to validate the soft-error resilience circuitry after fabrication, the hardware might have a feature to inject a pseudo 1-bit error. It is another coverage problem what additional logic is required to validate soft-error resiliency efficiently.

11.1.2.2 Test Coverage for Timing Error

Recent high-performance computing systems consist of more than tens of thousands processors. In order to reduce timing errors caused by aging in field, they

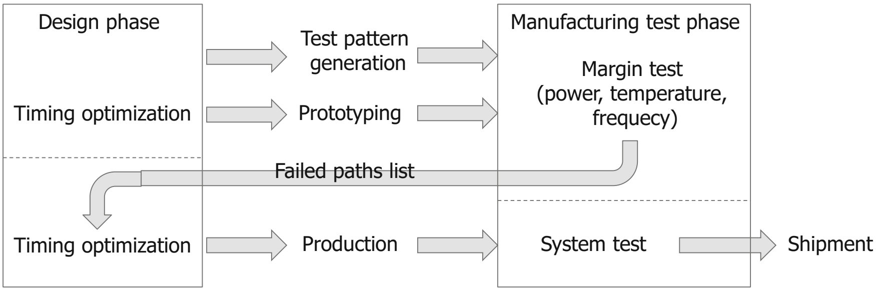


Fig. 11.2 Example flow of a chip test

require appropriate timing optimization for critical paths at design phase and manufacturing test to validate critical paths while keeping a high signal active ratio.

Figure 11.2 shows an example of chip test flow from the view of timing error.

- At design phase, timing is optimized by taking signal integrity and power noise into account. Circuit simulation considering parasitic elements is useful to assess signal integrity affected by cross-talk, ringing, etc.
- At prototyping phase, engineering sample has been tested to extract paths with low margins.
- Timing is further optimized for the extracted paths.
- Manufacturing test is applied to eliminate chips with low margins caused by manufacturing variability.

There are two problems in the flow as follows.

(1) At the design phase, static timing analysis (STA) is applied. When the latest device technology is used, calibration of the model parameters has to be done carefully.

(2) Test pattern for critical paths extracted by STA should be generated with high signal active ratio to validate signal integrity and power noise effect.

11.1.3 Summary

In this article, we described the following challenges of coverage metrics:

- How a verification coverage metric can be addressed by taking the characteristics of design bug into account.
- How a test coverage metric can be addressed by taking signal integrity and power noise effect into account.

11.2 Design Errors and Formal Verification

Masahiro Fujita, The University of Tokyo
Takeshi Matsumoto, Ishikawa National College of Technology
Kosuke Oshima, Hitachi, Ltd.
Satoshi Jo, The University of Tokyo

11.2.1 Logic Design Debugging

Logic design verification and debugging is one of the most time-consuming tasks in VLSI design processes. Once incorrect behaviors are detected through simulation and/or formal verification process, the design must be logically debugged. Incorrect behaviors are represented in the form of counterexamples which are generated from simulation/formal verification. Counterexamples are the input/output patterns, where output patterns are different from the correct expected patterns inferred from the specification. In this section, we deal with logic debugging processes mostly targeting gate-level designs by analyzing counterexamples. We show through experiments that even with small numbers of counterexamples, complete logic debugging is feasible, which shows practical effectiveness of the proposed approach. Also, in order to make the proposed method powerful enough for practical designs in terms of logic debugging, we introduce a "necessary condition" for the selection of signals in Sect. 11.2.4.3, when correcting the logical bugs. This necessary condition takes a very important role to filter out non-useful signals for the selection and significantly improves the performance of the logical debugging.

Once counterexamples in the verification processes are generated, logic debugging processes must start. Logic design debugging consists of two phases. The first phase is to locate suspicious portions of the design by analyzing the internal behaviors of the buggy design with its counterexamples. The second phase is to actually correct those suspicious portions by replacing them with appropriate new circuits.

Path tracing and its generalization with SAT (satisfiability checking)-based formulation are the common and widely used approaches for the first phase. They can locate suspicious portions assuming that those may be replaced with new circuits whose inputs are possibly all primary inputs of the target circuit. These techniques are very briefly reviewed in Sect. 11.2.2. For details, please see [3].

We present a formulation based on LUT (Lookup Table) for the second phase of the logic debugging process. As a LUT can represent any logic functions with the given set of input variables, correction is guaranteed to succeed as long as the input variables of the LUTs are appropriately selected. We present the correction method as well as heuristic methods for selecting input variables of LUTs in Sect. 11.2.3.

The last subsection gives future perspectives on logic design debugging.

11.2.2 Identification of Buggy Portions of Designs

In general, a counterexample is an example run of the target buggy design, where some of the output values are different from the expected values inferred from the specification, that is, they are incorrect. The first phase of the logical debugging is to locate the cause of the bugs by analyzing a given set of counterexamples. It is realized by locating the suspicious internal signals, whose values are the cause of the wrong output values.

This analysis can be realized by tracing who are in charge of the incorrect output values, which is called "path tracing" in general. By tracing the functional dependencies in the logic circuits, the set of internal gates which determine the values of such outputs can be generated. They should include the root cause of the bugs in the sense that by modifying the functionality of those gates, the incorrect output values can become correct.

Path tracing methods are generalized using SAT-based formulation, called SAT-based diagnosis, in [3]. Please note that the methods such as path tracing and the ones in [3] examine the designs only with counterexamples given and do not refer to specifications. Also they guarantee correctability if the set of gates identified can be replaced with some appropriate logic functions with possibly all primary inputs. That is, we may need to identify the appropriate sets of inputs of the gates, which could be very different from the current sets of inputs, for correction. This is a critical issue for the correction part of debugging as shown below.

11.2.3 Correction of Buggy Portions

11.2.3.1 Basic Idea

In this paper, we focus on debugging gate-level designs. We assume existence of a specification in terms of golden models in RTL or in gate level. Our method tries to let a given circuit under debugging behave equivalently to the specification through modifications inside the circuit. That is, we need to identify the appropriate different functions for some of the internal gates for corrections. To achieve this, we introduce some amount of programmability with LUTs and MUXs in the circuit under debugging and find a way to program the introduced programmable circuits for the purpose of formulating the debugging processes mathematically. Please note that after identifying such appropriate functions for internal gates, those gates are assumed to be completely replaced with new gates corresponding to those functions. That is, programmability is introduced only for mathematical modeling and is nothing to do with actual implementations.

The basic idea of our proposed debugging methods is to correct a circuit under debugging by finding another logic function with the same set of inputs for each gate that is identified as a bug location, in such a way that the entire circuit becomes equivalent to its specification. In other words, our method tries to replace each of the original (possibly) buggy gates with a different logic gate having the same input variables. So the new gate to be used for replacement may have to realize complicated logic functions with the same inputs and cannot be implemented with a single gate, but with a set of simple gates, such as NAND, NOR, etc. As described in the following, we utilize an existing method proposed by Jo et al. [4, 5] to efficiently derive logic functions of programmable circuits. There are, however, bugs which cannot be corrected if the input variables of the gates remain the same. In such cases, we need to add an additional input variable to LUTs or MUXs. When the number of variables in a circuit is very large, it is not practical to check all the variables one by one. To quickly find variables which cannot improve the chance of getting a correct logic when they are connected to LUTs or MUXs, we introduce a necessary condition that should be satisfied by each variable in order to improve the chance of correction. We also propose an efficient selection method based on that condition.

11.2.3.2 Base Algorithm: Finding a Configuration of LUTs Using Boolean SAT Solvers

For easiness of explanation, in this paper we assume the number of outputs for the target buggy circuit is one. That is, one logic function in terms of primary inputs can represent the logic function for the entire circuit. This makes the notations much simpler, and also extension for multiple outputs is straightforward.

As there is only one output in the design, a specification can be written as one logic function with the set of primary inputs as inputs to the function. For a given specification, $SPEC(x)$ and an implementation with programmable circuits, $IMPL(x, v)$, where x denotes the set of primary input variables and v denotes the set of variables to configure programmable circuits inside, the problem is to find a set of appropriate values for v satisfying that $SPEC$ and $IMPL$ are logically equivalent, which can be described as QBF (Quantified Boolean Formula) problem as follows: $\exists v \cdot \forall x \cdot SPEC(x) = IMPL(x, v)$. That is, with appropriate values for v, regardless of input values (values of x), the circuits must be equivalent to the specification, i.e., the output values are the same which can be formulated as the equivalence of the two logic functions for the specification and the implementation. There are two nested quantifiers in the formula above, that is, existential quantifiers are followed by universal quantifiers, which are called two-level QBF in general. Normal SAT formulae have only existential quantifiers and no universal ones.

In [4], Jo et al. proposed to apply CEGAR (Counterexample-Guided Abstraction Refinement)-based QBF solving method to the circuit rectification problem. Here, we explain the method using 2-input LUT for simplicity although LUT having any numbers of inputs can be processed in a similar way. A 2-input LUT logic can be represented by introducing four variables, $v_{00}, v_{01}, v_{10}, v_{11}$, each of which corresponds to the value of one row of the truth table. Those four variables are multiplexed with the two inputs of the original gate as control variables, as shown in

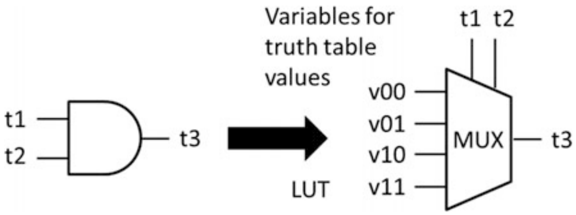


Fig. 11.3 LUT is represented with multiplexed four variables as truth table values

Fig. 11.3. In the figure, a two-input AND gate is replaced with a two-input LUT. The inputs, t_1, t_2, of the AND gate becomes the control inputs to the multiplexer. With these control inputs, the output is selected from the four values, $v_{00}, v_{01}, v_{10}, v_{11}$. If we introduce M of 2-input LUTs, the circuit has $4 \times M$ more variables than the variables existed in the original circuit. We represent those variables as v_{ij} or simply v which represents a vector of v_{ij}. v variables are treated as pseudo primary inputs as they are programmed (assigned appropriate values) before utilizing the circuit. t variables in the figure correspond to intermediate variables in the circuit. They appear in the CNF of the circuits for SAT/QBF solvers.

If the logic function at the output of the circuit is represented as $f_I(v, x)$ where x is an input variable vector and v is a program variable vector, after replacements with LUTs, the QBF formula to be solved becomes $\exists v \cdot \forall x \cdot f_I(v, x) = f_S(x)$, where f_S is the logic function that represents the specification to be implemented. Under appropriate programming of LUTs (assigning appropriate values to v), the circuit behaves exactly the same as specification for all input value combinations.

Although this can simply be solved by any QBF solvers theoretically, only small circuits or small numbers of LUTs can be successfully processed [4]. Instead of doing that way, we here like to solve given QBF problems by repeatedly applying normal SAT solvers using the ideas shown in [6, 7].

Basically, we solve the QBF problem only with normal SAT solvers in the following way. Instead of checking all value combinations on the universally quantified variables, we just pick up some small numbers of value combinations and assign them to the universally quantified variables. This would generate SAT formulae which are just necessary conditions for the original QBF formulae. Please note that here we are dealing with only two-level QBF, and so if universally quantified variables get assigned actual values (0 or 1), the resulting formulae simply become SAT formulae. The overall flow of the proposed method is shown in Fig. 11.4. For example, if we assign two combinations of values for x variables, say $a1$ and $a2$, the resulting SAT formula to be solved becomes like: $\exists v \cdot (f_I(v, a1) = f_S(a1)) \wedge (f_I(v, a2) = f_S(a2))$. Then, we can just apply any SAT solvers to them. If there is no solution, we can conclude that the original QBF formulae do not have solution neither. If there is a solution found, we need to make sure that it is a real solution for the original QBF formula. Because, we have a solution candidate $v_{assigns}$ (these are the solution found by SAT solvers) for v, we simply make sure the following: $\forall x \cdot f_I(v_{assigns}, x) = f_S(x)$. This can be solved by either usual SAT solvers or combinational equivalence checkers. In the latter case,

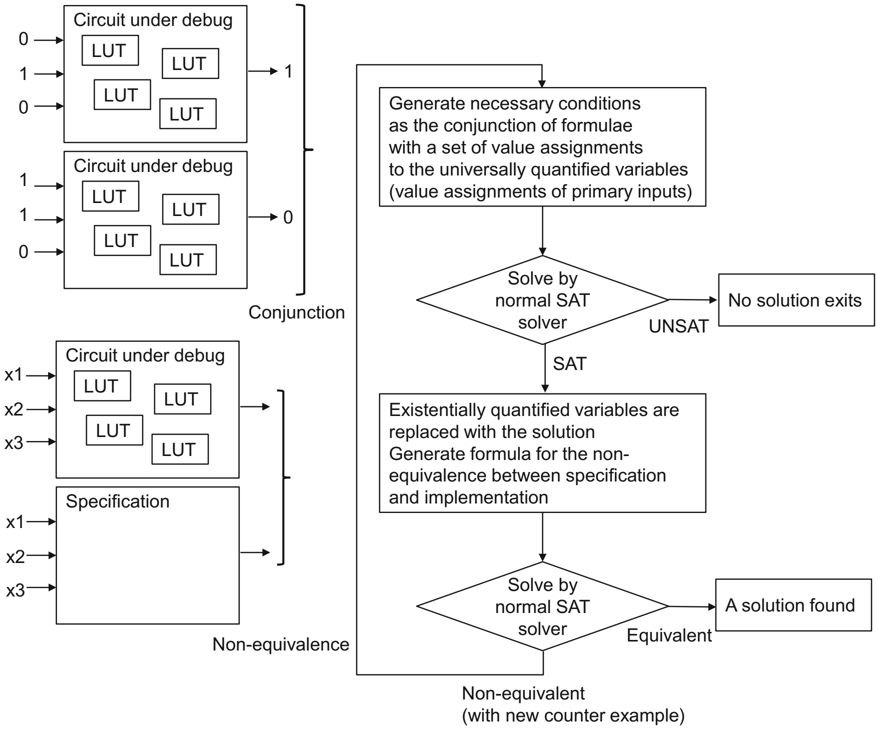

Circuit under debug
LUT
LUT
LUT
LUT
0
1
0
1
Circuit under debug
LUT
LUT
LUT
LUT
1
1
0
0
Conjunction
Circuit under debug
x1
x2
x3
LUT
LUT
LUT
LUT
Specification
x1
x2
x3
Non-equivalence
Generate necessary conditions as the conjunction of formulae with a set of value assignments to the universally quantified variables (value assignments of primary inputs)
Solve by normal SAT solver
UNSAT
No solution exits
SAT
Existentially quantified variables are replaced with the solution Generate formula for the non-equivalence between specification and implementation
Solve by normal SAT solver
Equivalent
A solution found
Non-equivalent (with new counter example)

Fig. 11.4 Overall flow of the rectification method in [4]

circuits with tens of millions of gates may be processed, as there have been conducted significant amount of researches for combinational equivalence checkers which utilize not only state-of-the-art SAT techniques but also various analysis methods on circuit topology. If they are actually equivalent, then the current solution is a real solution of the original QBF formula. But if they are not equivalent, a counterexample, say x_{sol}, is generated and is added to the conditions for the next iteration: $\exists v \cdot (f_I(v, a1) = f_S(a1)) \wedge (f_I(v, a2) = f_S(a2)) \wedge (f_I(v, x_{sol}) = f_S(x_{sol}))$. This solving process is repeated until we have a real solution or we prove the nonexistence of solution. In the left side of Fig. 11.4, as an example, the conjunction of the two cases where inputs/output values are $(0, 1, 0)/1$ and $(1, 1, 0)/0$ is checked if satisfiable. If satisfiable, this gives possible solutions for LUTs. Then using those solutions for LUTs, the circuit is programmed and is checked to be equivalent with the specification. As we are using SAT solvers, usually nonequivalence can be made sure by checking if the formula for nonequivalence is unsatisfiable.

Satisfiability problem for QBF in general belongs to P-Space complete. In general, QBF satisfiability can be solved by repeatedly applying SAT solvers, which was first discussed under FPGA synthesis in [8] and in program synthesis in

[9]. The techniques shown in [6, 7] give a general framework on how to deal with QBF only with SAT solvers. These ideas have also been applied to so-called partial logic synthesis in [5].

11.2.3.3 Proposed Method to Correct Gate-Level Circuits

Overall Flow

Figure 11.5 shows an overall flow of our proposed correction method. Given

- a specification,
- an implementation circuit that has bugs, and
- a set of candidate locations of the bugs,

The method starts with replacing each logic gate corresponding to a candidate bug location with a LUT. Each inserted LUT has the same set of input variables as its original gate. Then, by applying the method in [4, 5], we try to find a configuration of the set of LUTs so that the specification and the implementation become logically equivalent. Once such a configuration is found, it immediately means we get a logic function for correction. Then, another implementation will be created based on the corrected logic function, which may require re-synthesis or synthesis for ECO (Engineering Change Order). Although the method to compute a configuration of LUTs for correction in [4, 5] is relatively more efficient than most of the other methods, it can solve up to hundreds of LUTs within a practical runtime. Therefore, it is not practical to replace all of the gates in the given circuit with

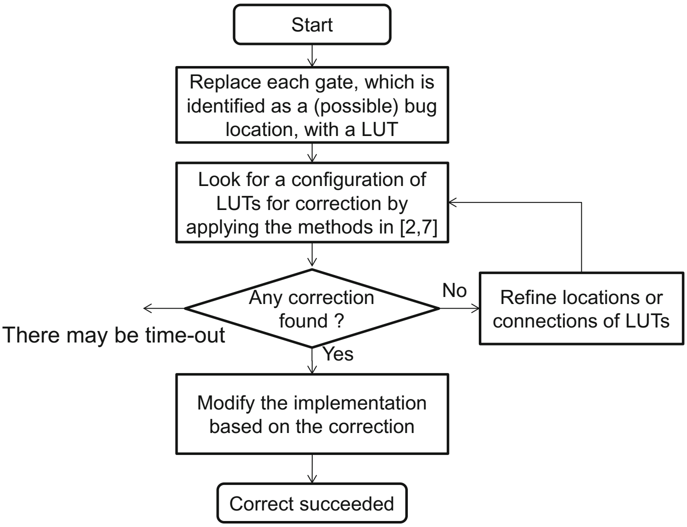

Start
Replace each gate, which is identified as a (possible) bug location, with a LUT
Look for a configuration of LUTs for correction by applying the methods in [2,7]
Any correction found ?
No
Refine locations or connections of LUTs
There may be time-out
Yes
Modify the implementation based on the correction
Correct succeeded

Fig. 11.5 An overall correction flow

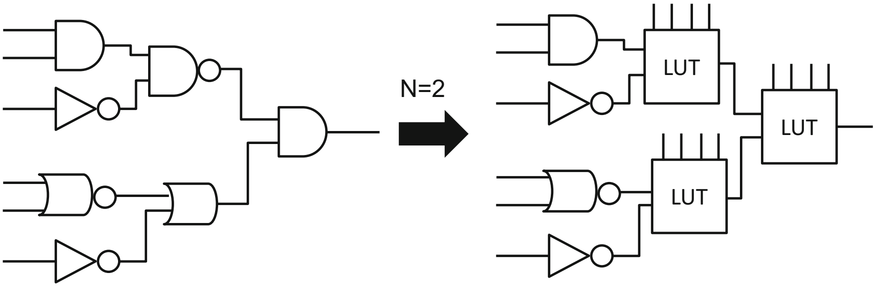


Fig. 11.6 An example of LUT insertions

LUTs, and the number of LUTs inserted into the implementation influence a lot on the runtime for correction. In order to obtain candidate locations of bugs, existing methods such as [3] can be utilized. In this work, we employ a simple heuristic, which is similar to the path tracing method that all gates in logic cones of erroneous primary outputs are replaced with LUTs when they are within a depth of N level from the primary outputs. Figure 11.6 shows an example of such introduction of LUTs. In this figure $N = 2$. In the experiments described in Sect. 11.4, N is set to 5. This number is determined through experiments. If the number is larger, there are more chances for the success of corrections. On the other hand, if the number is smaller, we can expect faster processing time.

There can be cases where any correction cannot be found for a given implementation with LUTs. There can be varieties of reasons on the failure. It may be due to the wrong selection of the target gates to be replaced, the inputs to LUTs are not sufficient, or other reasons. In this section, we assume that bugs (or portions that are implemented differently from designers' intention or specification) really exist within the given candidate locations. And, we may need to add more variables to the inputs of the LUTs to increase the chances of corrections, which are discussed in the next subsection.

Adding Variables to LUT Inputs

As mentioned above, there are bugs that cannot be corrected with LUTs having the same set of input variables as their original gates, if so-called "missing wire" bugs in Abadir's model [10] are happening. Figure 11.7 shows a simple example. In this example, the logic function of an implementation generates $A \wedge B \wedge C$, while its specification is $A \vee B \vee C \vee D$. With a LUT whose inputs are A, B, C that replaces the original AND gate in the incorrect implementation, we cannot get any configuration of its truth table for correction, since D is essential to the correct logic function. In general, assuming that bugs really exist within the gates that are replaced with LUTs, the reason why we cannot obtain any correction is due to the lack of variables that should be connected to appropriate LUTs. Therefore, what we

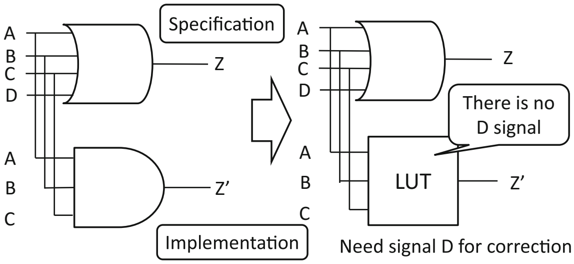


Fig. 11.7 An example bug that cannot be corrected with LUTs having the same inputs

need to do in the refinement phase in Fig. 11.5 is adding extra variables to LUT inputs and try to find a correction again. If we inappropriately add a set of variables to input of some LUTs, however, it simply results in no solution in the next iteration of the loop in Fig. 11.5. The number of ways to add extra variables to input of LUTs is large, which cannot be checked one by one in practice. In our method, we try to correct the implementation with adding as small numbers of variables as possible. First, all possible ways to add one variable to LUTs are tried. If no correction can be found, then the method looks for correction with two additional variables to one or two LUTs. Basically, we continue this process until we find corrections.

Using MUXs to Examine Multiple Additional Variables

As discussed above, the method looks for any correction with adding variables to the inputs of LUTs. Even if only one variable is added to the input of some LUT, we need to iterate the loop in Fig. 11.5 many times until any correction is found or there is a proof of no solution. For a large circuit, the number of iterations may be too large even for the case of adding one variable to a LUT. To make this process more efficient, we introduce a multiplexer and connect multiple variables, which are candidates to be added to a LUT, to its inputs. The output of the MUX and the additional input of the LUT are connected as shown in Fig. 11.8. Then, we can select which variable to be added to the LUT by appropriately assigning values to the control variables of the MUX.

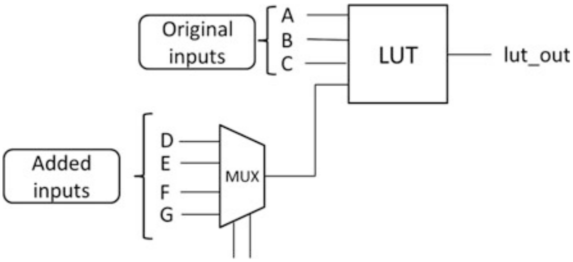


Fig. 11.8 Additional input variables to a LUT

Figure 11.8 shows how multiplexers work for examining candidate variables that may need to be added to the inputs of the LUT in order to get a correction. The LUT in the example originally has three inputs, $A, B,$ and C, which means this LUT is supposed to be replaced with some 3-input logic gate for corrections. Assume that we want to examine which variable to be added as an input of the LUT, using the MUX in the example, we can examine four additional candidate variables, $D, E, F,$ and G at one iteration. Here, we need to treat the control variables as program variables, that is, same as the ones in the LUTs. If any correction is found, the corresponding values of the control variables identify a variable for addition. That is, if it becomes an input of the LUT connected to the MUX, the implementation can be equivalent to its specification. Otherwise, all variables connected to inputs of the LUT cannot make the incorrect implementation equivalent to its specification. A straightforward way to realize something similar is to introduce LUTs having larger numbers of inputs rather than using MUX. This is definitely more powerful in terms of the numbers of function which can be realized at the output of the LUTs. In the example shown in Fig. 11.8, instead of using a MUX, a LUT having seven inputs may be used, and that LUT can provide much more different functions for possible corrections. The problem, however, is the number of required program variables. If we use a MUX in the example, we need $2^4 + 2 = 18$ variables. If we use a seven-input LUT, however, we need $2^7 = 128$ variables, which needs significantly more time to process.

Even when MUXs are used to examine multiple variables at the same time, we should be aware of the increase of the number of program variables. As can be seen in [4, 5], the number of program variables increases runtime for finding a correction, which corresponds to the runtime spent for each iteration of the loop in Fig. 11.5. Please note that one iteration in Fig. 11.5 may include many iterations in Fig. 11.4. In the experiments, we show a case study with varieties of numbers of inputs to MUX.

Filtering Out Variables Based on Necessary Condition

When a variable is added to an input of a LUT, it may not be an appropriate variable to correct the target bug. Even with the more efficient method using MUXs described above, we should not try to examine a variable which cannot correct the bug. In this subsection, we propose a method for filtering out such non-useful variables from the set of candidate variables that can be connected to inputs of LUTs utilizing necessary conditions on the correctability.

Necessary Condition for the Variables to Be Added

For simplicity, the following discussion assumes that there is one LUT added to an implementation circuit. It can be easily extended to the cases of a set of multiple LUTs, where each LUT does not have any other LUTs in its fan-in cone (i.e., an

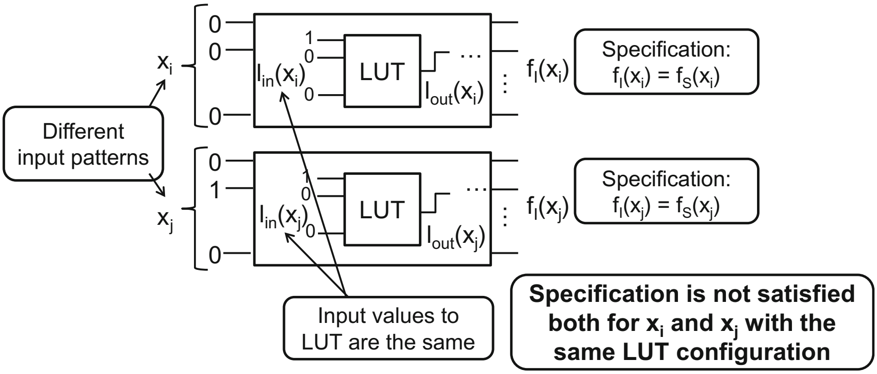


Fig. 11.9 Reason of no correction

LUT depends on other LUTs). However, we here omit such cases. When no correction is found, which corresponds to taking "NO" branch in Fig. 11.5, we cannot correct an implementation under debugging with the current LUT, which is the only LUT added, with its current input variables. The reason why there is no correction (i.e., no configuration of LUTs works correctly) is that the LUT outputs the same value for different two input values to the LUT. This happens when "No solution" is reached in Fig. 11.4. Figure 11.9 explains the situation. In the figure, x_i is an input pattern added in one of the previous iterations of the process shown in Fig. 11.4, and x_j is the pattern that is added as a result of the last iteration. Then, there can be situations where the following two conditions are satisfied.

1. For a pair of primary input patterns x_i and x_j, the input values to the LUT $l_{in}(x_i)$ and $l_{in}(x_j)$ are the same, where l_{in} represents a logic function that determines an input value to the LUT for a given primary input pattern. Therefore, the output values from the LUT are also the same, that is, $l_{out}(x_i) = l_{out}(x_j)$.
2. In order to make the implementation equivalent to the specification for both x_i and x_j, that is, $f_I(x_i) = f_S(x_i) \wedge f_I(x_j) = f_S(x_j)$, $l_{out}(x_i)$ and $l_{out}(x_j)$ must be different, where f_S, f_I denote logic functions of primary outputs of the specification and the implementation, respectively.

Note that $f_S(x_i)$ can be a different value from that of $f_S(x_j)$. With the conditions, there is no way to have an LUT configuration that satisfies the specification for both x_i and x_j at the same time. In this case, it cannot make an LUT configuration for both x_i and x_j if we add a variable v to the LUT that has the same value for x_i and x_j ($v(x_i) = v(x_j)$), since $l_{out}(x_i)$ and $l_{out}(x_j)$ are still the same. This is because the output of the LUT can be represented as $l_{out}(l_{in}(x), v(x))$ for a primary input pattern x and $l_{in}(x_i) = l_{in}(x_j) \wedge v(x_i) = v(x_j)$ implies l_{out} are equivalent for x_i and x_j for any configuration of the LUT.

The observation above suggests that we must not add a variable to the LUT input if it has the same value for x_i and x_j. It gives us a necessary condition that the added

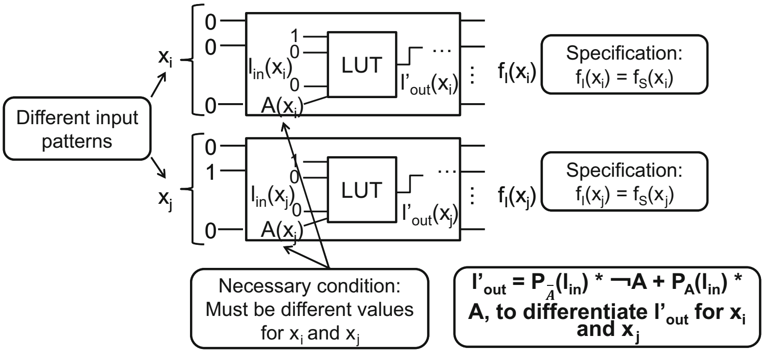

x_i
0
0
0
1
0
0
l_in(x_i)
LUT
l'_out(x_i)
A(x_i)
f_I(x_i)
Specification: f_I(x_i) = f_S(x_i)
Different input patterns
x_j
0
1
0
1
0
0
l_in(x_j)
LUT
l'_out(x_j)
A(x_j)
f_I(x_j)
Specification: f_I(x_j) = f_S(x_j)
Necessary condition: Must be different values for x_i and x_j
l'_out = P_Ā(l_in) * ¬A + P_A(l_in) * A, to differentiate l'_out for x_i and x_j

Fig. 11.10 Adding a variable satisfying a necessary condition

variable to a LUT must have different values for x_i and x_j. If this necessary condition is satisfied, there is a LUT configuration where $l_{out}(x_i) \neq l_{out}(x_j)$ is satisfied, which is a requirement to make $f_S = f_I$ for both x_i and x_j. Note that $f_S = f_I$ may not be satisfied even l_{out} is different for the two patterns.

Figure 11.10 shows how to make the output of the LUT different by adding a variable that satisfies the necessary condition. Here, we denote the added variable to the LUT as $A(x)$, where x is the primary input variables. An LUT configuration with its input $l_{in}(x)$ and $A(x)$ is represented by $l'_{out}(x)$, which is rewritten as $l'_{out}(x) = P_{\bar{A}}(l_{in}) * \bar{A} + P_A(l_{in}) * A$, where $P_{\bar{A}}(l_{in})$ and $P_A(l_{in})$ represent truth table values for l_{in} when $A = 0$ and $A = 1$, respectively. This is nothing but Shannon's expansion of l'_{out}. If the added variable $A(x)$ that satisfies the necessary condition takes 1 for x_i and 0 for x_j, we can make a LUT configuration satisfying $l'_{out}(x_i) \neq l'_{out}(x_j)$ by setting the two truth tables $P_{\bar{A}}$ and P_A appropriately. For the case of $x_i = 0$ and $x_j = 1$, a LUT configuration can be obtained in a similar way.

Based on the discussion above, we can filter out variables from candidates when they have the same value for both x_i and x_j. Now, we show an example of such filtering. Figure 11.11a is the specification which is $Z = A \vee B \vee C \vee D$. Here, we assume that this is one of the specifications and there are other outputs in the target circuit. Now, assume that a wrong implementation is generated as shown in Fig. 11.11b. Here the output only depends only on C and D, which is clearly wrong. For the input values where all of inputs are 0, this implementation looks correct as it generate the same output value, 0, as the specification. Please note that the implementation has more gates in the circuit in order to realize the other outputs which are not shown in the figure.

Then, we find a counterexample, which is $A = 0, B = 1, C = 0, D = 0$ as shown in Fig. 11.12a. For these values, the correct output value is 1, but the value of the output in the implementation is 0 as seen from Fig. 11.12b. Our debugging method first replaces the suspicious gate, the OR gate, with a LUT as shown in Fig. 11.12c. Unfortunately, there is no configuration for the LUT which makes the implementation correct, and so we need to add a variable to the LUT. Now, we have two

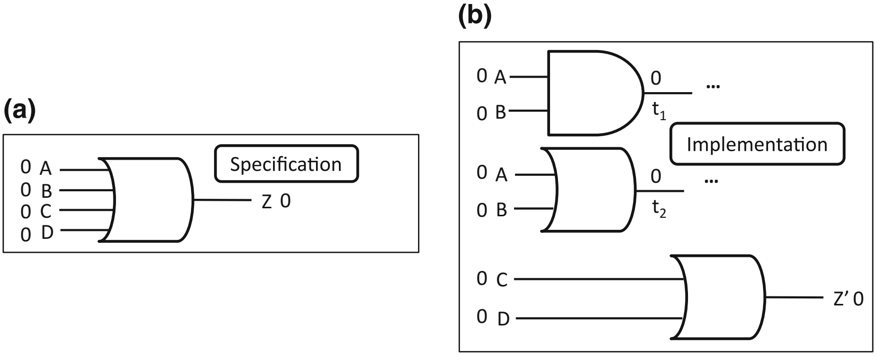


Fig. 11.11 An example specification and its buggy implementation

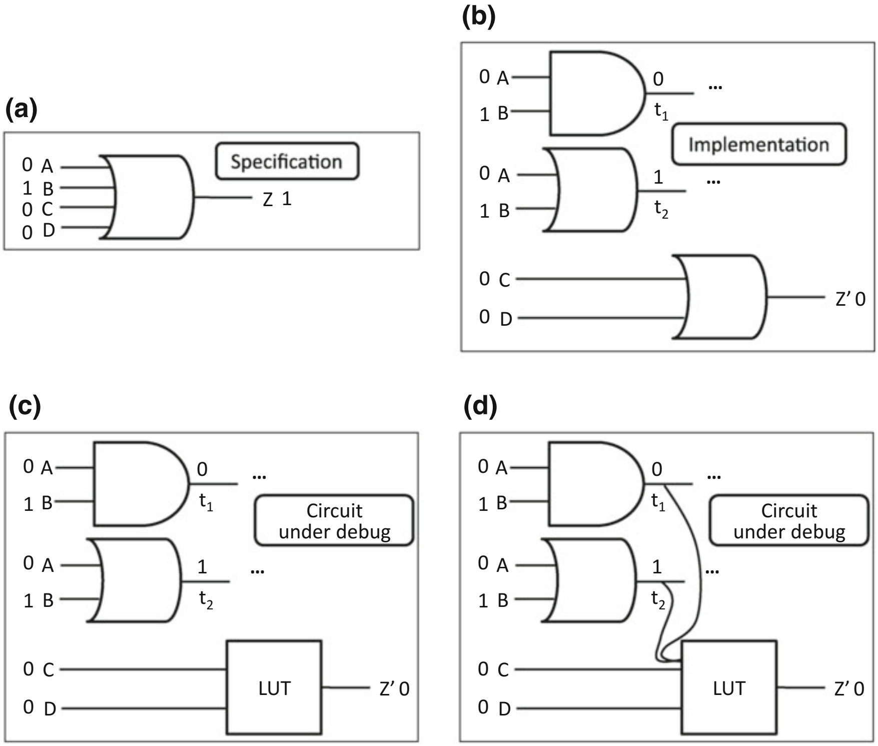


Fig. 11.12 A debugging process for the design in Fig. 11.9 with a necessary condition

candidates for the variable, t_1 and t_2 as shown in Fig. 11.12d. The necessary condition discussed above requires that the value of the variable must be different between the two cases, $A=0, B=0, C=0, D=0$ and $A=0, B=1, C=0, D=0$. From this condition, the variable t_1 is eliminated and the variable t_2 is selected.

An Improved Flow with Filtering Variables

Figure 11.13 shows an improved flow with filtering variables based on the necessary condition discussed above. When no correction is found for all the input patterns so far, the method searches for a set of variables that can be added to an LUT input. During this search, variables which do not satisfy the necessary condition are filtered out. This consists of the following two steps:

1. Find an input pattern x_i that is added in one of the previous iterations and has the same input values of an LUT as those of the lastly added pattern x_j.
2. Find a variable having different values for x_i and x_j.

As a result, the method tries to add a variable satisfying the necessary condition to some LUT input. Then, with the added LUT input, the method looks for another correction v by applying CEGAR-based method in [4, 5].

If this filtering method is applied with the method using MUXs to examine multiple variables simultaneously that is described above, the filtering method needs to pick up N variables, where N is the total number of input variables to MUXs.

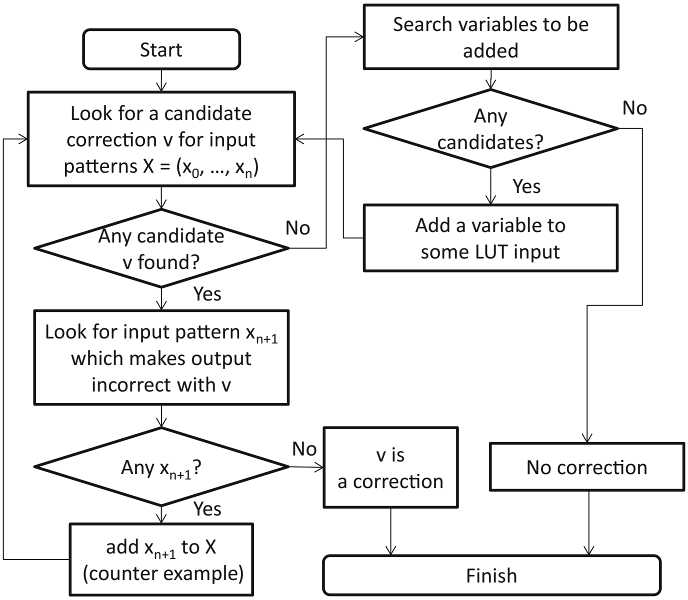

Start
Look for a candidate correction v for input patterns X = (x0, …, xn)
Any candidate v found?
No
Yes
Look for input pattern xn+1 which makes output incorrect with v
Any xn+1?
No
Yes
add xn+1 to X (counter example)
v is a correction
Search variables to be added
Any candidates?
No
Yes
Add a variable to some LUT input
No correction
Finish

Fig. 11.13 An bypass flow including filtering out variables

11.2.4 *Experimental Results*

11.2.4.1 Experimental Setup

Three sets of experiments are conducted in order to evaluate our debugging methods proposed in this paper. We use the following circuits for the experiments: ISCAS85 benchmark circuits, an industrial on-chip network circuit ("Industrial"), and an ARM Cortex microprocessor ("ARM processor"). While ISCAS85 circuits are combinational ones, the last two circuits are sequential ones. All are in gate-level designs. Table 11.1 shows the characteristics of these circuits. In order to apply our method, sequential circuits need to be time-frame expanded. The numbers of expanded time-frames (i.e., clock cycles for examinations) are shown in the second column for Industrial and ARM processor.

We use PicoSAT [11] as a SAT solver. In order to convert the netlists written in Verilog into SAT formulae, we use ABC [12] and AIGER [13]. All experiments reported in this section are run on a computer with Intel Core 2 Duo 3.33 GHz CPU and 4 GB Memory.

11.2.4.2 Simultaneous Examination on Multiple Variables Using Multiplexers

First, we perform an experiment with our method that introduces multiplexers (MUXs) into a circuit under debugging so that multiple extra variables are connected to LUTS through MUXs. In this experiment, we identify the erroneous primary outputs through simulation, and replace all gates in their logic cones within the depth of 5 levels from the erroneous primary outputs with LUTs. Then, we

Table 11.1 Characteristics of circuits

	# of expansion	Inputs	Outputs	Gates
ISCAS85 benchmarks				
c499		202	41	32
c880		383	60	26
c1355		546	41	32
c1908		880	33	25
c2670		1193	233	140
c3540		1669	50	22
c5315		2307	178	123
c7552		3512	207	108
Others				
Industrial	3	1201	1216	8289
ARM processor	1	895	923	4666

Table 11.2 Experimental results of simultaneous examination of candidate variables using MUXs

	Inputs of MUX	Change inputs	Time (s)
Industrial	1 (no MUXs)	–	Timeout (–)
	16	15	5281
	64	4	12794
	256	1	211
ARM processor	1 (no MUXs)	–	Timeout (–)
	16	8	11204
	64	2	8857
	256	1	5909

insert a N-input MUX to the circuit, and its output is connected to all LUTs. We randomly choose sets of variables out of all primary inputs of the circuit to be debugged, and they are connected to the inputs of MUXs.

If no solution for correction can be found, we replace all the input variables to MUXs with another set of variables that are not examined yet and execute the method again. In this experiment, the runtime is limited within 5 hours.

The results are shown in Table 11.2. N, the number of inputs to MUX, varies from 1 to 256. $N = 1$ means no MUX, in other words, a variable is directly added to an input of all LUTs. "Change inputs" represents the number of variable sets that are examined for correction. If this number is M, $N \times M$ variables are examined in total. As can be seen in the table, we need to run the method in [4, 5] only a few times when the number of MUX inputs is 64 or 256. "Time" shows the total runtime. We can see that the runtime for 256-input MUX is the shortest in both circuits. Also, it is notable that we cannot find a correction within 5 hours without MUX, since a lot of iterations are performed in order to check many variables one by one.

11.2.4.3 Candidate Variable Filtering Using the Necessary Condition

Next, we experiment our method to search for candidate variables that can be added to LUT inputs for a correction of the circuits. The method is based on the necessary condition discussed in Sect. 11.3.3. In this experiment, only an incorrect gate is replaced with an LUT. The candidates of variables are all variables in the circuit under debugging. For this experiment, we need to record the values of internal variables for all input patterns. For this purpose, we use Icarus Verilog simulator [14].

The results are shown in Table 11.3. In this experiment, there is no MUX inserted for the examination of multiple variables at once. Instead each variable is examined one by one. From the table, we can see only small numbers of iterations are required until getting corrections. Comparing to the results in Table 11.2 with

Table 11.3 Experimental results of filtering candidate variables based on the necessary condition

	Changed inputs	Time (s)
Industrial	29	524
ARM processor	24	293

$N = 1$, where any correction is not obtained within 5 h, the proposed filtering method based on the necessary condition makes the execution time much shorter. It implies that a large number of variables examined in the results shown in Table 11.2 do not satisfy the necessary condition. That is, the necessary condition works very well as filtering.

11.2.4.4 Applying Both Multiple Variable Examination and Candidate Filtering

In the previous experiments, we evaluate our proposed methods for finding variables which can rectify circuits when added to LUT input. That is, simultaneous examination of multiple candidate variables using MUXs and filtering candidate variables based on necessary condition are applied. In this section, we see the effects of applying both of the methods at the same time. For this experiment, we use ISCAS85 circuits and Industrial circuit.

For the experiment, one gate in each ISCAS circuit is replaced with a LUT, and one of its inputs is removed from the LUT. As a result, we realize cases where a potentially buggy gate is replaced with a LUT, but it lacks one input for rectification because we intentionally remove it. The gate replaced with a LUT and a variable to be removed are randomly chosen, and we make five instances for each ISCAS circuit. For Industrial circuit, we replace one of the buggy gates with a LUT. This replaced LUT needs one more input for rectification (without intentionally removing one of its original input) as the original circuit is buggy.

We apply the following three methods for each instance.

- **(PI)** Examining all primary input variables one by one until one can rectify the circuit.
- **(Filtering)** Examining only primary input and internal variables one by one which satisfies the necessary condition discussed in Sect. 11.3.3.
- **(Filtering + MUX)** Examining multiple variables which satisfy the necessary condition using MUX.

The results are shown in Table 11.4. In the table, # of var, Rectified, and # of examined represent the total number of candidate variables, (the number of successfully rectified)/(the total number of instances), and the average number of examined variables in successfully rectified cases, respectively. When # of examined is N/A, it means that none of the experiment instances can be rectified by the corresponding method. Ratio means the ratio of the number of examined variables

Table 11.4 Experimental results of applying both of our proposed method

Circuit	# of var	Method	Rectified	# of examined (ratio)	Runtime (s)
c499	243	PI	0/5	N/A	46.4
		Filtering	5/5	88.6 (36%)	48.3
		Filtering + MUX	5/5	88.6 (36%)	2.3
c880	443	PI	1/5	61.0 (14%)	80.8
		Filtering	5/5	54.2 (12%)	57.0
		Filtering + MUX	5/5	54.2 (12%)	2.6
c1355	587	PI	0/5	N/A	60.6
		Filtering	5/5	155.8 (27%)	227.7
		Filtering + MUX	5/5	155.8 (27%)	3.3
c1908	911	PI	2/5	34.0 (4.0%)	69.2
		Filtering	5/5	194.2 (21%)	284.5
		Filtering + MUX	5/5	194.2 (21%)	3.9
c2670	1194	PI	0/5	N/A	708.1
		Filtering	5/5	142.2 (12%)	83.2
		Filtering + MUX	5/5	142.2 (12%)	4.7
c3540	1670	PI	0/5	N/A	154.9
		Filtering	5/5	503.8 (30%)	915.9
		Filtering + MUX	5/5	503.8 (30%)	7.8
c5315	2476	PI	0/5	N/A	915.5
		Filtering	5/5	324.6 (13%)	268.1
		Filtering + MUX	5/5	324.6 (13%)	8.8
c7552	3604	PI	0/5	N/A	1484.3
		Filtering	5/5	1016.0 (28%)	3990.1
		Filtering + MUX	5/5	1016.0 (28%)	15.9
Industrial	3209	PI	0/1	N/A	Time out
		Filtering	1/1	100 (3.1%)	972.3
		Filtering + MUX	1/1	100 (3.1%)	172.5

with filtering to the total number of variables. Runtime in the table is the average runtime of the experimented instances.

From the table, we can see the following.

- When we want to rectify circuits utilizing programmability of LUT and one additional input to LUT, we need to add some internal variables (not primary input variables) to the LUT.
- When applying the filtering method to filter out variables not satisfying the necessary condition, we can reduce the numbers of examined candidates to 10–30% of the total variables.
- Examining multiple candidates simultaneously using MUXs reduces the runtime significantly.

11.2.5 Summary and Future Works

In this paper, we have proposed debugging methods for gate-level circuits applying partial synthesis techniques shown in [4, 5]. In the methods, possible bug locations, which may be given from bug locating methods, are replaced with LUTs, and a configuration of LUTs that makes an implementation under debugging and its specification equivalent is searched. To deal with the missing input variables to LUTs, we have also proposed methods to examine variables for LUT inputs in trial-and-error manner. Using MUXs, multiple variables are examined simultaneously, which largely reduces the number of iterations of the process. In addition, we have introduced a necessary condition that variables added to LUT inputs must be satisfied, so that variables not satisfying the condition can be removed quickly from the candidates. Through the experiments with ARM processor design, on-chip network controller taken from industry, and benchmark circuits, both of our proposals can significantly speed-up the process to get a correction (i.e., an appropriate configuration of LUTs to make an incorrect implementation correct).

We have also discussed about possible extensions of our proposed method in order to introduce sub-circuits having relatively larger numbers of inputs, such as 12 inputs to the buggy locations of the design under debugging. For such large numbers of inputs, it is not practical to represent the entire sub-circuit with a single 12-input LUT. Instead, we have discussed about the introduction of decomposition of such sub-circuits with sets of LUTs having much smaller numbers of inputs. Definitely, this is a very preliminary discussion and much of following works are expected.

As a future work, we plan to develop a method to reduce the candidate variables based on the necessary condition discussed in this paper for the cases where LUTs are dependent with each other. In such cases, the necessary condition may need to be refined to deal with dependency.

11.3 High-Quality Delay Testing for In-field Self-test

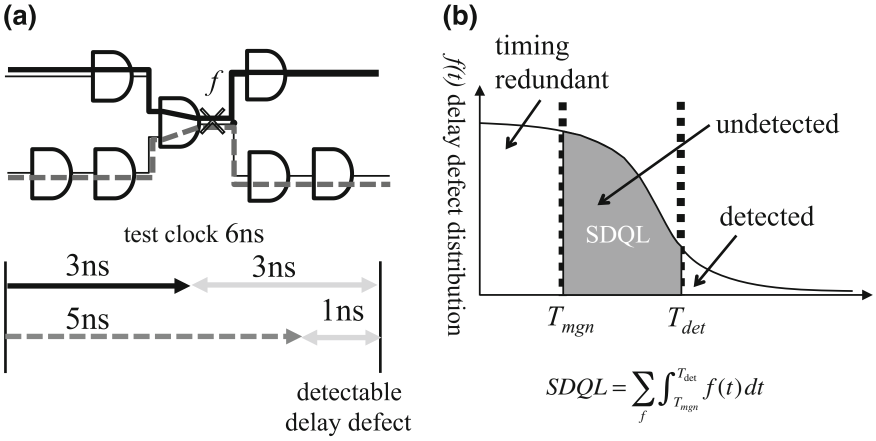
Michiko Inoue, Nara Institute of Science and Technology

Tomokazu Yoneda, Nara Institute of Science and Technology

11.3.1 Statistical Delay Quality Level SDQL

Built-In Self-Test (BIST) is an embedded component in a circuit that can apply self-test to the circuit itself. Since it is embedded in a circuit, it can be used to apply in-field test and contribute to improve the reliability of the circuit. BIST for high-quality delay test that detects small delay defects is effective not only to improve test quality of production test but also to efficiently and less costly realize failure prediction in field. This subsection introduces a method to improve test quality while reducing test data volume and test application time for BIST to be used in field. Failure prediction method by delay measurement using in-field BIST has been proposed [15]. To practically realize BIST in field, it is required to provide high-quality delay test under strict constraints on test data volume and test application time.

Statistical Delay Quality Level (SDQL) is proposed to evaluate delay test quality for small delay defects [16]. Intuitively, SDQL represents an amount of delay defects that can escape from detection by a given test set. Therefore, smaller SDQL means better test quality. For a given circuit, SDQL of a test set represents a total amount of delay defects that have to be detected but cannot be detected by the test set. Figure 11.14 shows a concept of SDQL. In Fig. 11.14a, there are two paths that pass through a delay fault f, where the lengths of the paths are 3 ns and 5 ns, respectively. If the path with length of 3 ns is sensitized by some test pattern (by propagating a transition through the path) with test clock of 6 ns, f is detected if the delay defect size exceeds 3 ns, while a delay defect exceeding 1 ns is detected if a different test pattern sensitizes the path with length of 5 ns. That is detectable delay defect size depends on test patterns. Suppose that the smallest detectable delay defect for f is 1 ns, that is, delay defect less than 1 ns is timing redundant and does not need to be detected. If the smallest detectable delay defect for f by a given test set is 3 ns, delay defect whose size is between 1 and 3 ns is escaped from the test. SDQL is a total amount of such test escapes over the all faults by considering a delay defect distribution (Fig. 11.14b).



$$SDQL = \sum_{f} \int_{T_{mgn}}^{T_{\det}} f(t)\, dt$$

Fig. 11.14 Statistical delay quality level (SDQL)

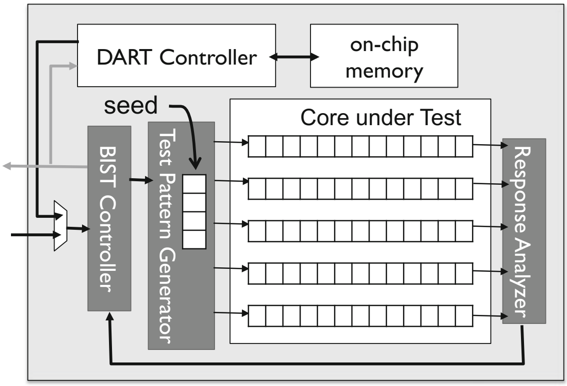


Fig. 11.15 In-field built-in self-test

11.3.2 In-field Test Using BIST

Failure prediction method using in-field BIST has been proposed [15], where in-field delay measurement is implemented by controlling BIST circuitry from on-chip DART controller (Fig. 11.15). Delay test is applied several times using different test clock frequencies, and actual delay is narrowed down between PASS and FAIL test clock frequencies.

BIST generates one deterministic and multiple pseudo-random test patterns from one seed, and therefore, frequent re-seedings can achieve high test quality with short test application time. However, frequent re-seedings require more test data volume, and test data such as seeds and the corresponding expected signatures should be stored in on-chip memory. In-field test has several constraints on on-chip memory and test application time, and therefore, small number of seeds with high delay test quality is required for accurate in-field delay measurement.

11.3.3 Seed Selection for High-Quality Delay Test

Test pattern selection [17] and seed selection [18] for high delay test quality based on SDQL have been proposed. Figure 11.16 shows a flow of seed selection [18]. In this method, first, given test patterns are translated into seeds. Then seeds are sorted in the order so that SDQL is decreased (improved) as early as possible. The ordered seeds can be used to minimize the number of seeds under a constraint on test quality, or to maximize test quality (minimize SDQL) under a constraint on the number of seeds. Seeds are selected in the obtained order while a selected seed set satisfies a given constraint.

Seed ordering can be done by selecting test patterns one by one by repeatedly obtaining SDQL using timing-aware fault simulation. However, it is unpractical since timing-aware fault simulation is too time consuming. Seed ordering [18] is

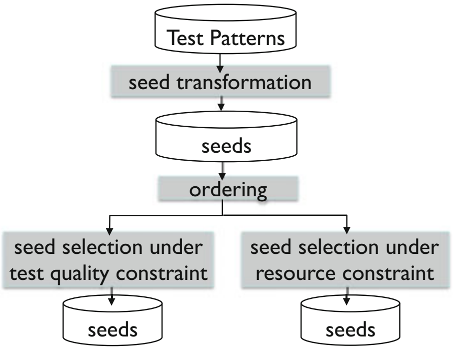

Test Patterns
seed transformation
seeds
ordering
seed selection under test quality constraint
seed selection under resource constraint
seeds
seeds

Fig. 11.16 Seed selection for high-quality delay test

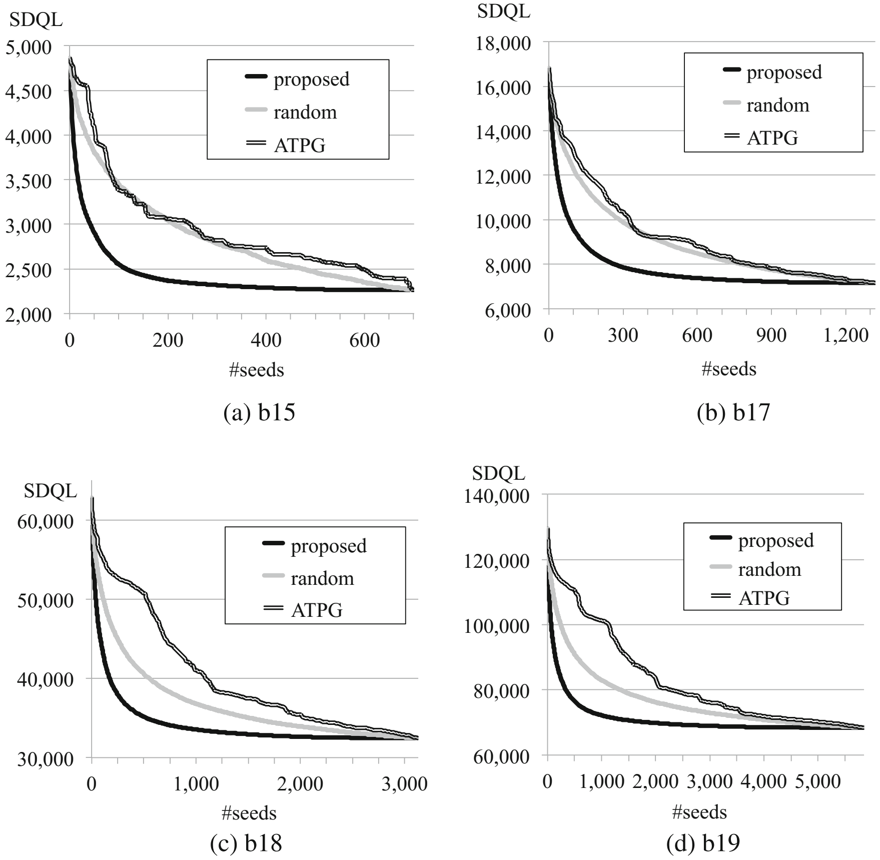
accelerated by using lengths of sensitized paths (T_{det} in Fig. 11.14b) instead of actual SDQL values. In the proposed method, first lengths of sensitized paths for all the faults are obtained for each seed. Then seeds are selected one by one based on the obtained lengths of sensitized paths. Timing-aware fault simulation is required for once as a preprocessing in the first step, and it can order a given test pattern set in a reasonable time.

Experiments have been conducted for several ITC'99 benchmark circuits. Synopsys TetraMAX ATPG with Small Delay Defect Test mode [19] is used for timing-aware test generation and fault simulation. Table 11.5 shows the characteristics of the circuits and the results of test pattern generation and seed transformation and ordering. The columns "# test patterns", "# seeds" show the number of test pattern generated by TetraMAX, and the number of seeds transformed from the test patterns. Test patterns generated by timing-aware ATPG and n-detect test patterns targeting transition faults are preliminarily compared, and timing-aware ATPG is adopted to obtain better SDQL with a smaller number of seeds. The columns "FC (%)", "SDQL", and "TGT (m)" show transition fault coverage, SDQL, and test generation time for the test patterns, respectively, and "ordering time (m)" show processing time for seed ordering. The results show that the proposed method efficiently orders the seeds.

Figure 11.17 shows the effectiveness of the proposed method. The figure compares SDQL transitions among the proposed seed ordering, random ordering, and an original ATPG order. The proposed seed ordering achieves less (better) SDQL with a smaller number of seeds. Tables 11.6 and 11.7 show some examples

Table 11.5 Circuit characteristics, results of test generation, seed transformation, and ordering

Circuit	# gates	# faults	# FFs	# scan chains	# test patterns	# seeds	FC (%)	SDQL	TGT (m)	Ordering time (m)
b15	8,985	17,329	417	8	727	700	82.0	2498.0	1.89	0.6
b17	27,766	65,218	1,317	26	1,375	1,319	86.2	7841.8	9.18	2.3
b18	79,400	172,403	3,020	80	3,293	3,129	79.7	33986.1	43.82	19.7
b19	152,599	353,301	6,042	120	6,131	5,850	79.0	70768.2	115.39	74.9



(a) b15

(b) b17

(c) b18

(d) b19

Fig. 11.17 SDQL transition

Table 11.6 The number of selected seeds under SDQL constraints

Circuit	b15		b17		b18		b19	
SDQL constraint	2,500	3,500	8,000	10,000	35,000	45,000	70,000	90,000
Proposed	116	17	266	81	525	85	1,875	146
Random	473	83	780	288	1,516	249	4,541	542
ATPG	597	88	816	328	2,049	707	5,139	1,486

of seed selection under SDQL constraints and seed count constraints, respectively. The number of seeds and SDQL are reduced by ordering seeds using the proposed method, especially when SDQL constraints are relatively large or seed count constraints are relatively small. These cases correspond to requirements of small

Table 11.7 SDQL of selected seeds under seed count constraints

Circuit	b15		b17		b18		b19	
# seeds constraint	100	200	500	1,000	500	1,500	500	1,500
Proposed	2,550	2,369	7,474	7,193	35,149	32,950	76,420	70,643
Random	3,443	3,044	8,826	7,566	40,555	35,047	90,964	78,917
ATPG	3,387	3,064	9,177	7,612	50,756	37,493	110,546	89,716

test data volume or short test application time. That is, the proposed seed ordering can be effectively used in in-field BIST environments.

There are some variations of the proposed method. A simplified version just targets transition fault coverage, where time-consuming fault simulation is not required and ordering can be done more efficiently. The proposed ordering method can be extended to handle mixed-mode BIST where one deterministic test pattern and multiple pseudo-random test patterns are generated from one seed. In an extended version of the proposed method, the longest sensitized paths are evaluated for each test pattern set generated from the same seed. These variations including the original version can give an adequate solution to meet several requirements such as test data volume (seed count), test quality (SDQL), and processing time.

11.4 Temperature-and-Voltage-Variation-Aware Test

Tomokazu Yoneda, Nara Institute of Science and Technology

Yuta Yamato, Nara Institute of Science and Technology

11.4.1 Thermal-Uniformity-Aware Test

In advanced technologies, temperature-induced delay variations during the test are as much as those caused by on-chip process variations [20]. Temperature difference within a chip can be as high as 50 °C and typical time intervals for temperature changes over time are very short time of milliseconds. Besides, the execution of online self-test may last for a long time [21]. For example, the extremely thorough test patterns that specifically target aging [22] may take several seconds to complete. This indicates that, for accurate aging prediction, we need to embed a lot of temperature sensors into several locations within a chip to collect spatially and temporally temperature profile during. However, this is not the cost-effective solution since it incurs a lot of overhead. Even if we could accept the overhead, it requires (1) a lot of data to be stored in the memory and (2) a complex procedure to eliminate the temperature-induced delay variations from the measured delay values

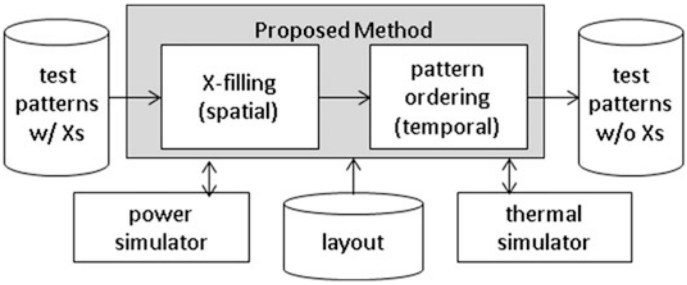


Fig. 11.18 Test pattern optimization flow

for aging analysis. Therefore, we need a cost-effective solution to eliminate the temperature-induced delay variations for accurate aging prediction.

Yoneda et al. proposed a test pattern optimization method to reduce the spatial and temporal temperature-induced delay variations. The proposed method consists of the following two steps: (1) X-filling [23] and (2) test pattern ordering [24] as shown in Fig. 11.18.

11.4.1.1 X-filling for Spatial-Thermal-Uniformity

The proposed method starts with a test sequence including unspecified bits (X's) generated by a commercial ATPG. As the first step, the thermal-uniformity-aware X-filling technique [23] is performed to obtain a test sequence of test patterns with fully specified bits. For each test pattern i together with the test response of $i - 1$, the Xs are specified so as to minimize the spatial temperature variance during scan shift operation while preserving the power consumption at relatively low level. Figure 11.19 shows the temperature profile for ITC'99 benchmark b17 after Step 1. In this example, the circuit was divided into 16 blocks based on the layout and each line on the graph represents the temperature profile of a block. Compared to the temperature profiles of the test patterns with minimum transition fill (conventional low power patterns) in Fig. 11.20, the spatial temperature variation is reduced significantly. However, temporal temperature variations (around 20 °C in this example) are still remaining.

11.4.1.2 Test Pattern Ordering for Temporal Thermal Uniformity

The proposed test pattern ordering technique [24] determines an order of the fully specified test patterns so that the temporal temperature variance is minimized while preserving the spatial temperature variance achieved in the first step. The main idea is to adopt a sub-sequence-based ordering strategy. The method divides the test pattern sequence into several sub-sequences based on thermal simulation, and

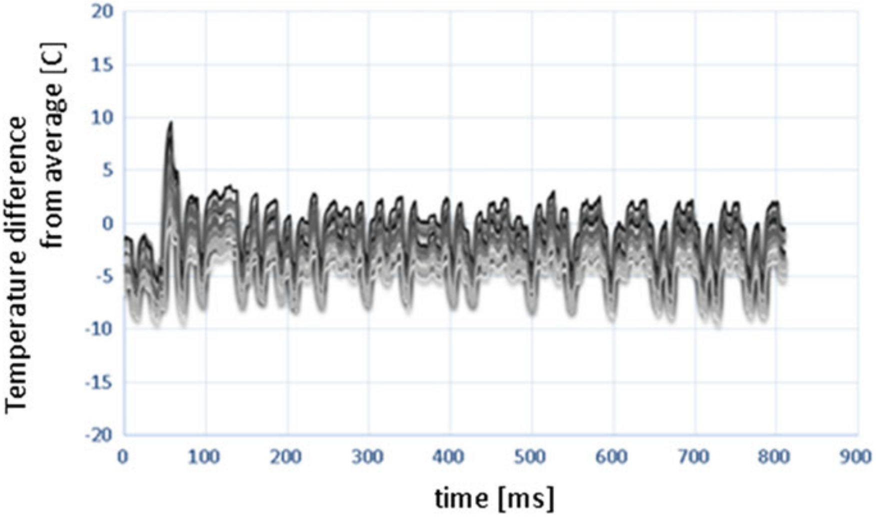


Fig. 11.19 Temperature variation in test patterns with thermal-uniformity-aware X-filling

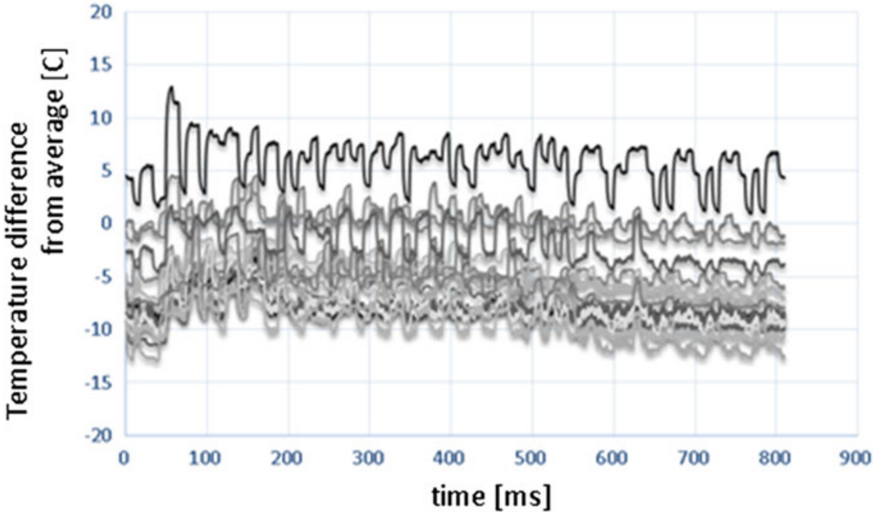


Fig. 11.20 Temperature variation in test patterns with minimum transition fill

orders the *heating* and *cooling* sub-sequences in an interleaving manner to reduce the temporal temperature variation. The spatial thermal-uniformity achieved in the first step is valid only for the current response-pattern pair which is simultaneously shifted during a test in the current order. Therefore, the sub-sequence-based ordering itself can preserve the spatial-thermal-uniformity without any consideration

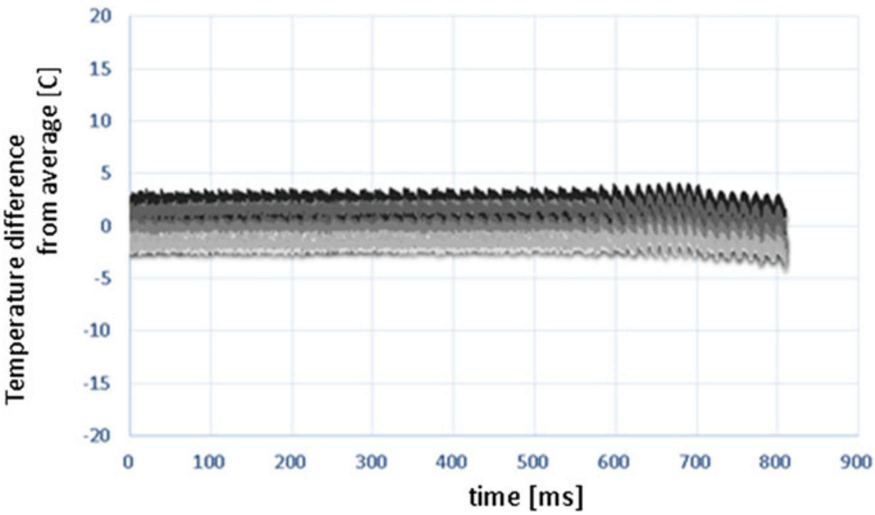


Fig. 11.21 Temperature variation in test patterns after thermal-uniformity-aware test pattern ordering

if the length of sub-sequences is long enough, and allow us to minimize the temporal temperature variance as shown in Fig. 11.21. Experimental results show that the proposed test pattern optimization method obtained 73% and 95% reductions in spatial and temporal temperature variation, respectively, on average for several ITC'99 benchmarks.

11.4.2 Fast IR-Drop Estimation for Test Pattern Validation

In addition to temperature, voltage is another main contributor to delay variation. Excessive voltage drop causes severe yield loss problems during delay test. Generally, delay testing is performed using scan design, a typical design for testability (DFT) technique. During scan testing, circuits operate with high switching activity since it causes state transitions which cannot occur during functional operation. In case that instantaneous switching activity is high, large current flows along power distribution network in a short period of time. This results in voltage decrease at power supply port of cell instances due to resistance of metal wires (IR-drop). Since IR-drop increases signal transition delay at cell instances, if cumulative delay increase on a sensitized path exceeds the specified timing margin, timing failure occurs. In such case, even functionally good chips may also fail the test and will not be shipped, i.e., yield loss. Therefore, test patterns that can cause excessive IR-drop should be identified and removed or modified before test application [25].

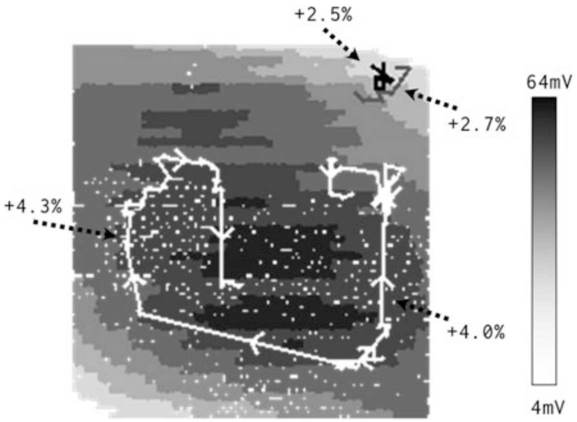


Fig. 11.22 Variation in path delay increase due to IR-drop

Figure 11.22 shows variation in delay increase of sensitized paths depending on the amount of IR-drop. It can be seen that paths running through the instances with high IR-drop suffers from higher delay increase. Based on this observation, it is necessary to compute the amount of IR-drop for every cell instance for each pattern to accurately evaluate test patterns. Though this is generally realized by precise circuit-level simulation, it usually takes long computation time and thus may be impractical for large industrial designs. On the other hand, evaluation using estimated power dissipation or signal switching count is much more scalable and widely used. However, since the length of sensitized paths differs depending on patterns even their power dissipations are similar, it can be difficult to directly evaluate the risk of IR-drop-induced timing failures.

To accurately evaluate test patterns in a realistic amount of time, the authors in [26] have proposed a fast pattern-dependent per-cell IR-drop estimation method. The basic idea is to reduce the number of time-consuming IR-drop analyses during entire analysis. General flow and the way to reduce the number of IR-drop analyses are described in the following subsections.

11.4.2.1 General Flow

Figure 11.23 shows a comparison between typical IR-drop analysis flow that performs IR-drop analysis for all patterns and the proposed flow. Differently, from the typical flow, the method first selects a few representative patterns as targets of IR-drop analysis. IR-drop analyses are performed only for the selected patterns. Then, fast IR-drop estimation function is derived for each cell instance using analyzed IR-drop and corresponding power profile. After that, IR-drop for the remaining patterns is computed using the functions.

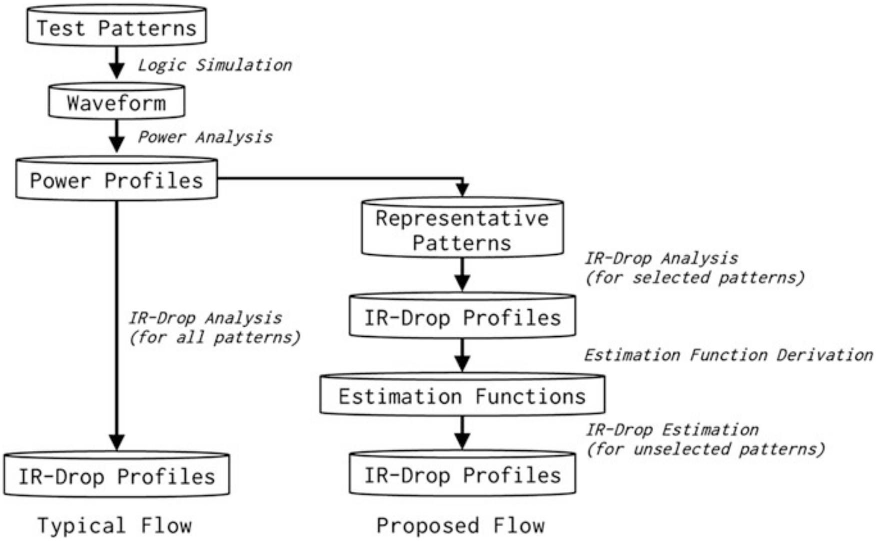


Fig. 11.23 Comparison between typical flow and proposed flow

11.4.2.2 Reducing Number of IR-Drop Analysis

The idea of reducing the number of IR-drop analyses is based on high correlation between circuit's average power dissipation over a clock cycle and IR-drop for each cell. As can be seen in Fig. 11.24, by focusing on individual cell instance,

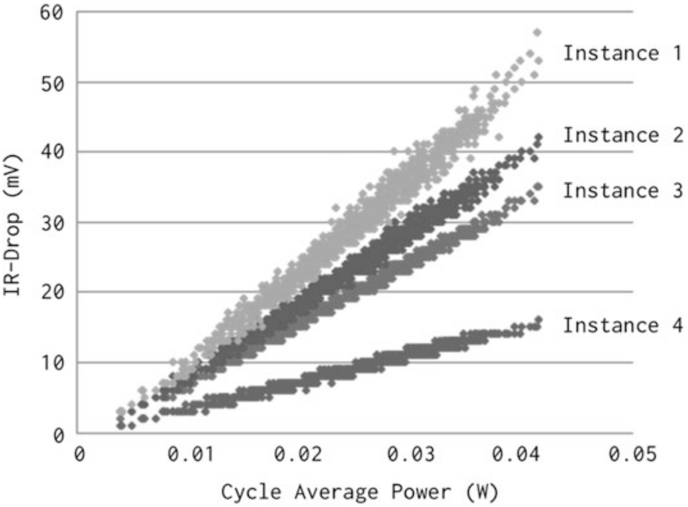


Fig. 11.24 Correlation between global cycle average power and individual cell instance

cycle average power and IR-drop has an almost linear correlation. The proposed method derives IR-drop estimation function for each cell by linear regression using a few IR-drop analysis results of representative patterns. For the remaining patterns, IR-drop for each cell instance can be computed using its cycle average power. Since the estimation functions are linear function, the computation effort is significantly reduced compared to IR-drop analysis.

Experimental results have shown that the proposed method achieves more than 20X speed-up to 6 mV error on average compared to typical flow.

References

1. IEEE Standard for SystemVerilog—Unified Hardware Design, Specification, and Verification Language, IEEE Std 1800 TM-2012, Chaps. 16, 19 (2012)
2. IEEE Standard for Property Specification Language (PSL), IEEE Std 1850TM-2005 (2005), pp. 101–111
3. M. Fahim Ali, A. Veneris, A. Smith, S. Safarpour, R. Drechsler, M. Abadir, Debugging sequential circuits using Boolean satisfiability, in *IEEE/ACM International Conference on Computer Aided Design, 2004. ICCAD-2004* (2004), pp. 204–209
4. S. Jo, T. Matsumoto, M. Fujit, SAT-based automatic rectification and debugging of combinational circuits with LUT insertions. *Test Symposium (ATS), 2012 IEEE 21st Asian* (2012), pp. 19–24
5. M. Fujita, S. Jo, S. Ono, T. Matsumoto, Partial synthesis through sampling with and without specification. ICCAD **2013**, 787–794 (2013)
6. M. Janota, J. Marques-Silva, Abstraction-based algorithm for 2QBF, in *Theory and Applications of Satisfiability Testing (SAT) 2011*. Lecture Notes in Computer Science, vol. 6695 (2011) pp. 230–244
7. M. Janota, W. Klieber, J. Marques-Silva, E. Clarke, Solving QBF with counterexample guided refinement, in *Theory and Applications of Satisfiability Testing (SAT) 2012*. Lecture Notes in Computer Science, vol. 7317 (2012), pp. 114–128
8. A. Ling, P. Singh, S.D. Brown, FPGA logic synthesis using quantified boolean satisfiability. SAT **2005**, 444–450 (2005)
9. A.S.-Lezama, L. Tancau, R. Bodik, S.A. Seshia, V.A. Saraswat, Combinatorial sketching for finite programs. *ASPLOS* (2006), pp. 404–415
10. M.S. Abadir, J. Ferguson, T.E. Kirkland, Logic design verification via test generation. IEEE Trans. Comput. Aided Design Integr. Circuits Syst. **7**(1), 138–148 (1988)
11. A. Biere, PicoSAT essentials. J. Satisfiability, Boolean Model. Comput. (JSAT) (2008), pp. 75–97
12. R. Brayton, A. Mishchenko, ABC: an academic industrial-strength verification tool. Comput. Aided Verif. **6174**, 24–40 (2010)
13. AIGER, http://fmv.jku.at/aiger/
14. Icarus Verilog, http://iverilog.icarus.com/
15. Y. Sato, S. Kajihara, T. Yoneda, K. Hatayama, M. Inoue, Y. Miura, S. Untake, T. Hasegawa, M. Sato, K. Shimamura, DART: dependable VLSI test architecture and its implementation, in *Proceedings IEEE International Test Conference* (2012), p. 15.2
16. Y. Sato, S. Hamada, T. Maeda, A. Takatori, Y. Nozuyama, S. Kajihara, Invisible delay quality-SDQM model lights up what could not be seen, in *Proceedings IEEE International Test Conference 2005* (IEEE, 2005) p. 47.1
17. M. Inoue, A. Taketani, T. Yoneda, H. Fujiwara, Test pattern ordering and selection for high quality test set under constraints. IEICE Trans. Inf. Syst. **95**(12), 3001–3009 (2012)

18. T. Yoneda, I. Inoue, A. Taketani, H. Fujiwara, Seed ordering and selection for high quality delay test, in *Proceedings IEEE Asia Test Symposium (ATS) 2010* (IEEE, 2010), pp. 313–318
19. TetraMAX ATPG User Guide, Version C-2009.06-SP2 (2009)
20. S.A. Bota, J.L. Rossello, C.D. Benito, A. Keshavarzi, J. Sequra, Impact of thermal gradients on clock skew and testing. IEEE Des. Test Comput. **23**(5), 414–424 (2006)
21. Y. Li, O. Mutlu, S. Mitra, Operating system scheduling for efficient online self-test in robust systems, *in Proceedings International Conference on Computer-Aided Design (ICCAD '09)* (Nov 2009), pp. 201–208
22. A.B. Baba, S. Mitra, Testing for transistor aging, in *Proceedings VLSI Test Symposium (VTS '09)* (May 2009), pp. 215–220
23. T. Yoneda, M. Inoue, Y. Sato, H. Fujiwara, Thermal-uniformity-aware X-filling to reduce temperature-induced delay variation for accurate at-speed testing, in *Proceedings VLSI Test Symposium (VTS '10)* (Apr 2010), pp. 188–193
24. T. Yoneda, M. Nakao, M. Inoue, Y. Sato, H. Fujiwara, Temperature-variation-aware test pattern optimization, in *European Test Symposium (ETS '11)* (May 2011), p. 214
25. P. Girard, Survey of low-power testing of VLSI circuits. IEEE Des. Test Comput. **19**, 80–90 (2002)
26. Y. Yamato, et al., A fast and accurate per-cell dynamic IR-drop estimation method for at-speed scan test pattern validation, in *Proceedings International Test Conference (ITC '12)*, paper 6.2 (2012)

Chapter 12
Unknown Threats and Provisions

Nobuyasu Kanekawa, Takashi Miyoshi, Masahiro Fujita, Takeshi Matsumoto, Hiroaki Yoshida, Satoshi Jo, Seiji Kajihara, Satoshi Ohtake, Masashi Imai, Tomohiro Yoneda, Hiroyuki Takizawa, Ye Gao, Masayuki Sato, Ryusuke Egawa and Hiroaki Kobayashi

Abstract It is hard to envision all possible use cases or environmental conditions that might happen to a VLSI system during its lifetime and could adversely affect its performance and/or dependability. The job of designing and testing a VLSI includes the challenge of being prepared even against problems hard to foresee, within the restrictions of practical cost and time. This chapter is intended to offer a perspective for unidentified future threats to dependability and provisions in design and test that could be taken to mitigate them. First of all, in Sect. 12.1, we look back

N. Kanekawa (✉)
Hitachi, Ltd., Hitachi, Japan
e-mail: nobuyasu.kanekawa.ef@hitachi.com

T. Miyoshi
Fujitsu Laboratories Ltd., Kawasaki, Japan

M. Fujita · S. Jo
The University of Tokyo, Tokyo, Japan

T. Matsumoto
Ishikawa National College of Technology, Tsubata, Ishikawa, Japan

H. Yoshida
Fujitsu Laboratories of America, Sunnyvale, CA, USA

S. Kajihara
Kyushu Institute of Technology, Iizuka, Japan

S. Ohtake
Oita University, Oita, Japan

M. Imai
Hirosaki University, Hirosaki, Japan
e-mail: miyabi@eit.hirosaki-u.ac.jp

T. Yoneda
National Institute of Informatics, Tokyo, Japan
e-mail: yoneda@nii.ac.jp

S. Asai (ed.), *VLSI Design and Test for Systems Dependability*,
https://doi.org/10.1007/978-4-431-56594-9_12

on the trend in the fault causes experienced over time, and discuss unidentified future threats and technical challenges. Section 12.2 takes up the cloud data center that provides IaaS (Infrastructure as a Service) as a typical electronic system requiring high levels of dependability from a few different subsystem perspectives, i.e., server, storage, and communications, and discusses relevant emerging requirements. In Sect. 12.3, the concept of "patchable hardware and rectification for post-Silicon validation" is introduced. Section 12.4 deals with collecting the field test data for preventive maintenance and potentially for post-failure analysis and future study based on the technology called DART (Dependable Architecture with Reliable Testing). Section 12.5 deals with the fault detection and reconfiguration method for multiple-core processor is discussed. Finally, in 12.6, checkpoint-restart for heterogeneous multiple processor systems is proposed as a standard procedure for dependability.

Keywords Unknown/Unidentified/Unpredicted threats · DART
Patchable hardware · Fault detection · Reconfiguration · Checkpoint-Restart
VLSI · Multiprocessor · Multicore · Data center · Cloud
IaaS

H. Takizawa · Y. Gao · M. Sato · R. Egawa · H. Kobayashi
Tohoku University, Sendai, Japan
e-mail: takizawa@tohoku.ac.jp

Y. Gao
e-mail: gaoye@tohoku.ac.jp

M. Sato
e-mail: masayuki@tohoku.ac.jp

R. Egawa
e-mail: egawa@tohoku.ac.jp

H. Kobayashi
e-mail: koba@tohoku.ac.jp

12.1 A Historical Review of Faults and Unidentified Future Problems

Nobuyasu Kanekawa, Hitachi, Ltd.

12.1.1 Introduction

The major causes of faults in the system using the VLSI (Very-Large-Scale Integrated circuit) have changed with the technological evolution and increase in the degree of integration.

It is our hope that a brief review of this history will be useful in trying to predict emerging threat and prepare countermeasure technology.

The motivation for the author to write a section in this book is having participated in the workshops and review meetings in the DVLSI (Dependable Very-Large-Scale Integrated circuit) research project several times and taken part in making up a plan for this publication as a volunteering participant. From this viewpoint, I have surveyed the change in the major causes of faults experienced in the past and contemplated future problems, hoping to be useful for future development.

12.1.2 The Change of the Fault Causes by the Ages

Figure 12.1 shows the change of the fault causes by the ages. The permanent fault in hardware was the major trouble causes in the early phases of the development of VLSI systems, and yet it relatively decreased with the progress and the popularization in quality control. Contrarily, design faults have increased in proportion with the increase in system scale and complexity [1].

The rule of thumb (rule learned by experience) called Moore's Law, [2] which means that the performance and integration of the semiconductor double every 1.5–2 years as shown by Fig. 12.2 is widely known.

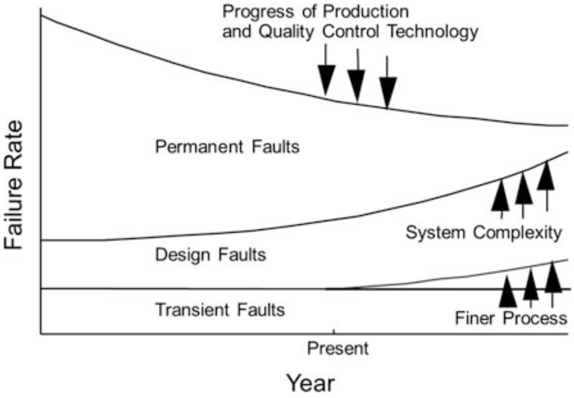


Fig. 12.1 Change of the fault causes by the era

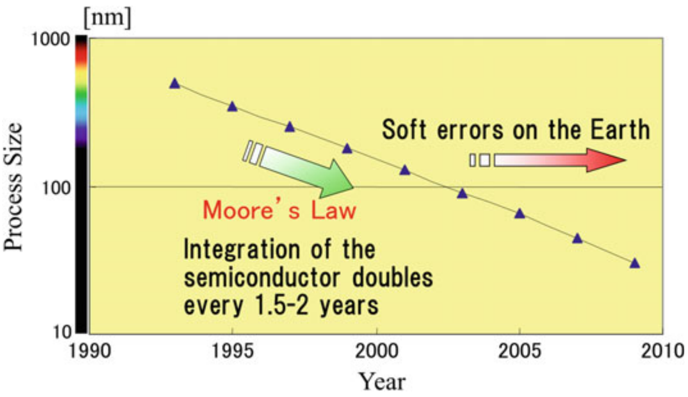


Fig. 12.2 Moore's law and soft error

Conventionally, it has been generally said that the soft error is caused at the terrestrial (ground) level by alpha rays that originate from the radioisotope in package materials and the solder.

More recently, soft error outbreak by cosmic rays (mainly neutron) was predicted on the ground level [3], and now it is a reality [4]. Not only increase of soft error occurrence by the miniaturization of the semiconductor process, but also increase of the system scale, namely the increase of the memory size in a system, has made the soft error issue a major problem, nowadays.

12.1.3 Future Problems (=Challenge)

Herewith, I enumerate the problems of the dependability technology that will be needed toward the future. These are the problems and challenges pursued in search for more ideal and demanding systems requirements.

(1) Effective fault recovery technique with the least penalty

A technique called redundancy is widely used as a usual countermeasure in order to attain high reliability in the electronic system. However, it has to be noticed that redundancy leads to increase in power consumption, chip area, and costs. Therefore, it is an ideal to be able to minimize these penalties.

(2) Automatic logic synthesis, routing, and layout technology (tools) for dependability

It is an ideal that redundancy can be implemented automatically by automatic logic synthesis, routing, and layout.

(3) Protection and circumvention against the noise from a power supply and the global signal line (Ref. Chap. 4 of this book.)

(4) Fault tolerance of the power supply

EMC characteristics and stability of power supply is indispensable to guarantee the steady operation of the system. (Ref. Chap. 4 of this book.)

(5) Human factor (error, intentional attack, tampering) countermeasures

Not only countermeasures to the human fault but also security, or countermeasures against malicious attacks on systems need to be addressed as an important issue for securing the reliability of the system.

(6) Discrimination of transient faults and intermittent faults

Conventionally, corrective maintenance, or acting in response to a failure, has been the dominant way to a countermeasure against faults of the semiconductor. Technology such as the DART [5] will make it possible to realize the concept of preventive maintenance in the presence of a predicted fault that progresses in the Arrhenius deterioration process.

Moreover, it is indicated by the DART technology that the fault forecasting and preventive maintenance are enabled if discrimination of transient faults and intermittent faults is made possible because intermittent faults may become the harbinger of permanent faults. And the occurrence of transient faults obeys Poisson distribution, where the occurrence of intermittent faults does not obey.

Furthermore, if the diagnostic functions such as the DART technology is built in many LSIs to collect massive fault data in the field, it is expected that the analysis of the big data will or data mining will provide useful knowledge for future, more dependable, designs.

(7) Technique to secure reliability for the emerging applications

It is a matter of course that a high-reliability technology corresponding to the future application of the LSI is demanded. Emerging applications here includes dependable processors using on-chip redundancy [6, 7], x-by-wire [8, 9], ADAS (Advanced Driver Assistance System), cloud computing, microrobot for the surgery operation, many-core processors, and so forth.

(8) Device parameter control by manipulating the distribution of the dopant atoms by the minute processing [10].

This will be one of the indispensable requirements for the Moore's Law to last in future. In addition, there is a theory that the molecular size of the photo-resist will be a limit for miniaturization.

(9) Measures for the events beyond expectations

The countermeasures that have been prepared for broader and generalized threats could be more useful in dealing with unexpected threats as a therapy than ad hoc countermeasures taken for individual failure events.

If we look back on the old days when the human was coping with the threats of epidemics using black magic, we all recognize the usefulness of systematic research of science and engineering which revealed the presence of bacteria and viruses, and a modern epidemics prevention method came to be taken in late years. Therefore, it is necessary to understand the real nature of the threats precisely to be able to deal with them.

12.1.4 Conclusions

The author wrote about the change of the VLSI system failure cause and future problems in this article. The proportion of design faults increased with the increase of the system scale. Furthermore, soft error occurrence will be remarkable with the miniaturization of the semiconductor process. With the change of such failure cause, the techniques such as human factor countermeasures, security, soft error countermeasure, and fault prediction will be necessary in the future. The limit of Moore's Law will get over by the wisdom of the human, and the miniaturization of the semiconductor will continue advancing toward the future.

12.2 Challenges to Dependability at Data Centers

Takashi Miyoshi, Fujitsu Laboratories Ltd.

12.2.1 Cloud Data Centers

The recent spread of cloud computing has caused a paradigm shift from "Ownership" to "Use" of IT systems in the Enterprise market. It is necessary to accommodate more users at cloud data centers compared with past enterprise systems that will force data centers to come up with various ideas to reduce Operating Expenses or OPEX. For example, systems can be made more flexible with scale-out techniques using virtualization technologies.

This section presents data centers that offer Infrastructure as a Service (IaaS), and discusses their requirements for dependability. Service providers in the IaaS model offer users servers and storage, and the user side constructs OSs, middleware, and applications. The IaaS providers are aimed at making their systems large scale to reduce the operating costs of data centers. For example, a large-scale provider operates more than 10,000 servers at a data center. Thus, the provider uses a large-scale and uniform system that enables fewer operators to manage it and to reduce operating costs. Such management costs in the cost structure of data centers increase in proportion to the scale of the system while investment costs of new IT equipment and power and cooling costs remain constant due to improvements in process technologies. The dependability of such IaaS systems is discussed in the following subsections.

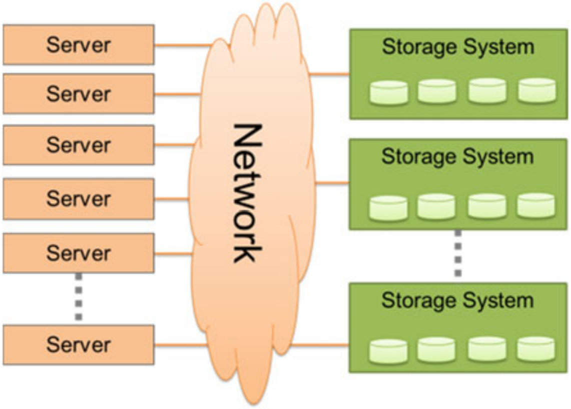
12.2.2 Dependability of Current IaaS Systems

A typical IaaS system is composed of the general-purpose server units, storage units, and network switches shown in Fig. 12.3. This system is controlled by infrastructure management middleware. The dependability of such IaaS system should be considered as a whole rather than the dependability of its individual components.

Availability of Services
Availability is generally one of the most important factors in IaaS. The service provider and the user agree beforehand through a service-level agreement (SLA) to guarantee user availability. If the SLA is not satisfied due to, e.g., system breakdown with hardware failure, the provider must pay penalties, i.e., exemptions from monthly charges. In other words, availability is used as an indicator of dependability that can directly be observed by users.

Durability of Data
The durability of user-owned data is also a critical factor. A permanent loss of user data is treated as a severe accident. Such data loss accidents in large-scale data centers are occasionally reported as big news. As important data are backed up as needed in conventional enterprise systems, the durability of data and the cost of backup is a trade-off there. However, it is necessary for IaaS that provides storage services to guarantee high levels of durability so that numerous users can use storage. For example, a durability of 99.999999999% (11 nines) is stated, for instance, in storage services with OpenStack Swift [11]. This percentage means that one file out of 10,000 may lose data permanently once in 10 million years on average. However, no storage service can ever guarantee a durability of 100%. The level of durability of data services should be agreed in SLAs. Note that durability of data does not necessarily require high reliability of each system in a site because the durability can be achieved by geographical replication across multiple regions.

Fig. 12.3 Typical IaaS configuration



Improving Dependability of Servers

We will now discuss measures to improve availability and durability based on the components of IaaS. First, server activities are monitored with Heartbeat by the middleware. When there is no Heartbeat response from the server for a while, the suspicious server unit is marked as having "failed" and removed from the server cluster. Jobs that were running on the server unit are restarted on another server in the cluster. The cause of the non-response could be hardware failures, soft errors, or even software bugs. The heartbeat mechanism is not concerned with the causes and simply treats the server unit as having failed. Once a server unit is removed from the cluster, it is replaced with a new unit later. Service providers try to reduce operating costs in this way by using coarse granularity of management and by hiding internal complexity in the server.

Improving Dependability of Networks

Redundant system architectures are adopted in networks as well as conventional enterprise systems. When a switch fails on a channel, all the traffic on the same channel is forwarded to another channel and the failed switch is replaced. However, there are cases where redundancy is not adopted in racks for upper level services such as Platform as a Service (PaaS). When a switch in a rack fails in such cases, none of the servers in the rack will be able to communicate any longer. Instead, the PaaS system guarantees availability by distributing required resources on multiple racks. The influence of failures is determined by the entire system in this manner, and reliability, availability, and cost are balanced.

Improving Dependability of Storages

There are many examples where distributed storage is constructed like OpenStack Swift on server clusters for IaaS storage services [11]. Swift adopts a replication technique (replica) to improve the durability of data, where the same data content is distributed on multiple server nodes. It is important to effectively choose the location of replicated data. The design of distributed storage involves the configuration of racks and power supply to prevent multiple data from being lost when a single failure occurs. Furthermore, disaster recovery (DR) that synchronizes data between geographically remote sites is becoming more important to prepare for natural disasters like earthquakes.

Thus, dependability is not guaranteed for device units but for systems in the data centers of IaaS.

12.2.3 New IaaS System and Its Influence on Dependability

New demands to support various types of services in IaaS have been occurring. For instance, there is a requirement to isolate services where the execution of a user should not be affected by other users' activities. It is also becoming more important to support big data processing and mission-critical workloads. A "Resource

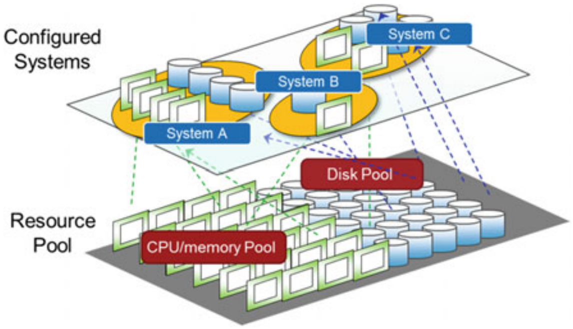


Fig. 12.4 Resource pool architecture

Pool Architecture" shown in Fig. 12.4. has been suggested to enable such new services [12].

System management in the resource pool architecture controls hardware components such as CPUs, memories, and HDDs/SSDs instead of servers and storage units, which allows finer grain resource management and enables them to be efficiently used. Each component is consolidated into the hardware pool. When a user runs an application, required components are selected and combined into a system. Thus, users can obtain a suitable system for their applications on demand.

An IaaS system where users can specify server configurations through self-portals was constructed based on the resource pool architecture. Users can easily run a wide range of applications with this kind of IaaS system, including time-constrained batch processing and big data processing that require stable I/O performance. A CPU/memory pool and disk pool are particularly used in the IaaS system. The interconnects between the CPU/memory pool and disk pool are called "Disk Area Networks" [13].

The influence of adopting the resource pool architecture on dependability is discussed below.

Precise Identification of Failures

First, it is easy to locate failed components and affected areas when failures occur in the system, which should improve its availability. For example, conventional systems use virtualization technology to create resource pools. Even if a single HDD contains an erroneous sector, it might affect multiple servers because physical HDDs are shared. It is not obvious in actual systems in which servers are affected by errors. Component-level management, on the other hand, enables failed parts and affected parts to be easily matched through errors. That reduces operating costs such as those for analysis when failures occur and also enables faster recovery and better availability of the entire system.

Reduced Maintenance Costs

Second, hardware component pools will reduce maintenance costs when errors occur in the system. Data center operators can also reduce the number of replacements of failed parts by pooling spare parts. Conventional IaaS often uses distributed storage that is constructed with server clusters and their local disk drives. For example, if 128 servers where each server contains seven active HDDs and one spare HDD are used in distributed storage, any single HDD failure requires the HDD to be immediately replaced; otherwise, the redundancy of the storage system is degraded. Other distributed storage systems may consist of HDD pools with the same resource size, i.e., 1028 HDDs in total where 128 HDDs out of 1024 are spare drives. In this case, the system would require no replacements until 128 HDDs had broken down. Thus, no maintenance would be required and operating costs would be reduced by pooling and managing components.

Impact of Failures of Disk Area Network
A consolidating point for I/O access is newly added by introducing a Disk Area Network. Therefore, the extent of the impact of failures increases in the Disk Area Network itself. A single failure may affect all of the systems that share a resource pool. The units of the Disk Area Network are carefully designed to reduce the impact of failures. The data plane that transfers user data has a simple structure with fewer parts to increase reliability. Redundancy in the Disk Area Network units is determined based on the possibility of failures and impact on the system. These designs are created by using a target operating model.

Increase in Number of Cables
Finally, the influence of an increase in the number of cables is described. A large number of coaxial cables are used in a Disk Area Network. Large numbers of cables greatly affect serviceability. Thus, optical cables should be applied in these kinds of implementations. Optical components for consumer products are required to lower costs of optical cables. However, consumer products often do not satisfy the reliability levels required by servers. Workarounds at upper levels should be applied to reduce this gap. For example, link-level redundancy and error recovery with upper level software would be a practical solution.

12.2.4 Data-Center-Level Dependability

The dependability of cloud data centers that offer IaaS is described in this section. Reduced operational cost is the key in scale-out architectures. Therefore, cloud data centers need simple and easy to manage hardware components so that any failure can be handled by upper management software. Moreover, the importance of data integrity is the same as that in other enterprise systems, and numerous service providers make it a point of differentiation.

The resource pool architecture introduced a new concept like fine-grained management. It has various influences on dependability compared to conventional IaaS systems. We introduced cases that optimized reliability, availability, and serviceability based on an operation model of the offered services.

Finally, the requirements for components used at such data centers have also been changing. High levels of reliability have so far been valued in the components used in basic servers. The number of FITs was important there. However, the requirements have changed with respect to dependability at cloud data centers. The systems have been designed with the idea that any hardware will eventually fail because there are enormous numbers of components at data centers. Consequently, it is important to simplify the hardware. Also, the impact of hardware failure should be clarified so that service providers can describe its impact in the SLA. Furthermore, it is possible to optimize the cost of error recovery not from the components themselves but from the entire system. Therefore, cooperation with upper layer software is needed. Optimization including the components and upper layer software will become increasingly critical in the future.

12.3 Post-silicon Validation and Patchable Hardware for Rectification

Masahiro Fujita, The University of Tokyo
Takeshi Matsumoto, Ishikawa National College of Technology
Hiroaki Yoshida, Fujitsu Laboratories of America
Satoshi Jo, The University of Tokyo

12.3.1 Hardware Patching

As digital systems become larger and larger, it is practically impossible to detect all of the logical bugs in the chips before their fabrications. A number of logical bugs are now found in the fabricated real chips. They have escaped from all of the verification efforts in the pre-silicon stages, such as logic simulation, formal analysis, and emulation/prototyping. It is now occupying large portions of design time to verify and debug designs after silicon. These are called post-silicon verification and debugging problems. In practice, all of the fabricated chips for the first time have some kinds of logical bugs which are only found after their fabrications.

The remaining bugs in the fabricated chips may cause serious security problems on the systems that use the chips, as important information which should be kept secret, such as the key for an encryption, may be disclosed to outside of the chips due to logical bugs. Since the ranges or types of logical bugs cannot be controlled, under buggy designs anything could happen and cannot be predicted. Therefore, it is extremely important not only to eliminate the logical bugs as much as possible in the pre-silicon phases but also to have mechanisms by which security issues caused by the logical bugs can be rectified in the fields. In order to eliminate security issues caused by logical bugs, logical bugs must be found after silicon (post-silicon) and

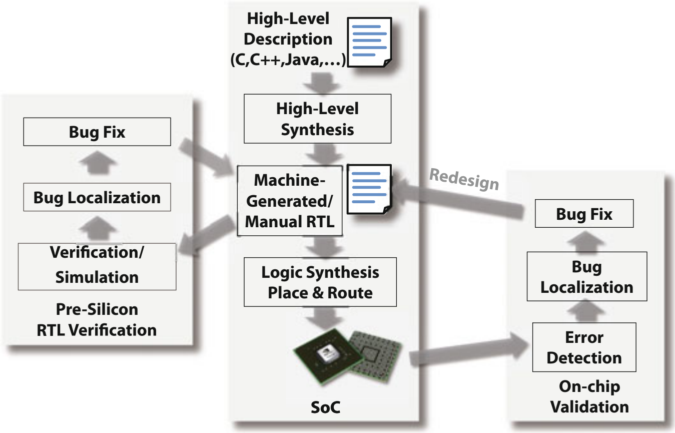


Fig. 12.5 Hardware design and verification flow

there must be some ways to change the behaviors of the fabricated chips in the fields in such a way that the security problems can be eliminated.

The hardware design and verification processes are shown in Fig. 12.5. A design may start from high level, such as C design descriptions, which are automatically synthesized into RTL (Register Transfer Level) designs by high-level synthesis tools, or may start with manually created RTL designs. Once there are RTL designs, real verification efforts start as shown in the figure, and bug elimination is tried as much as possible with logic simulation, formal verification, emulation/prototyping, and others. After some confidence is obtained from the verification processes, logic and layout synthesis are applied to generate mask patterns which are to be fabricated. Unfortunately, there are not a few cases where some bugs are found in the fields. If that ever happens, a chip must be debugged and be re-fabricated, which could be a huge amount of extra efforts and cost.

Some of the logical bugs found in the fabricated chips may be compensated by appropriately changing the software running on the chips. For example, when some functionality does not work due to some bugs, the software may be able to realize similar functionality only with software without using the buggy portions of the hardware, though significant performance decrease must be allowed. If that is not feasible, chip design and fabrication process must be performed again, which is very costly and called re-spin.

Therefore, it is practically important to have mechanisms by which some amount of functionality in the manufactured chips can be changed in the fields. We call such a mechanism "patching mechanism" in this section. The design flow proposed in this section is shown in Fig. 12.6. Here, after generating RTL designs, they are expanded with partially programmable or patching mechanisms. Although those mechanisms are overhead from the viewpoint of normal operations of the chips,

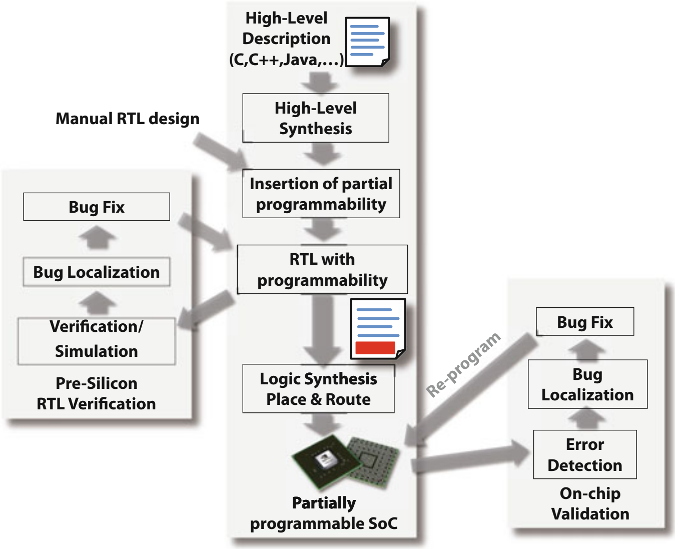


Fig. 12.6 Hardware design and verification flow with patching mechanisms in the fields

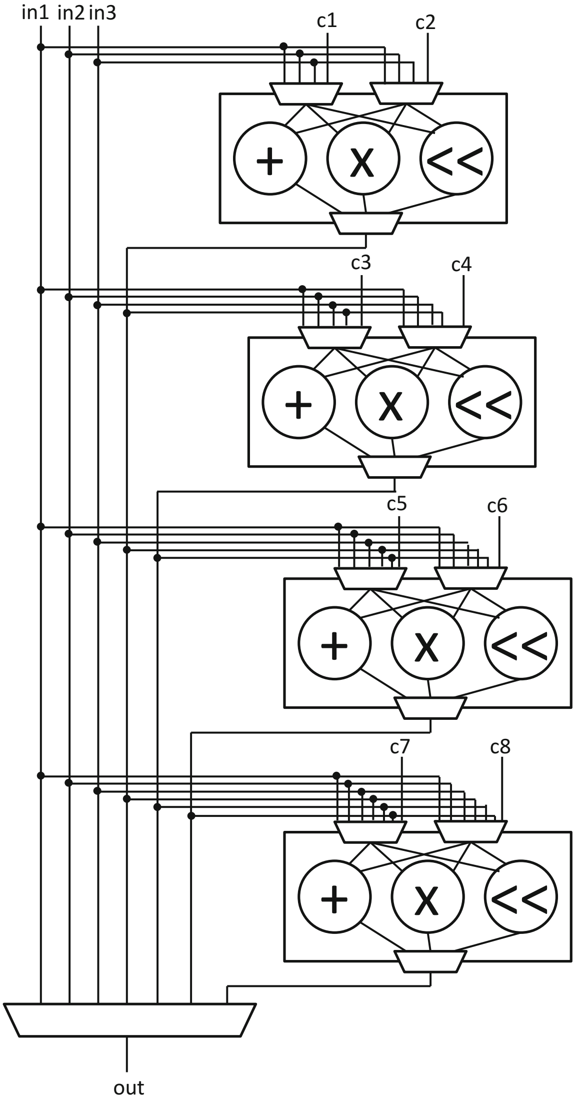
they make it possible to change the limited amount of functionality of the fabricated chips so that bugs found after chip fabrications may be rectified.

In general, RTL designs can be partitioned into control parts and datapaths. In this section, we mostly discuss the programmable datapaths, as the programmability of control parts can be realized with the same techniques shown in the Sect. 11.2. Please note that re-programming programmable datapaths in the fields need also the changes in control parts.

12.3.2 Introduction of Partially Programmable Datapath

In general, datapath in RTL designs is a collection of functional units, registers, various switches including multiplexers, buses, interface to memories, interfaces to peripherals, and others. As we like to introduce some amount of programmability in terms of functionality to be realizable in the datapath, we introduce programmable datapath which consists of a set of functional units, which are interconnected with a rich amount of multiplexers. An example of such programmable datapath is shown in Fig. 12.7. Here, in total, a sequence of four operations are to be performed in the input signals, $in1, in2$, and $in3$, and the possible operations are addition, multiplication, and shift. They are interconnected with multiplexers, and depending on how those multiplexers are controlled, a sequence of four operations out of addition, multiplication, and shift can be performed on $in1, in2, in3$. The result is sent to *out*. In the figure there are also constants, $c1, c2, \dots, c8$ which can be used as arguments

Fig. 12.7 An example of programmable datapath



for the operations. Here, we assume the values of these constants can be modified from the outside of the chip.

The programmable datapaths to be introduced can be a subset of the one in Fig. 12.7, if smaller area overhead is preferred. An example programmable datapath which is a subset of the one in Fig. 12.7 is shown in Fig. 12.8. Here, the first two operations are either addition or shift whereas the last two operations are either addition or multiplication. Although this can realize only subsets of the functionality on the inputs, it is much smaller. Basically, designers decide how much

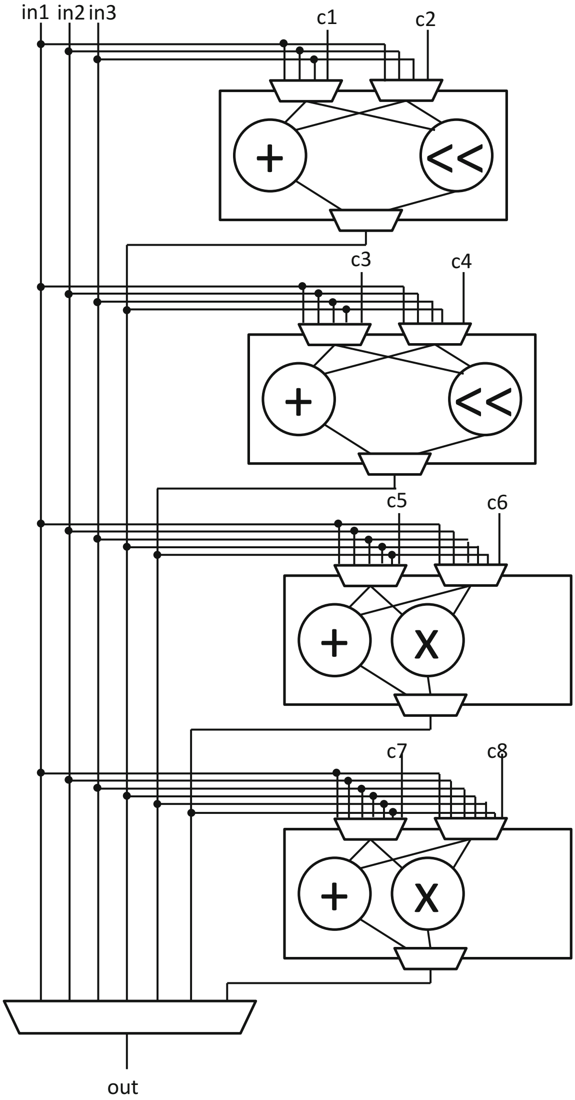


Fig. 12.8 A more restricted programmable datapath

programmability is to be introduced by considering the overhead of the programmable datapaths and the amount of programmability to be provided.

For example, if we like to realize $out = in1 + 20 * in2$, the multiplexers of the programmable datapaths are programmed and controlled in the way shown in Fig. 12.9. Please note that $4 + 16 = 20$ which is used to realize a scalar multiplication. After fabricating the chip, if we need to change this part of the chip functionality to $out = in1 + 5 * in2 + 4$, the same programmable datapaths can be programmed to the one shown in Fig. 12.10. Here, the way to compute

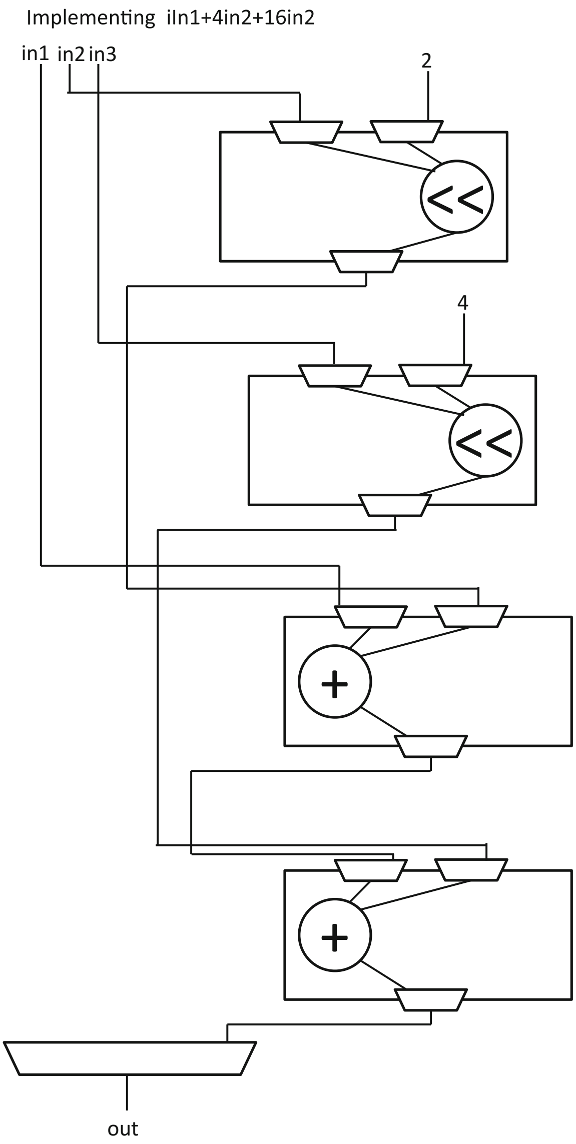
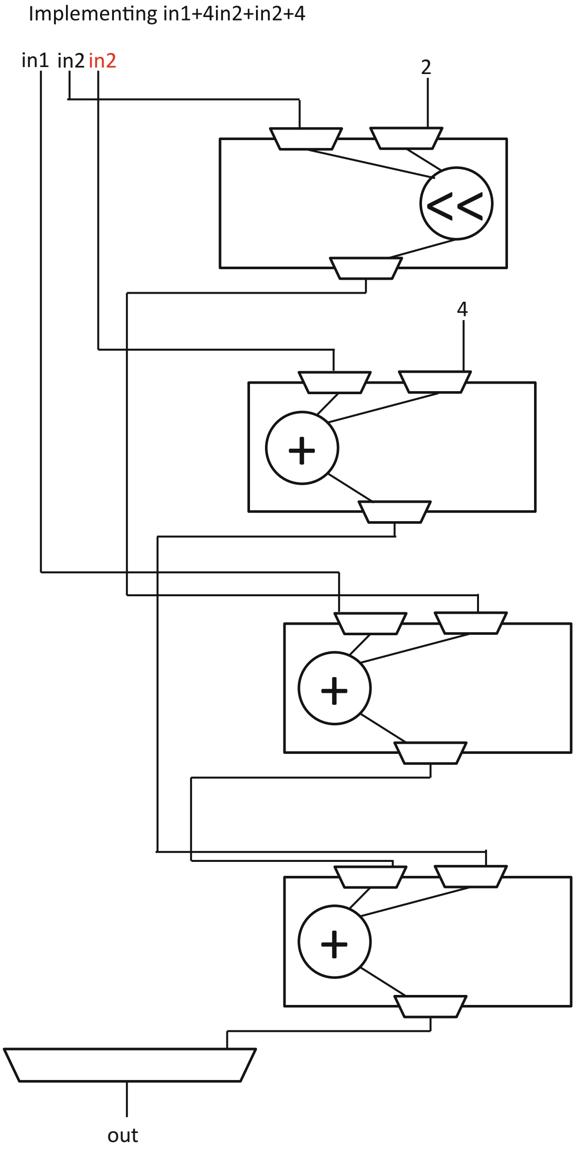


Fig. 12.9 An example expression to be realized with the programmable datapaths

$out = in1 + 5 * in2 + 4$ is $out = in1 + 4 * in2 + in2 + 4$. As can be seen from these examples, some amount of changes in functionality can be realized with programmable datapaths, and the amount of programmability is to be controlled by designers in the design phases of the chip.

Fig. 12.10 Other example expressions to be realized with the programmable datapaths



12.3.3 *The Proposed Method for Patching Datapath*

The basic idea on the processing flow for the programmable datapath is shown in Fig. 12.11. In normal high-level synthesis or manual RTL designs, functionality of the chip is defined in terms of data flow graph (DFG) or control data flow graph (CDFG). Such graphs are automatically generated by high-level synthesis tools

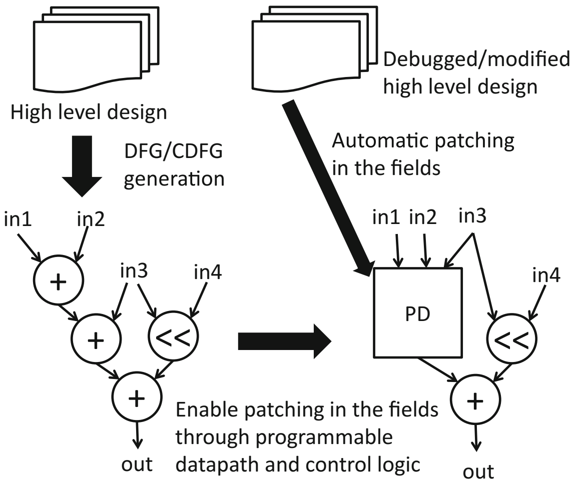

High level design
DFG/CDFG generation
Debugged/modified high level design
Automatic patching in the fields
in1
in2
in3
in4
+
<<
out
PD
Enable patching in the fields through programmable datapath and control logic

Fig. 12.11 The processing flow for programmable datapath

from high-level design descriptions such as C-based designs. Or those graphs are implicitly or explicitly used in manual design processes. Here, we assume that designers have some ideas on possible bugs or changes of specifications which can happen later in the design processes as well as actual usages of the fabricated chips, and make the portions of DFG/CDFG partially programmable through the use of programmable datapaths.

The DFG/CDFG examples for the patches shown in Figs. 12.9 and 12.10 are shown in Fig. 12.12. Let us assume that the original high-level design does the operations shown in the left DFG in the figure. As shown in the center of the figure,

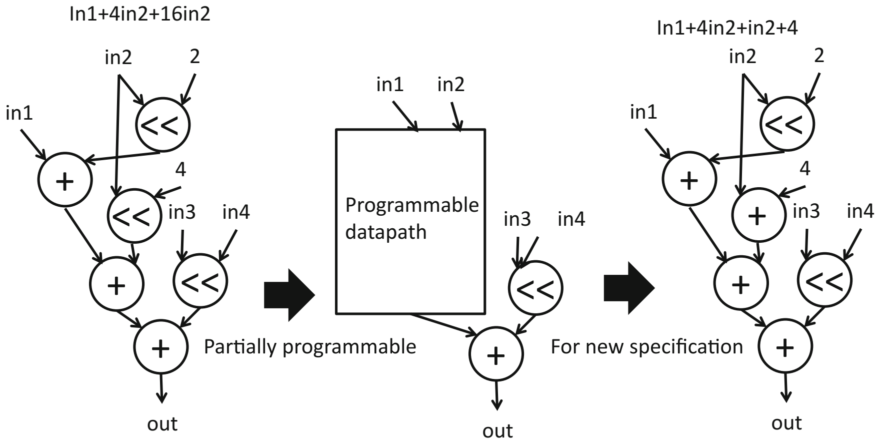


Fig. 12.12 Redesign example of DFG/CDFG

designers analyze their designs and conclude the partial insertion of programmable datapath. Then after chip fabrication, even if the expression to be realized is changed as shown in the right of the figure, by re-programming the programmable datapaths, it can be accommodated in the fields without refabricating the chip. In order to re-program programmable datapaths, the control parts of the designs must be modified accordingly, which can be taken care of by the methods shown in the Sect. 11.2 of this book.

12.3.4 Automatic Programming for New Specification and Preliminary Results

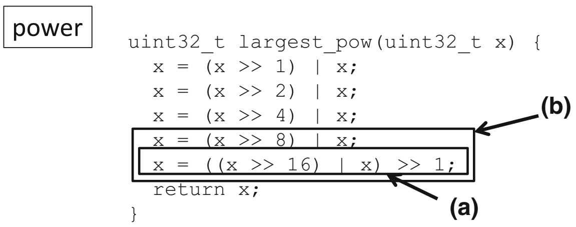
The problem to re-program the programmable datapath in such a way that the re-programmed one can realize the new specification can be formulated as Quantified Boolean Formula problem in the same way that is discussed in the Sect. 11.2. As the possible functions to be used in the programmable datapaths are predetermined, the entire compilation problem can be formulated as the problem on how to control multiplexers, which can be represented in Boolean formulae. Therefore, we can utilize the techniques shown in that section as they are. Alternatively, we can use Satisfiability Modulo Theory (SMT) solvers instead of SAT solvers to solve the programmable datapath problems, as SMT solvers can deal with word variables with arithmetic operations.

Here, we show preliminary experimental results. The C description shown in Fig. 12.13 is to count the number of 1's in the given integer value. Also, the one shown in Fig. 12.14 is to return the largest power of 2 which is less than the given value. These examples are dealing with integer variables in C program which are 32-bit width. The experiments are performed by first replacing the statements under rectangles with programmable datapaths and then automatically generating correct ways to program the re-programmable datapaths with SMT solvers. In the case of the example in Fig. 12.14, we replace two different sets of statements. We also perform experiments with simple filters having 8, 16, and 32 bits. The results are shown in Table 12.1. As can be seen from the table, although the ways to program

bit_count

```
uint32_t bit_count(uint32_t x) {
  x = (x & 0x55555555) + ((x >> 1) & 0x55555555);
  x = (x & 0x33333333) + ((x >> 2) & 0x33333333);
  x = (x & 0x0F0F0F0F) + ((x >> 4) & 0x0F0F0F0F);
  x = (x & 0x00FF00FF) + ((x >> 8) & 0x00FF00FF);
  x = (x & 0x0000FFFF) + ((x >> 16) & 0x0000FFFF);
  return x;
}
```

Fig. 12.13 Counting the numbers of 1s in a word



```
uint32_t largest_pow(uint32_t x) {
  x = (x >> 1) | x;
  x = (x >> 2) | x;
  x = (x >> 4) | x;
  x = (x >> 8) | x;
  x = ((x >> 16) | x) >> 1;
  return x;
}
```

Fig. 12.14 Returning the largest power of 2 which is less than the given value

Table 12.1 Preliminary experimental results on programmable datapath

Example	Programmable datapath			Result	Time (s)
	N_{in}	N_{op}	OP		
filter (8bit)	3	4	{+, ×, <<}	Success	30
filter (16bit)	3	4	{+, ×, <<}	Success	285
filter (32bit)	3	4	{+, ×, <<}	Timeout	>10,800
bit_count	1	3	{+, >> , &}	Success	2442
power (a)	1	3	{≫, |}	Success	8
power (b)	1	6	{≫, | }	Timeout	>10,800

can be quickly found in most cases, in some cases where either the bit width is large or the operations are complicated, the generation of the programs does not finish in 3 hours.

12.3.5 Summary and Future Works

The basic ideas on patchable hardware are shown in [14]. Basically, we can introduce partial programmability in control parts and datapaths in given RTL designs. That is, given RTL designs can be expanded to include programmability mechanisms. In this section, we have discussed programmability in datapaths. As for the programmability in control parts, the techniques shown in the Sect. 11.2 of this book, can be used to patch control parts.

The preliminary experimental results shown above as well as the results shown in [14] indicate that the amount of programmability should not be unnecessarily large from the viewpoints of area/performance overheads and the computation time required to generate ways to program multiplexers in the programmable datapaths.

The proposed patching mechanism can be a key for post-silicon verification and debugging. In that direction, the proposed method should be formulated as a general framework for post-silicon analysis. That is, some sorts of IPs should be developed based on the proposed approach by which various combinations of smaller designs or IPs can be fully debugged. This is a very important topic for IP reuse and we are working in that direction by combining the proposed method with other methods for post-silicon verification and debugging.

12.4 Logging and Using Field Test Data for Improved Dependability

Seiji Kajihara, Kyushu Institute of Technology
Satoshi Ohtake, Oita University

12.4.1 DART Test Architecture

DART [15, 16] is a field test technology that has been developed to ensure high-level reliability for VLSIs in an electronic system by carrying out self-test including delay test. The system stops the functional operation and moves to a self-test mode, which not only detects an aging-induced fault but also predicts the occurrence of an aging-induced fault in the near future temporarily. The architecture of a VLSI implementing DART is given in [17]. Field test is realized by co-operating the framework of scan design and logic BIST, which are prepared for manufacturing test, and newly developed monitor circuits (temperature and voltage monitor, TVM). Test results allow us for fault detection and also aging prediction by logging and analyzing them. The DART test architecture is shown in Fig. 12.15.

In Sect. 12.4.2, we introduce what kinds of test data we can obtain and log with in-field test. In Sect. 12.4.3, we show how the test data can be utilized, and in Sect. 12.4.4 we conclude this section.

12.4.2 Logging Field Test Data

DART grasps the progress of aging of VLSIs in field from the increase of path delay in the circuit. The paths whose delay is measured are selected such that

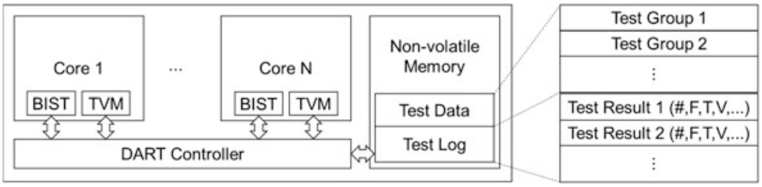


Fig. 12.15 DART test architecture

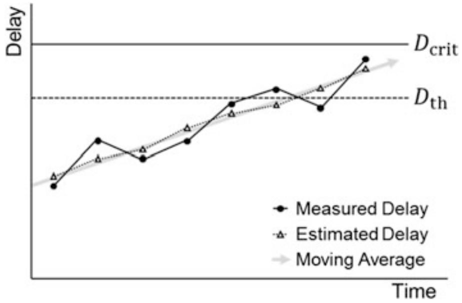


Fig. 12.16 Estimation of path delay

aging-induced faults on the paths are activated early in field. The path delay is calculated from the maximum frequency that is measured by testing the path with changing test clock timing. The measured test data can be logged onto on-chip or off-chip memory. Note that the detail of how to measure the maximum path delay is described in [18].

Increase of path delay is caused not only by aging but also the variation of temperature and the power supply voltage during testing. In order to extract the aging effect from the measured path delay, we need to know the temperature and the voltage during testing. Therefore, we implement a mechanism of the temperature and the voltage measurement with a simple method on the chip [18–20]. By using the measured temperature and voltage, the path delay at a standard temperature and voltage can be estimated from the measured path delay as shown in Fig. 12.16. The measured temperature (T) and voltage (V) can be recorded as a part of test log as shown in Fig. 12.17.

In field, testing can be performed periodically and repeatedly. Test patterns applied in field test are prepared at the design phase. Unlike the manufacturing test, the test chance is more than once and test patterns applied at each test session do not have to be same. It is recorded test patterns applied and what time test it is at each test session. These data will contribute to the reproduction of faults and the grasp of the progress of aging in field.

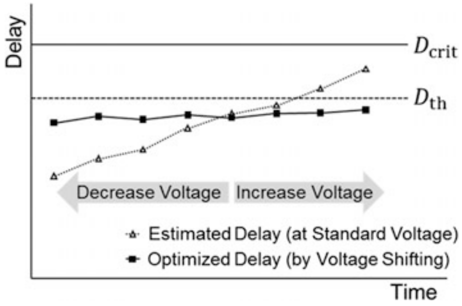


Fig. 12.17 Optimization of path delay using voltage shifting

12.4.3 *Application of Logged Field Test Data*

12.4.3.1 Prediction of Aging-Induced Fault and Adaptive Test Scheduling

Degradation which will soon be a fault is detected using the log of past field test results. Detailed information about threats of degradation and roles of field test are available in Sect. 12.5.2 and the test architecture of DART is described in [17].

In-field test, although there exist several restrictions such as shorter test application time and smaller test data volume compared with those of manufacturing test, required fault coverage is similar to that of manufacturing test. To fit respective test constraints of different applications of a VLSI, a test set is partitioned into subsets and one subset is applied to the VLSI at one test session of field test. To cover all the test sets, multiple chances of field test are used. The order of application of these subsets does not need to be fixed. The test schedule can adaptively be determined based on the past test results. By using the adaptive test scheduling, a part of the VLSI which have a decreased delay margin can be tested frequently. This feature is useful for prevention of fault appearance or early detection of faults. By analyzing the operation time of the VLSI, which is indirectly known from the number of test chances, and the logged delay variation, frequency in test can also be determined adaptively. The DART mechanism can optimize the workload, which influences the system operation, induced by itself.

12.4.3.2 Fault Diagnosis and Repair

The DART mechanism detects degradation as a delay fault using a variable test clock timing of which frequency can be faster than that of the system clock of the VLSI. Fault diagnosis for such a delay fault aims at identifying the location of the degradation and the size of the delay increased. According to the diagnostic information, the delay margin can be adjusted by calibrating the voltage and/or the clock frequency of the VLSI dynamically if these are possible in the field. This can extend the term to become a fault and prolong the life of the VLSI. If degradation has not progressed yet, the calibration optimizes the voltage and the clock frequency at a point of time and the best performance of the VLSI, i.e., decrease its power consumption and increase the clock frequency, can be derived at the point. An example of path delay optimization using voltage shifting is shown in Fig. 12.17.

For a faulty VLSI of which a fault appeared in the field, in order to investigate the cause of the fault, reproducibility of the fault is an important issue. The DART mechanism makes a log of the failing test patterns and operating environment such as temperature and voltage. The log contributes to facilitating fault location and improving efficiency of fault analysis.

12.4.3.3 Performance Optimization: Appropriate Design Margining

It is known that using a VLSI in high temperature accelerates progress of its degradation. Although the grade of degradation can usually be predicted using simulation experiments, data of degradation progress, in reality, is virtually unavailable. In general, the clock period of the VLSI includes several percent of delay margin corresponding to degradation pessimistically in its design process. From the log of the DART mechanism including operating temperature and voltage and the history of delay margin shifting, degradation affected by the operating environment can be analyzed. The result of the analysis can prevent too pessimistic or too optimistic design margining and support performance optimization before shipment of fabricated VLSIs. By analyzing the operation time and environment from the log, different application- or operating-environment-dependent appropriate delay margin can be configured to the same VLSI product, that is, the performance of the VLSI is optimized based on its application and operating environment with achieving a specific dependability.

12.4.3.4 Distinction Between Transient Fault and Intermittent Fault

Faults in VLSI are classified into permanent faults and temporary faults. There are two types of temporary faults; a transient fault and an intermittent fault. An example of a transient fault is a fault caused by a soft error. The transient fault is irrelevant to hardware defects. An example of an intermittent fault is that a path with small timing margin due to aging fails in a special environment such as a high temperature. Although such a path does not fail at a normal temperature, it may become a permanent fault due to further delay degradation. Because a chip with intermittent faults is recommended to be replaced or repaired before it changes to the permanent fault. On the other hand, a chip on which a transient fault happens does not have to be replaced. Therefore, it is important to distinguish between intermittent faults and transient faults. Both the transient faults and the intermittent faults are temporary faults and their faulty behavior looks similar. Field test log which includes information on test patterns and the environment during testing will contribute to distinguish them.

12.4.4 Conclusion

In this section, we described the data types which can be obtained as a log by the DART mechanism and their major applications. We introduced that the log of the delay margin and the operating environment of a VLSI, which enables prediction of degradation-induced faults, improvement of fault diagnosability, and so on, is useful for improved dependability of the VLSI. Furthermore, giving feedback about the test data to manufacturing test contributes test cost optimization.

12.5 Fault Detection and Reconfiguration in NoC-Coupled Multiple-CPU Cores for Deadline-Specified Periodical Tasks

Masashi Imai, Hirosaki University
Tomohiro Yoneda, National Institute of Informatics

12.5.1 Fault in Multiple-CPU Core Systems

It is recognized that chip multiprocessor (CMP) and multiprocessor system-on-a-chip (MPSoC) which integrate multiple-CPU cores, multiple memory cores, and multiple intellectual property (IP) cores in a single chip have been an integral part of the development of the modern VLSI architecture. They are a promising VLSI architecture not only for high performance but also for dependability. In a multiple-CPU core system, even if one of the CPU cores becomes faulty, the remaining CPU cores can continue to operate. When a permanent fault occurs in a CPU core, it is important to detect the fault and reconfigure the entire system in order to achieve a graceful degradation. Recently, several studies have been made on these fault-tolerant techniques using CMPs [21–27]. On the other hand, in these multiple-CPU core systems, interest in on-chip networks has been growing as a feasible solution to achieve high-performance communication between CPU cores since a simple bus architecture does not scale with the system size. Thus, in this section, a fault detection and reconfiguration method for Network-on-Chip (NoC)-based multiple-CPU core systems is proposed. It is assumed that the target application is several periodic tasks which are executed repeatedly in a specified deadline. For example, in an automotive engine control system, various periodic tasks control actuators in response to the corresponding sensor inputs in a 4 ms deadline period [28].

Figure 12.18 shows a basic architecture of the target system. Pentagons represent NoC routers “R *xy*” which have five input ports and five output ports. Each CPU core “CPU *xy*” has its small private memory “MEM *xy*” and connects the corresponding router “R *xy*” through a network interface (NI). It is assumed that the amount of each private memory is restricted, i.e., it cannot store all the target periodic tasks. In the target system, input–output (I/O) cores are connected to routers with $y = 1$. They gather sensor inputs from the outside of the chip through the external network and issue control signals to the outside of the chip in order to control the corresponding actuators. The network topology in the chip is assumed to be a 2D mesh since its physical implementation is simple, and many previous works use this topology [29–32].

It is assumed that the fault model is the single-core fault model [27]. It means that a fault is only capable of occurring in a single CPU core at any one moment

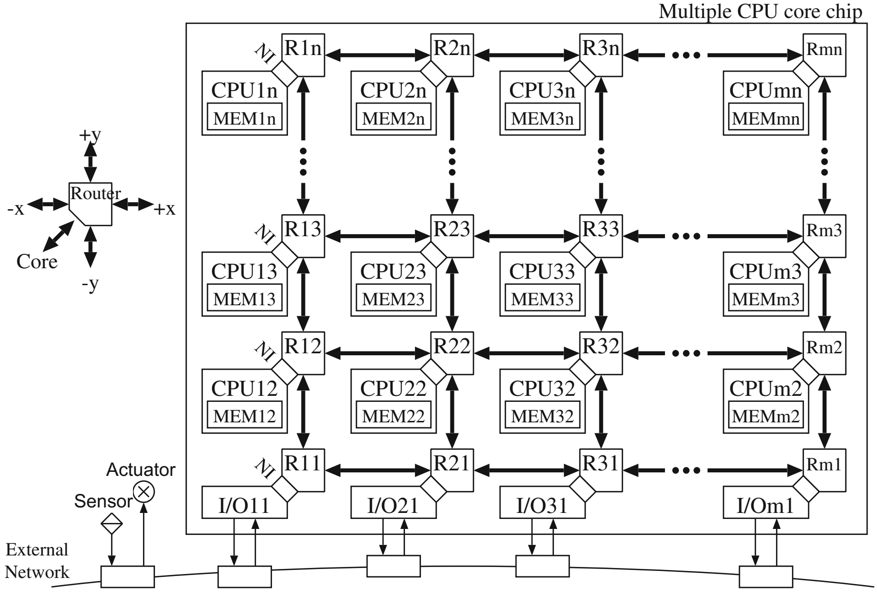


Fig. 12.18 NoC-based system overview

in time. In addition, faults in on-chip networks are not considered since the on-chip networks can be built on some kind of existing dependable routing algorithm and schemes [27, 33–35]. The fault includes both a transient fault and a permanent fault. When a transient fault occurs in a CPU core, the core can be recovered by re-executing from the last checkpoint. On the other hand, when a permanent fault occurs, the core in which the fault occurred must be identified and isolated in the following operations. Usually, transient faults tend to occur much more frequently than permanent faults.

12.5.2 Fault Detection and Reconfiguration Mechanism

When the single-core fault model is assumed, a Triple Modular Redundancy (TMR) execution is the basic way to diagnose faults, while it consumes large power. Generally, the fault occurrence frequency in VLSI chip is extremely low. Thus, the proposed method consists of two phases, the replication-and-comparison phase and the retry-and-decision phase. In the replication-and-comparison phase, two identical copies of each task are executed on a pair of CPU cores and their results are compared. If no fault occurs, all of them should match. Normally, the replication-and-comparison phase continues for a long time since the probability of fault occurrence is low. As a result, a dependable task execution with the minimum redundant power dissipation on a multiple-CPU core system can be achieved.

On the other hand, if a fault is detected by a mismatch in the replication-and-comparison phase, the retry-and-decision phase starts. In the retry-and-decision phase, the mismatched pair and one of the other CPU cores which stores the mismatched task in their private memories compose a TMR. Then, the mismatched task is re-executed on the TMR and their results are compared. If no mismatches are found at the second comparison, the fault detected at the first comparison can, therefore, be assumed to be transient. This means that the next tasks can be executed without altering the CPU core pairs. On the contrary, if two of the three second comparison results are mismatches, the faulty CPU core can be identified as the one that is included in both of the mismatched pairs, and the fault detected in both the first comparison and the second comparison can, therefore, be assumed to be permanent. Thus, the faulty core is isolated to reconfigure the entire system for continuous operation in a degraded mode. Then, the periodic task executions continue until the remaining CPU cores do not satisfy the specific redundancy.

In the target architecture shown in Fig. 12.18, the I/O core manages the CPU core pairing and the task assignment. For simple explanation, it is assumed that there is a fault-free I/O core. The above fault detection and reconfiguration mechanism can be executed according to the task table shown in Table 12.2. In the task table, each column represents stored tasks in the private memory of the corresponding CPU core. A, S, and I represent two active CPU cores, a standby CPU core, and an inactive CPU core, respectively. The active CPU cores compose a pair and execute the specific task in the replication-and-comparison phase. The standby CPU core composes a TMR with the active CPU cores in the retry-and-decision phase. The inactive CPU core is spare for reconfiguration. If the amount of private memory in each CPU core is sufficient to store redundant tasks, the number of inactive CPU cores can be increased. In that case, the inactive CPU core should be represented as I *Number*. The number represents the priority of the inactive CPU cores. When a permanent fault occurs in one of active CPU cores, the standby CPU core changes to the active CPU core, and the inactive CPU core changes to the standby CPU core, respectively.

Figure 12.19 shows an operation example when a permanent fault occurs in the CPU22. At the first comparison, it is recognized that the two CPU cores CPU12 and CPU22 did not produce the same result. Thus, the retry-and-decision phase starts. The three CPU cores CPU12, CPU22, and CPU32 compose a TMR according to the task table. Then, the mismatched task TaskA is re-executed. At the second comparison, two mismatches would exist in the TMR, i.e., CPU12 < > CPU22

Table 12.2 Task table for dependable execution

	CPU12	CPU22	CPU32	CPU42	…	CPU33	CPU43	…
Task A	A	A	S	I				
Task B			A	A		I	S	
⋮								

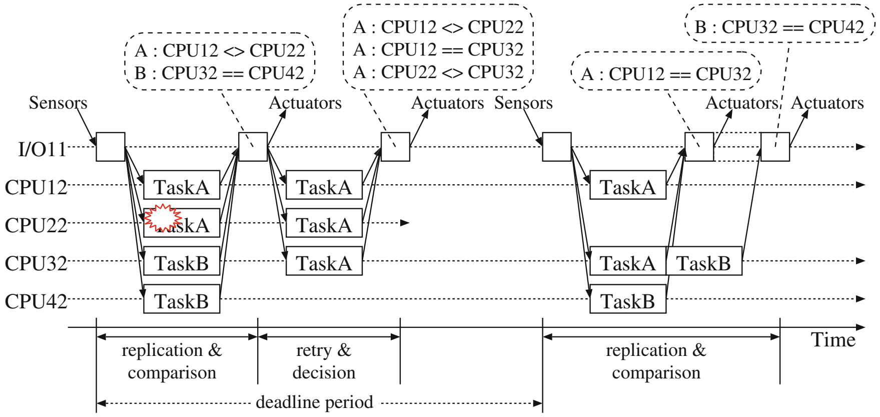


Fig. 12.19 Permanent fault operation

Table 12.3 Task table after a permanent fault occurs in CPU22

	CPU12	CPU22	CPU32	CPU42	…	CPU33	CPU43	…
Task A	A		A	S				
Task B			A	A		I	S	
⋮								

and CPU22 < > CPU32. Thus, CPU22 can be confirmed as faulty and the remaining CPU cores would then be able to compose other pairs after the second comparison. In this case, the CPU cores CPU12 and CPU32 compose a new pair, that is, CPU32 performs both TaskA and TaskB sequentially as shown in Fig. 12.19. Table 12.3 shows the modified task table after the above operations. CPU32 (CPU42) is changed from S (I) to A (S). And CPU22 is no longer used since there is no entry in the CPU22 column. As the result, the entire system achieves graceful degradation.

12.5.3 Reliability Comparison

The mean time to failure (MTTF) evaluation results of the proposed scheme is reported. The MTTF depends on the redundancy of stored tasks. If all the tasks are duplicated, i.e., there are no standby CPU core and no inactive CPU core, the entire system should get failed when a permanent fault occurs. If all the tasks are quadruplicated, i.e., there is a standby CPU core and an inactive CPU core as shown in Table 12.2, it can be allowed that *N* CPU cores get failed in a 2*N* core NoC-based multiple-CPU core system in a fortunate case. In this case, all the remaining CPU cores perform two tasks sequentially. However, in an unfortunate case, the entire

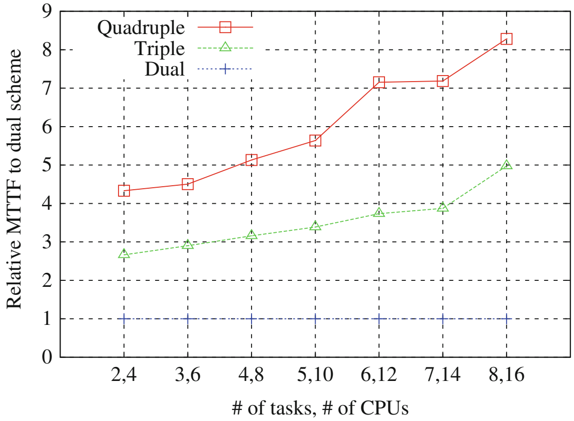


Fig. 12.20 MTTF ratio comparison

system should get failed when only three CPU cores get failed. The MTTF can be calculated using the failure rate of the CPU core. Figure 12.20 shows the ratio of MTTF to the duplicated scheme. The horizontal axis represents the number of tasks and the number of CPU cores. The vertical axis represents the ratio of MTTF. In Fig. 12.20, triangles and squares represent the triplicated scheme and the quadruplicated scheme, respectively. The triplicated scheme requires 1.5 times larger memory size than the duplicated scheme. Then, the quadruplicated scheme requires 2 times larger memory size than the duplicated scheme. As shown in Fig. 12.20, the MTTF ratios of the triplicated scheme and the quadruplicated scheme are larger than 1.5 and 2.0 in all the conditions. Thus, it can be concluded that the proposed scheme can achieve highly dependable systems with reasonable overhead and it is more effective as the number of simultaneously executed tasks increases.

12.6 Checkpoint-Restart for Heterogeneous Multiple-Processor Systems

Hiroyuki Takizawa, Tohoku University
Ye Gao, Tohoku University
Masayuki Sato, Tohoku University
Ryusuke Egawa, Tohoku University
Hiroaki Kobayashi, Tohoku University

12.6.1 Checkpoint-Restart for Heterogeneous Computing Systems

Any single technology would be unable to assure the dependability of a system. A system becomes dependable only if its dependability is considered in all aspects of its design. Thus, in addition to the device technologies addressed in this book, we need to consider software technologies that can contribute to system dependability.

Section 12.6 describes a so-called checkpoint-restart (CPR) technology, which is one of the most popular and the most powerful technologies to enhance the dependability of a system. CPR is to take a snapshot of a running program, called a checkpoint, from which the system can resume the program execution state and restart the program, instead of running it again from the beginning. CPR can roll back the execution state of a program to a healthy one recorded in the past. Therefore, CPR is an indispensable feature to build a dependable system that resists transient hardware faults and also prepares even against unidentified threats.

So far, a program execution state has been defined as the state of a process that is a collection of registers, stack memory, global variables, heap memory, and so on. However, in the heterogeneous multiple-processor era, more information is necessary to resume the state of program execution and thus to restart the program, because multiple processes and/or threads running on potentially different kinds of processors and/or cores closely collaborate to execute one program.

Suppose a heterogeneous computing system, in which a host processor controls another kind of processors, often called *accelerators*. An application program is launched on the host processor, and its execution is “partially” offloaded to the accelerators. An accelerator has its own memory space, and some of data can be stored exclusively in the memory space. In such a case, it is obvious that the program execution state is comprised by not only the host processor’s state but also the accelerators’ ones. The program cannot restart unless the states of all the processors are resumed. Since accelerators are usually special-purpose processors, they are not necessarily capable of taking their checkpoints by themselves. In a heterogeneous computing system, therefore, the host processor should save the states of the accelerators as well as the host processor itself. In spite of the importance, however, there has existed no established way for CPR of such a heterogeneous computing system.

Various CPR tools have been developed without considering the existence of accelerators in a system, and none of them can correctly take a checkpoint of a heterogeneous computing system. If an application program uses an accelerator, such a CPR tool does not save the state of the accelerator, and hence the program cannot correctly recover its execution state. Moreover, since the CPR tool does not know how to access the accelerator, kernel mode access to such an unknown device usually leads to kernel crashes or unstable behaviors, and thus degrades the system dependability. Consequently, a conventional CPR tool cannot correctly take the checkpoint of a heterogeneous computing system.

In the standard C programming, a heap memory chunk is allocated by calling the `malloc` function and deallocated by the `free` function. By monitoring all of those function calls, we can implicitly and transparently record the initial address and size of every currently available chunk. As a result, we can automatically save the contents of those memory chunks into a checkpoint. This is a standard way to taking a checkpoint of heap memory chunks. Similarly, we are able to take a snapshot of an accelerator if the accelerator is always controlled by calling specific functions and if all of those function calls are monitored. If we can completely monitor those function calls, we can keep tracking what kinds of resources of an accelerator are currently allocated and how their states are configured.

12.6.2 Transparent Checkpoint-Restart of OpenCL Programs

We focus on Open Compute Language (OpenCL) Version 1.0 [36] as the programming interface for accelerators. OpenCL is an open standard for programming various accelerators in a unified fashion, and provides a set of functions as the application programming interface (API) for managing an accelerator. OpenCL implementations are now available for programming of today's major accelerators such as graphics processing units (GPUs), Many Integrated Cores (MIC), and Field-Programmable Gate Arrays (FPGAs). In the OpenCL programming model, an application program running on the host processor, called a *host program*, is supposed to offload its computationally expensive parts on to an accelerator by using those API functions. Without going through the function calls, the host processor cannot allocate, configure, use, and deallocate any resources on the accelerator. In the host program, those allocated resources are represented as OpenCL objects. Therefore, the purpose of our work is to demonstrate that the host processor can correctly save and resume the accelerator state, i.e., OpenCL objects, by monitoring the OpenCL API calls and thereby recording changes in the states of OpenCL objects.

We have proposed a CPR tool, named CheCL (Checkpointer for OpenCL), for CPR of OpenCL programs [37]. CheCL works with a conventional CPR tool that is developed for writing the host memory image of a process into a checkpoint file. CheCL is responsible for saving and restoring OpenCL objects.

To avoid the conventional CPR tool from accessing an unknown device such as an accelerator at taking a checkpoint, CheCL employs an API proxy technique to decouple an OpenCL program from OpenCL implementations such as OpenCL libraries and runtime systems. In the case of using CheCL for executing an OpenCL program, the program is executed by at least two processes, an application process and an API proxy, as shown in Fig. 12.21. CheCL provides wrapper functions that mimic OpenCL API functions. Every OpenCL API call of the application process is actually calling such a wrapper function and then forwarded to the API proxy,

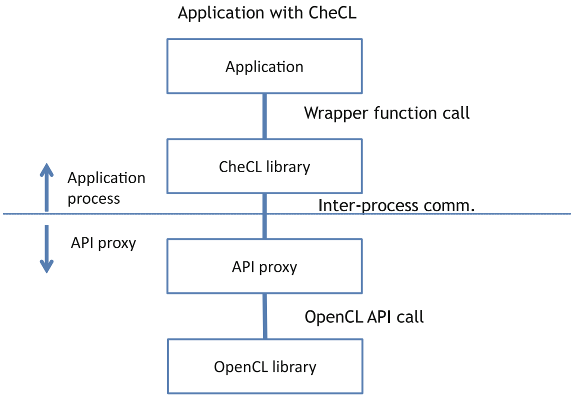


Fig. 12.21 Decoupling of OpenCL runtime system from an application program using two processes, an application process and API proxy

which is another process automatically forked by the application process. Then, the API proxy invokes the actual OpenCL API function to change the state of an OpenCL object after the wrapper function records the new state in the host memory space. Notice that the API proxy is an OpenCL process, and the application process is itself a standard process just communicating with the API proxy. This means that it does not directly use any devices unknown to the conventional CPR tool working with CheCL, and thus it is safely checkpointable.

12.6.3 Evaluation and Discussions

In [37], we have demonstrated the feasibility of transparent checkpointing of OpenCL programs, and quantitatively evaluated the runtime overheads. Figure 12.22 shows the performance evaluation results to show the timing overheads of our CheCL implementation, which uses BCLR [38] to dump the host memory data into a checkpoint file. For the evaluation, 39 benchmark programs are selected from NVIDIA SDK samples, the SHOC benchmark suite [39], and the Parboil benchmark suite [40]. NVIDIA Tesla C1060, AMD RADION 5870, and Intel Core i7 920 are used as accelerators. The execution time of each benchmark program running with CheCL is compared to that without CheCL. In Fig. 12.22, the former execution time is normalized by the latter one to show how much the timing overhead is required for managing each accelerator via the API proxy.

Figure 12.22 shows that CheCL can correctly run a wide variety of programs, because it covers almost all the OpenCL API functions. This indicates that the API proxy approach taken by CheCL can correctly monitor API calls and transparently record the changes in accelerators' states, i.e., OpenCL objects. Therefore, these results clearly show the feasibility of transparent checkpointing of OpenCL programs by using CheCL.

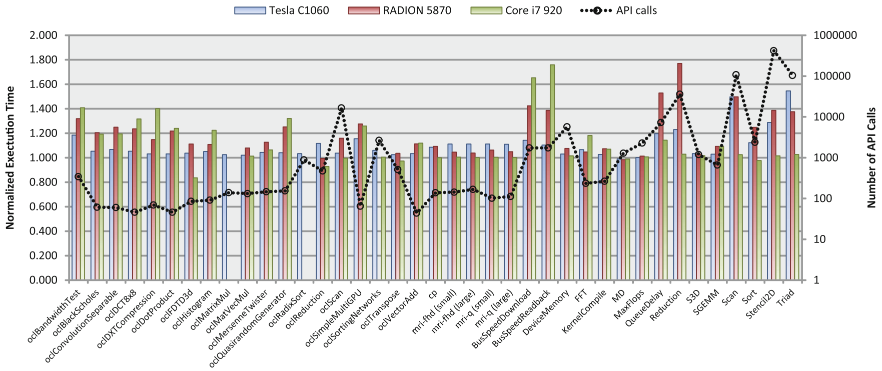


Fig. 12.22 Timing overheads caused by the API proxy approach to indirectly manage accelerators

The performance evaluation results in Fig. 12.22 also indicate that the timing overhead is likely to be large if an application program just repeats invoking API functions in a short period, or if its execution time is dominated by the data transfer time between the host processor and the accelerator. Accordingly, although the API proxy approach induces runtime overheads, our evaluation results suggest that the overheads would be acceptable in practical application programs well-designed for accelerator computing, in which the data transfers between the host processor and the accelerator are minimized.

In [37], it is also discussed that CheCL can enable process migration of OpenCL programs among different kinds of accelerators, because OpenCL objects do not have any architecture-dependent information. Moreover, since the file I/O time is a dominant factor of the total checkpointing time, and hence the checkpointing time is almost proportional to the checkpoint file size, as shown in Fig. 12.23, CheCL has been further improved to use a hierarchical storage system to reduce the overheads of reading and writing a checkpoint from/to a file [41]. Recently, we have also examined an auto-tuning method for adjusting some parameters required

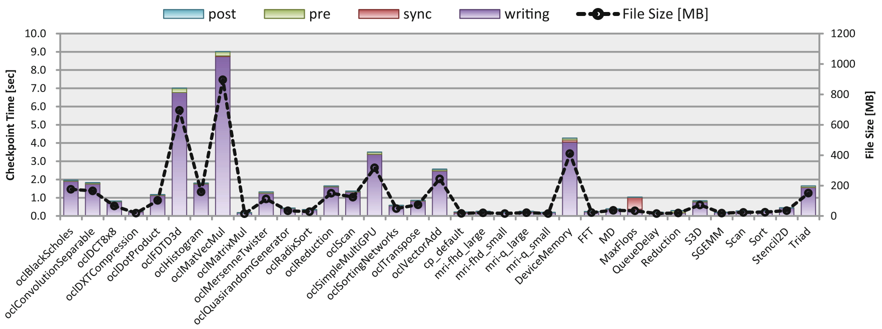


Fig. 12.23 Most of the checkpointing time is spent for writing a checkpoint into a file

for efficient use of the hierarchical storage system [42]. Efficient use of deeper memory hierarchy, which will be opened up by 3-dimensional die stacking technologies, will be the key to achieve more efficient and effective CPR for more complicated future computing systems.

References

1. N. Kanekawa, Trends in fault causes and challenges for the future. Trans. Reliab. Eng. Assoc. Jpn. **35**(8), 509–510 (2013)
2. G.E. Moore, Cramming more components onto integrated circuits. Electron. Mag. **38**(8), 114–117 (1965)
3. T.J. O'Gorman et al., Field testing for cosmicray soft error in semiconductor memories. IBM J. R&D **40**(1), 41–50 (1996)
4. E. Ibe, Current and future trend on cosmic-ray-neutron induced single event upset at the ground down to 0.1-micron-device, in *The Svedberg Laboratory Workshop on Applied Physics, Uppsala*, No. 1, 3 May 2001
5. Y. Sato et al., DART: dependable VLSI test architecture and its implementation, in *Proceedings of International Test Conference (ITC'12)*, paper 15.2 (2012)
6. N. Kanekawa et al., Self-checking and fail-safe LSIs by intra-chip redundancy, in *Proceedings of 26th International Symposium on Fault-Tolerant Computing, FTCS-26* (1996) pp. 426–430
7. N. Kanekawa, Potential of fault-detection coverage by means of on-chip redundancy—IEC61508: are there royal roads to SIL 4?. IEICE Trans. Inf. Syst. **E96-D**(9), 1907–1913 (2013)
8. K. Sakurai et al., Dependable and cost-effective architecture for X-by-wire systems, in *FISITA 2008 World Automotive Congress Sep-08.* Paper No. F2008-05-048
9. K. Sakurai et al., Membership middleware for dependable and cost-effective X-by-wire systems, in *SAE 2008 World Congress Apr-08.* Technical Paper No. 2008-01-0478
10. B. Becker et al., DFG-projekt real test—test und zuverlässigkeit nanoelektronischer systeme (DFG-project—test and reliability of nano-electronic systems). IT Inf. Technol. **48**(5), 304–306 (2006)
11. Open Stack Swift, http://docs.openstack.org/developer/swift
12. T. Miyoshi, K. Oe, J. Tanaka, T. Yamamoto, H. Yamashima, New system architecture for next-generation green data centers: mangrove. FUJITSU Sci. Tech. J. **48**(2), 184–191 (2012)
13. M. Yamazaki, Realization of the multi-tenant environment for physical IaaS using recource pool architecture. Tech. Rep. IEICE **113**(169), 1–6 (2013)
14. H. Yoshida, M. Fujita, An energy-efficient patchable accelerator for post-silicon engineering changes, in *The 9th International Conference on Hardware/Software Codesign and System Synthesis (CODES + ISSS 2011)* (2011), pp. 13–20
15. H. Yi et al., A failure prediction strategy for transistor aging. IEEE Trans. Very Large Scale Integr. Syst. **20**(11), 1951–1959 (2012)
16. Y. Sato et al., DART: dependable VLSI test architecture and its implementation, in *Proceedings of IEEE International Test Conference*, Paper 15.2 (2012)
17. K. Hatayama, *Circuit and System Mechanisms for High Field Reliability—DART Technology*, Chapter 16
18. Y. Sato, *In-Field Monitoring of Device Degradation for Predictive Maintenance*, Section 6.3
19. Y. Miura et al., On-chip temperature and voltage measurement for field testing, in *Proceedings of IEEE European Test Symosium* (2012), p. 204
20. Y. Miyake et al., Temperature and Voltage estimation using ring-oscillator-based monitor for field test, in *Proceedings of IEEE Asian Test Symposium* (2014) [to appear]

21. S.S. Mukherjee, M. Kontz, S.K. Reinhardt, Detailed design and evaluation of redundant multithreading alternatives, in *Proceedings ISCA02*, May 2002, pp. 99–110
22. M. Gomaa, C. Scarbrough, T.N. Vijaykumar, I. Pomeranz, Transient-fault recovery for chip multiprocessors, in *Proceedings ISCA03*, June 2003, pp. 98–109
23. C. LaFrieda, E. Ipek, J.F. Martinez, R. Manohar, Utilizing dynamically coupled cores to form a resilient chip multiprocessor, in *Proceedings of DSN07*, June 2007, pp. 317–326
24. R. Gong, K. Dai, Z. Wang, Transient fault tolerance on chip multiprocessor based on dual and triple core redundancy, in *Proceedings of PRDC08*, Dec 2008, pp. 273–280
25. S. Kumar S. Hari, M.-L. Li, P. Ramachandran, B. Choi, S.V. Adve, mSWAT: low-cost hardware fault detection and diagnosis for multicore systems, in *Proceedings of MICRO09*, December 2009, pp. 122–132
26. J.L. Weston, M. Imai, T. Nagai, T. Nanya, An efficient decision unit for the pair and swap methodology within chip multiprocessors, in *Proceedings of PRDC10*, Dec 2010
27. M. Imai, T. Yoneda, Fault diagnosis and reconfiguration method for network-on-chip based multiple processor systems with restricted private memories. IEICE Trans. Inf. Syst. **E96-D** (9), 1914–1925 (2013)
28. C. Mannakkara, D. Wang, V. Holimath, T. Yoneda, A case study on dependable network-on-chip platform for automotive applications. IEICE Technical Report, CPSY/DC-2011, no. 3, pp. 11–16 (2011)
29. Y. Durand, C. Bernard, D. Lattard, FAUST: on-chip distributed architecture for a 4G baseband modem SoC, in *Proceedings of IPSOC05* (2005), pp. 51–55
30. T. Bjerregaard, J. Sparso, A scheduling discipline for latency and bandwidth guarantees in asynchronous network-on-chip, in *Proceedings of ASYNC05* (2005), pp. 34–43
31. S. Bell et al., TILE64 processor: a 64-core SoC with mesh interconnect, in *Proceedings of ISSCC08* (2008), pp. 88–89, 598
32. S.R. Vangal et al., An 80-tile sub-100w teraflops processor in 65-nm CMOS. IEEE J. Solid-State Circuits **43**(1), 29–41 (2008)
33. Y. Fukushima, M. Fukushi, S. Horiguchi, Fault-tolerant routing algorithm for network on chip without virtual channels, in *Proceedings of DFT2009*, Oct 2009, pp. 313–321
34. M. Valinataj, S. Mohammadi, J. Plosila, P. Liljeberg, A fault-tolerant and congestion-aware routing algorithm for networks-on-chip, in *Proceedings of DDECS* (2010), pp. 139–144
35. S. Pasricha, Y. Zou, D. Connors, H.J. Siegel, OE + IOE: a novel turn model based fault tolerant routing scheme for networks-on-chip, in *Proceedings of CODES + ISSS* (2010), pp. 85–93
36. Khronos OpenCL Working Group (2009) The OpenCL specification version:1.0 document revision: 48. http://www.khronos.org/registry/cl/
37. H. Takizawa, K. Koyama, K. Sato, K. Komatsu, H. Kobayashi, CheCL: transparent checkpointing and process migration of OpenCL applications, in *2011 IEEE International Parallel & Distributed Processing Symposium* (2011), pp. 864–876
38. P.H. Hargrove, J.C. Duell, Berkeley lab checkpoint/restart (BLCR) for linux clusters, in *Proceedings of SciDAC 2006* (2006)
39. A. Danalis et al., The scalable heterogeneous computing (SHOC) benchmark suite, in *The 3rd Workshop on General-Purpose Computation on Graphics Processors (GPGPU 2010)* (2010)
40. IMPACT Research Group (2007) Parboil benchmark suite, http://impact.crhc.illinois.edu/parboil.php
41. A. Amrizal, S. Hirasawa, K. Komatsu, H. Takizawa, H. Kobayashi, Improving the scalability of transparent checkpointing for GPU computing systems, in *IEEE Region 10 Conference (TENCON 2012)* (2012), pp. 1–6
42. A. Amrizal, S. Hirasawa, H. Takizawa, H. Kobayashi, Automatic parameter tuning of hierarchical incremental checkpointing, in *High Performance Computing for Computational Science, VECPAR 2014*. Lecture Notes in Computer Science, vol. 8969 (2014), pp. 298–309

Part III
Design and Test of VLSI for Systems Dependability

Chapter 13
Design Automation for Reliability

Hiroto Yasuura

Abstract For design of dependable VLSI design, we need design automation tools, which are compatible with the existing VLSI design toolchain for hierarchical design from system architecture level to device level. The existing toolchain contains analysis and synthesis tools for cost (area), performance, and power consumption of the VLSI. Since dependability is a new measurement of VLSI system design, new methods of evaluation and optimization of the designed VLSI system should be established. The difficulty of the evaluation and optimization of dependability is caused by variety of measurements, probabilistic phenomena, and hierarchical discontinuity of dependability. In this section, design automation tools for soft error are presented, as an example. Soft error occurs collisions of neutrons. An analysis tool of physical level simulates a process of changes of density of charges caused by the collision. In electric circuit level, the neutron collision is presented as an appearance of temporary unexpected current source in the circuit. Circuit simulators can be used to analyze the effect of the temporary current source. Only huge voltage change, which is a pulse signal larger than logical threshold of gates and bit flip of memory elements, should be considered in the logical circuit level. In logic circuit level, propagation of the pulses should be analyzed. Some pulses may disappear by masking effects of logical gates and flip-flops. Memories have to be analyzed by different approaches utilizing the regularity. In register transfer and system architecture levels, a system error occurs only when the wrong data is read out and used in the subsequent computation process affecting the final output of the VLSI system.

Keywords Hierarchical design · Design automation · Analysis tools
Probabilistic simulation · Simulators

H. Yasuura (✉)
Kyushu University, Fukuoka, Japan
e-mail: yasuura.hiroto.117@m.kyushu-u.ac.jp

S. Asai (ed.), *VLSI Design and Test for Systems Dependability*,
https://doi.org/10.1007/978-4-431-56594-9_13

13.1 Design Automation Tools and Dependability

VLSI systems are completely designed using design automation (DA) tools, which consist of design description tools, analysis tools, and synthesis ones. Traditional design automation tools create optimum design considering trade-off among cost, performance, and energy consumption of a designed system. For dependable VLSI system design, a new criterion, dependability, or reliability should be added in the trade-off design. Thus, new tools for dependability have to keep compatibility with DA tools for the traditional criteria (There are many textbooks on design automation for example [1]).

Hierarchical design can be managed for the complexity of designed systems, which consists of more than billions of transistors. Design process is divided into the following five layers:

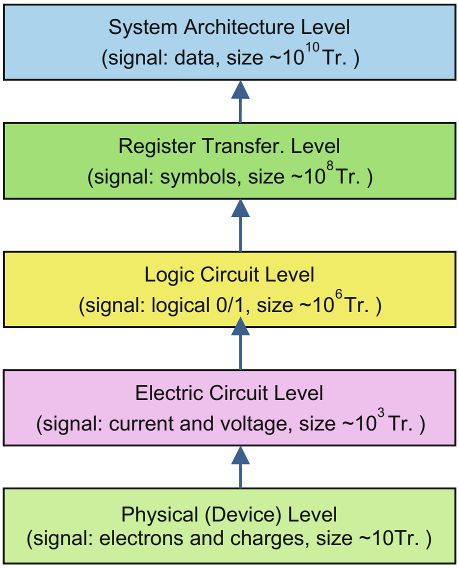
System Architecture Level (signals: data),
Register Transfer Level (RTL) (signals: symbols),
Logic Circuit Level (signals: logical 0 and 1),
Electric Circuit Level (signals: current and voltage), and
Device (Physical) Level (signals: electrons and charges).

In each level, you have to treat different abstraction levels of signals and design description. In the physical level, a few devices such as transistors are objects of DA tools and behavior of the devices are presented as motions of electrons and charged particles. In the electric circuit level, current and voltage are signals to carry information and circuits at most thousands of transistors can be analyzed and synthesized. In the logic circuit level, signals are simplified as binary logical values (0 and 1) and you can handle circuits with millions of transistors. In the register transfer level and system architecture level, signals are abstracted as values of symbols of variables and data as well as software programs and circuits with billions of transistors are managed on DA tools (see Fig. 13.1).

DA tools have also been developed for each level to analyze and to optimize cost, performance (speed or time delay), and energy consumption of systems or circuits. For dependability, you also need to develop tools to treat dependability or reliability and the new tools should be consistent with the existing DA tools to share the design data of the object systems. The consistency of design data in the hierarchical design makes it possible to optimize designed systems by trade-off among cost, performance, energy consumption, and dependability.

From the viewpoint of dependability of VLSI systems, detailed behavior of electrons or charges is not important in the electric circuit level. Only change of currents and/or voltages of the circuit by malfunction occurred by behavior of electrons or charges are important. In the logic circuit level, change of logical signal 0/1 occurred by change of current and/or voltage is essentially interesting for designer. In the register transfer or system architecture levels, differences of signals (symbols and/or data) are essentially important for the VLSI system design. The differences in normal behavior and malfunction of each level are caused by the

Fig. 13.1 Hierarchical design


System Architecture Level
(signal: data, size ~10^10 Tr.)
Register Transfer. Level
(signal: symbols, size ~10^8 Tr.)
Logic Circuit Level
(signal: logical 0/1, size ~10^6 Tr.)
Electric Circuit Level
(signal: current and voltage, size ~10^3 Tr.)
Physical (Device) Level
(signal: electrons and charges, size ~10Tr.)

differences of them in the lower level. But total dependability of the VLSI system is defined in the system architecture level. From analysis of the behavior in the physical level, how to deduce the dependability in system architecture level is the key technology of design automation for dependability.

In the existing design automation system, description tools are data formats and description languages, which can represent the models of circuits and systems in each design abstraction level. Tools for dependability should share the same models and description format of the system with conventional DA tools, because of sharing of design data. Standard description of circuits, such as SPICE netlist for the electric circuit level, HDLs (Hardware design languages), in logic circuit and RT levels, is used as description tools.

Cost, performance, and energy consumption of circuits and systems are evaluated by the analysis tools. Simulators are the most popular tools for analysis at all levels. According to the loss of information by signal abstraction in higher design levels, the result of analysis includes errors of evaluation for each measurement. The trade-off between accuracy and computation time caused by the preciseness of the circuit model is very important. The difference of simulation time for the same circuit is 10^2–10^4 times between two adjacent levels. For example, if you use a logic simulator for the logical circuit level, you can reduce computation time more than ten thousands times compared with a circuit-level simulation for the electrical circuit level. Using simulation in higher level, you can reduce computation time for more than hundreds times, but you lose detailed information on behavior of the circuits and systems. In other words, using simulation in higher level, you can simulate a circuit with more than hundreds times larger number of transistors in the same computation time and resources. Using simulation at higher levels, your analysis contains more errors. The trade-off between computation time and accuracy must be considered as main issues in the usage of analysis tools. In development of analysis tools for dependability, reduction of computation time developing efficient algorithms to minimize computation time and loss of accuracy is the most important problem as well as the existing simulators with long histories of researches on improvement of speed-up and accuracy.

The other important issue of simulation is what kind of input stimulus applies to the target system for simulation. The quality of stimulus also strongly affects the accuracy of the result of analysis. Since dependability and reliability are often defined as a probabilistic process, probabilistic approach of simulation rather than deterministic approach should be introduced. This is a new challenge of simulation and circuit analysis technologies, when you develop DA tools for dependability.

Synthesis process is a cyclic operation of analysis, evaluation, and redesign (improvement) for design optimization. Using the result of analysis and evaluation, you can change the design and check the effect of the improvement of the design change by analysis again. Optimization can be done by repetition of the above process under a given strategy to optimize the value of measurements, such as cost, performance, energy consumption, and dependability.

To improve dependability of systems and circuits, the following redesign techniques will be introduced into synthesis tools. In the physical level, improvement is done in device structures to increase tolerance to noises. In the electric circuit level, circuit structure and combination of devices are optimized. Introducing redundancy is mainly used in the logic circuit level, register transfer level, and system architecture level.

Challenges of DA tools on dependability are summarized as follows:

(1) Variety of measurements: There are various causes to affect dependability of systems. You need to develop tools to treat and evaluate different measurements (or parameters) representing dependability and reliability.

(2) Probabilistic phenomena: Most problems affecting system dependability are probabilistic phenomena. Probabilistic approach to analysis and evaluation may be effective for tools for dependability. New circuit models and algorithms are required for the probabilistic approaches.

(3) Hierarchical discontinuity: The measurements of dependability have different properties from the traditional measurements of design quality, such as cost, performance, and energy consumption. The traditional measurements have continual properties between a system and its components. For example, chip area of a system, one of the major measurements of cost of the system, is approximately the sum of areas of its components. Thus, you can estimate the total area of the system by summing up the areas of all components of the system. But dependability of a system is not expressed by a simple function of dependability of each component. How to evaluate dependability of the system from the dependability of each component is a big challenge of DA tool development.

13.2 Analysis Tools for Soft Errors

As an example of DA tools for dependability, let us consider tools for soft error analysis. In Fig. 13.2, the causal relation of soft error, which the analysis tools should evaluate, is presented [2].

Soft error occurs collisions of neutrons. The collision causes abnormal sets of charges in a device. Analysis tool of physical level simulates a process of changes of density of charges caused by the collision. Basic techniques of device simulation can be used, but various cases should be analyzed considering the difference of

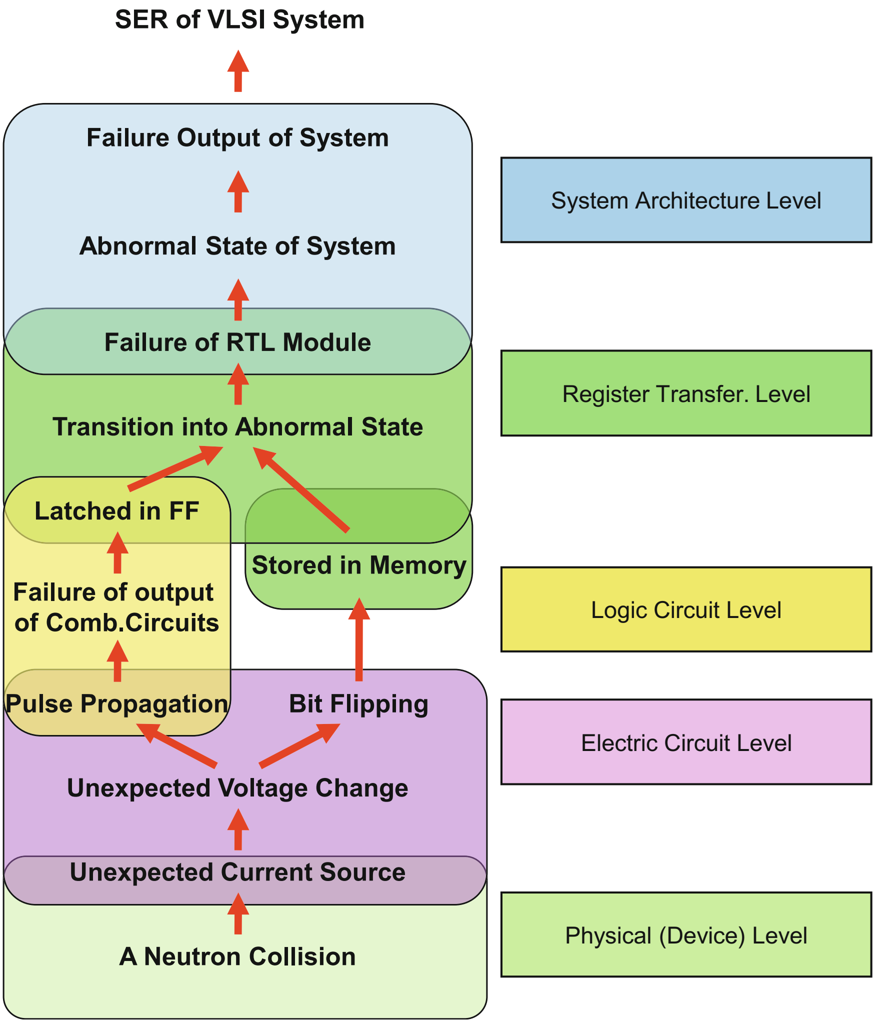


Fig. 13.2 Analysis of soft error

potion, angle, and speed of neutrons. Multiple particle hittings are also to be considered.

In electric circuit level, the neutron collision is presented as an appearance of temporary unexpected current source in the circuit. Circuit simulators can be used to analyze the effect of the temporary current source such as changes of voltage of various portions of the circuit. Only huge voltage change, which is a pulse signal larger than logical threshold of gates and bit flip of memory elements, should be considered in the logical circuit level [3].

In logic circuit level, propagation of the pulses should be analyzed. Some pulses may disappear by masking effects of logical gates and flip-flops. For example, narrow pulses are filtered by logic gates, and logical operation of gates and flip-flops can restrain propagation of the pulses. Only failure output signals of combinational circuits, which are actually latched by flip-flops, affect malfunctions of internal state transition of the circuit [4, 5]. Memories, which contain huge number of transistors with regular structure, have to be analyzed by different approaches utilizing the regularity [6].

In register transfer and system architecture levels, even if a failure result of computation by soft error is stored in memory, a system error occurs only when the wrong data is read out and used in the subsequent computation process affecting the final output of the systems. Screening of the ineffective events on failure data is the major problem of the analysis [7].

Combining abovementioned analysis tools, you can evaluate soft error rate of a VLSI system. It is difficult to analyze the propagation of the effect of soft error, because the propagation process is very complicated and also hard to formulate as deterministic process. Since the influences of the neutron collisions do not always cause soft error in the system architecture level and the relations between collisions and system behavior are difficult to analyze deterministically, dependability of the system must be modeled as probability of the malfunction of the system behavior caused by the collisions of neutrons. Statistical and probabilistic approach has to be introduced to analyze the causal effects between collisions and system failures.

References

1. L.T. Wang, K.T.T. Cheng, Y.W. Chang (eds.), *Electronic Design Automation: Synthesis, Verification, and Test, Morgan Kaufmann* (2009)
2. M. Yoshimura, Y. Matsunaga, Bridging the gap between device level modeling and register transfer level modeling, in *1st RIIF Workshop*, pp. 1–6 (2013)
3. T. Takata, Y. Matsunaga, A robust algorithm for pessimistic analysis of logic masking effects in combinational circuits. IPSJ Trans. Syst. LSI Des. Methodol. **5**, 55–62 (2012)
4. T. Takata, M. Yoshimura, Y. Matsunaga, Efficient fault simulation algorithms for analyzing soft error propagation in sequential circuits. IPSJ Trans. Syst. LSI Des. Methodol. **6**, 127–134 (2013)
5. M. Yoshimura, Y. Akamine, Y. Matsunaga, An exact estimation algorithm of error propagation probability for sequential circuits. IPSJ Trans. Syst. LSI Des. Methodol. **5**, 63–70 (2012)

6. M. Sugihara, T. Ishihara, K. Murakami, Architectural-level soft-error modeling for estimating reliability of computer systems. IEICE Trans. Electron. **E90-C**(10), 1983–1991 (2007)
7. M. Sugihara, On synthesizing a reliable multiprocessor for embedded systems. IEICE Trans. Fundam. **E93-A**(12), 2560–2569 (2010)

Chapter 14
Formal Verification and Debugging of VLSI Logic Design for Systems Dependability: Experiments and Evaluation

Masahiro Fujita, Takeshi Matsumoto, Amir Masoud Gharehbaghi, Kosuke Oshima, Satoshi Jo, Hiroaki Yoshida, Takashi Takenaka and Kazutoshi Wakabayashi

Abstract In this chapter, we discuss logic verification and debugging methods with evaluation results on the industrial designs as well as benchmark circuits. First, formal verification methods, mainly for formal equivalence checking problems, are quickly reviewed with respect to C-based design flows. Through various evaluations including the ones with industrial designs, it is found that, if the two design descriptions are textually or structurally close, formal verification is useful and scalable, whereas if the two are very different, such as the case between designs in C and RTL/gate level, unless information on internal signals are available, the verification problem remains very hard. As an attempt to overcome the problem, a new method, which generates C descriptions from RTL/gate level in order to convert the equivalence checking problems between C and RTL/gate level into the ones between two C designs is introduced. Then, formal logic debugging methods are evaluated using industrial buggy circuits. The correction problems for the buggy designs are classified into three situations, and each one is discussed with experiments on industrial designs. In the first two situations, which covers around 70–80% of bugs in industrial designs, the strategy to transform the buggy designs into correct ones is fairly simple and also scalable. In order to cover the rest of the buggy designs, however, the most general and difficult situation which needs global topological changes must be dealt

M. Fujita (✉) · A. M. Gharehbaghi · S. Jo
The University of Tokyo, Tokyo, Japan
e-mail: fujita@ee.t.u-tokyo.ac.jp

T. Matsumoto
Ishikawa National College of Technology, Tsubata, Ishikawa, Japan

K. Oshima
Hitachi Ltd., Hitachi, Tokyo, Japan

H. Yoshida
Fujitsu Laboratories of America, Sunnyvale, CA, USA

T. Takenaka · K. Wakabayashi
NEC, Kawasaki, Japan

S. Asai (ed.), *VLSI Design and Test for Systems Dependability*,
https://doi.org/10.1007/978-4-431-56594-9_14

with. As an attempt to resolve the problem, a completely new approach for such a situation, which searches for appropriate and minimum sets of signals for gates without explicitly generating the functions of the gates is introduced.

Keywords Formal equivalence checking · Logic design debugging · Satisfiability checking · Difference of descriptions · Symbolic simulation

14.1 Goal of Logic Verification and Necessity of Formal Analysis

As digital systems become larger and larger, it is more critical and more time consuming for a design to be assured to be logically correct. The target hardware may not work correctly due to varieties of reasons. For example, if a design operates too slowly, it may not satisfy the timing constraints (mostly inferred from the setup time and hold time of flip-flops), and it generates wrong output values depending on input values. However, the most common reason why the hardware does not work as intended is simply due to logical bugs in the design. Just like software bugs, designers introduce logical bugs into the design descriptions which are synthesized to become actual chips.

Logic verification is the process to check if given designs behave correctly before fabricating the chips, and there are two types of problems: model checking and equivalence checking. Model checking, or sometimes called property checking, is trying to make sure that the behavior of a given design satisfies the properties associated with the design. Generally speaking, properties are also given separately from the design as the specification. Equivalence checking is trying to make sure that the two given designs behave equivalently. Both are important items to be certified, and depending on the situations in design flows where logic verification is performed, appropriate one is checked. For example, if designers have a number of properties, or sometimes called assertions, as the specifications for the target designs, model checking should be applied. On the other hand, if designers have a so-called "golden model" for the target design and they have also another implementation design, the golden model and the implementation design must behave equivalently, and hence, equivalent checking should be applied. Golden models can be just the previous designs whose functionality should be kept in the current designs, or they are given in high-level design languages such as C, and the implementation designs in gate level should behave equivalently. These are becoming common problems in C-based design methodologies, and this section deals with the equivalence checking between high-level design descriptions in C and the corresponding gate-level implementation designs.

There are basically three ways, i.e., simulation, emulation, and formal analysis (formal verification), to make sure the correctness of a design. The most commonly used method is simulation, that is, simulating a design with a set of given input patterns. As logic simulators are available for all design phases, such as C level designs, Register Transfer Level (RTL) designs, gate level designs, and more detailed ones, logic simulation is the most basic and widely used method to make sure the correctness of the target designs. The main problem with logic simulation is that it certifies the correctness of the given design only for the input patterns on which logic simulation has checked. As for the input patterns which are not yet tried by logic simulation, no one knows whether it may generate the correct output patterns or not. Also, logic simulation is very slow when the target design becomes large. As a consequence, not so many input patterns are checked, which results in poor assurance on the correctness of the target design.

If the input patterns are generated randomly, some specific portions of the designs may be activated or observed through simulation only with very low probability, which are called "corner case" problems. For example, if a design has a conditional statement, *if* $(X = 1234)$ *then* do_A *else* do_B;, bugs in do_A may not be detected by any input patterns which do not make the value of X to be 1234. Definitely, for large and complicated designs, verification methods besides logic simulation must be applied.

Logic emulation is the method which significantly speeds up logic simulation by utilizing special hardware or FPGA (Field Programmable Gate Arrays). As logic emulation performs the same functionality of logic simulation, and the speed is 1,000 times or faster, much more input patterns can be checked with logic emulation compared to logic simulation which is based on simulation software rather than special hardware. With the speed of logic emulation, it is often possible to run application programs on top of the target design, and by running them, much more logical bugs can be found. This is because if application programs run for longer cycles, they activate the target design in various ways and may hit some of the corner cases with relatively good possibility. Although in the current design flows for large and complicated designs, logic emulation is one of the most critical methods for logic verification, it may still miss some important corner cases. Therefore, another method which can cover the remaining corner cases should be applied to make sure practically sufficient correctness of the design.

Formal verification or formal analysis of design descriptions is to apply mathematical reasoning to the verification of the target design. It is equivalent to checking all the input patterns to see if the output patterns are correct in "implicit" ways. It is obvious that checking on all input patterns are practically impossible if that is performed "explicitly", like logic simulation or emulation. However, it may be feasible to do so if that is performed implicitly. There can be mathematical proofs which say some small subsets of "symbolic" input patterns can infer 100% correctness of the target design if the simulation is performed "symbolically", which is called symbolic simulation. Instead of using concrete values, such as 0 and 1, symbolic simulation accepts symbolic input values which include symbolic constants. As symbolic constants represent both 0 and 1, or more generally they represent all possible integer values in the case of an integer variable, one symbolic simulation covers a large set of concrete input patterns and may hit corner cases in much more efficient ways than logic simulation and emulation. For example, the conditional statement discussed

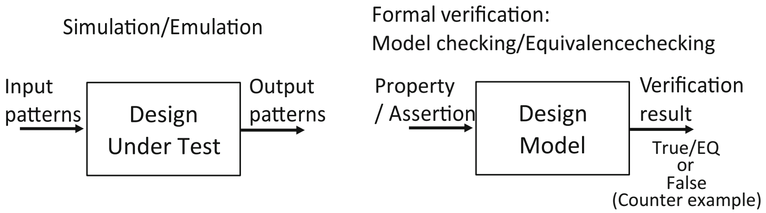


Fig. 14.1 Simulation/Emulation and formal verification

above relating to corner case problems, *if* $(X = 1234)$ *then* do_A *else* do_B;, a symbolic constant for X covers all possible values and hence they include 1234.

The output patterns by symbolic simulation have not only symbolic constants but also logic expressions which consist of symbolic constants and various logic/arithmetic operators. Those symbolic output patterns are mathematically analyzed by Satisfiability (SAT) checking software, such as the one shown in [1] or Satisfiability Modulo Theories (SMT) solvers, such as the one shown in [2]. These give mathematical proof on the correctness of the symbolic simulation results. The performance of SAT/SMT solvers have been dramatically improved for the last ten years or so, symbolic simulation is now a powerful way to make sure the correctness of the target designs through formal analysis of the symbolic simulation results.

The difference between simulation/emulation and formal verification is illustrated in Fig. 14.1. It is important to recognize that logic simulation/emulation guarantees the correctness of the target design only for the input patterns that are applied, whereas formal verification can cover all possible input patterns with symbolic values. In the following, we discuss formal equivalence checking methods under C-based design flows. More detailed discussion on formal verification can be found, for example, in [3, 4] and a textbook on logic verification of System on Chip (SOC) [5].

If logic verification processes find a bug, i.e., for some input patterns the output patterns are shown not to be correct, logic debugging processes must be applied. So in the second part of this chapter, logic debugging methods with formal analysis is discussed with experimental results on benchmark circuits and designs from industry.

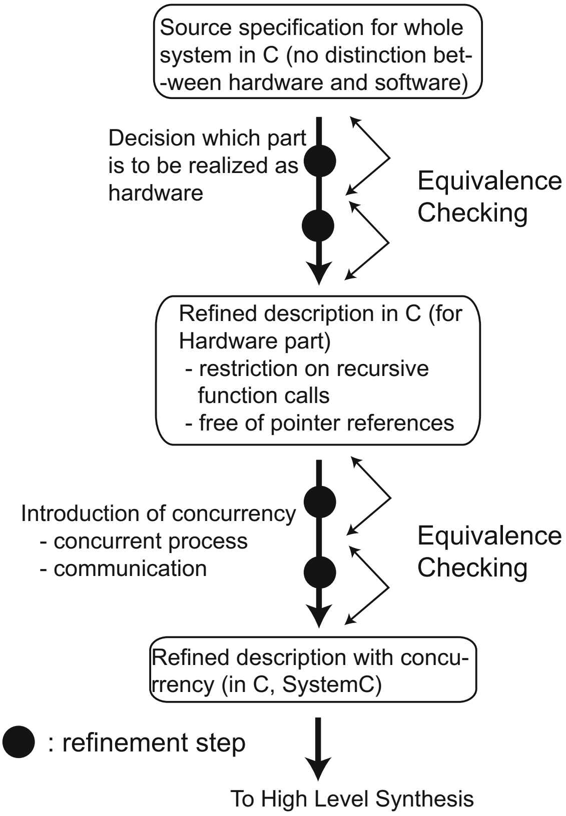
This chapter is organized as follows. In the next section, C-based design flows and how equivalence checking should be applied are discussed. Two common situations are picked up and the performance of the state-of-the-art equivalence checking methods are shown with experimental results. Then, in the following section, automatic logic debugging methods with formal analysis are discussed with various experimental results on industrial designs. A detailed discussion on logic debugging methods is also given in Sect. 11.2. The final section gives concluding remarks.

14.2 Formal Equivalence Checking Under C-Based Design

14.2.1 C-Based Design Flow and Logic Verification

C-based design is to start the design processes with a C description for the target system. C or C++ or their extensions, such as SystemC [6] and SpecC [7] used to describe the behaviors of the target. Although C-based design can be used for pure hardware systems, C-based designs are typically applied to hardware-software co-designs, as C can describe software as well. A typical design flow of C-based design for hardware–software co-systems is shown in Fig. 14.2. It starts with a functional description in C which captures all of the required functions in the target system. Then, based on the IP (Intellectual Property, existing designs) and other constraints, which functions are to be implemented in hardware and which are in software are determined, which is called hardware–software partitioning. The functions to be implemented with software follow a regular software development flow, and so, they are omitted from the figure.

Fig. 14.2 Series of refinement steps for more effective and high-quality high-level synthesis


Source specification for whole system in C (no distinction bet--ween hardware and software)
Decision which part is to be realized as hardware
Equivalence Checking
Refined description in C (for Hardware part)
- restriction on recursive function calls
- free of pointer references
Introduction of concurrency
- concurrent process
- communication
Equivalence Checking
Refined description with concu-rrency (in C, SystemC)
● : refinement step
To High Level Synthesis

Functions to be implemented with hardware must be redescribed in such a way that the descriptions are friendly for hardware implementation. For example, global variables in C may not result in efficient hardware, as they are referred by many functions, which become many wire connections in the implementation. Instead, communication among functions should be minimized as much as possible to make the layout process of hardware design less problematic. In addition, some types of C descriptions, such as complicated pointer references, should be converted into simpler descriptions in order to utilize high-level synthesis tools more effectively. Moreover, some of the functions can be redescribed to be executed in parallel for higher performance. After those rewriting, high-level synthesis tools automatically refine the C descriptions into RTL designs, which are further synthesized into gate-level designs by logic synthesizers. As for details of how to use high-level synthesis tools and their technology, there are a number of textbooks, such as [8].

High-level synthesis tools generate RTL designs in hardware description languages. Those can be simply processed by logic synthesis tools or some additional optimization, such as introduction of clock gating for lower power designs and scan paths for design for testability, may be performed before logic synthesis.

One thing to be noted here is that the quality of high-level synthesis results highly depends on the way the target hardware is described in C [8]. There are many implicit rules for efficient and high-quality high-level synthesis. As the original C descriptions may not follow these rules, typically manual refinements on the C description should be performed before applying high-level synthesis tools, which are parts of refinements in the design flow of Fig. 14.2. There are series of manual refinement steps in such a way that the final C description is very friendly to high-level synthesis tools, that is, high-level synthesis tools can generate high-quality RTL designs.

Therefore, there are basically two equivalence checking problems associated with C-based design flows. The first one is to make sure the refinement steps applied to the original C description keep the behaviors of the hardware. The other one is to check the equivalence checking between the C description and its synthesized RTL or gate level design description. Both are important problems, and the latter is more difficult and complicated process than the former, as the two descriptions to be compared are very different, in general. It is often required to use information on the relationships among internal signals between the two descriptions in order to process large and complicated designs for the latter equivalence checking problem. Especially that is the case when implementation design in RTL or gate level is complicated in the sense that scheduling of operations, such as parallel and pipeline processing, are very different from the C description.

As for the former equivalence checking problems, a very efficient equivalence checking method for the equivalence checking of each step of refinements is presented in the following. As series of refinements can be analyzed and verified by repeatedly applying formal analysis to each step of refinements, the method is very effective and scalable compared to the equivalence checking between C designs and RTL/gate-level designs.

14.2.2 Equivalence Checking Problems in C-Based Design Flow

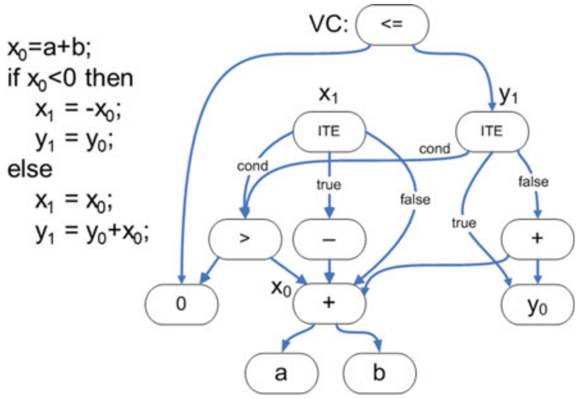
As discussed above, there are two important equivalence checking problems associated with the C-based design, which are discussed in the following.

14.2.2.1 Equivalence Checking Between Two Designs in C

Symbolic simulations are applied to both of the two C designs, and then the results are compared with SAT/SMT solvers. The results of symbolic simulation are formulas having symbolic constants that represent the values of the input variables and arithmetic and logical operators. For each statement in C, symbolic simulators generate the corresponding expression. As the symbolic simulation results must be compared, symbolic simulations must finish, meaning that equivalence checking is performed under bounded numbers of executed statements, which is called bounded equivalence checking. If the C descriptions have infinite loops, there may not be any way to finish computations, and so the bounded equivalence checking becomes incomplete in the sense that equivalence can only be checked up to the bounded number of executed statements. This is mostly acceptable, as simulation and emulation are also bounded analysis, although unbounded equivalence checking is desired, if ever possible.

Symbolic simulation results are generally represented with shared graph structures. An example is shown in Fig. 14.3. Here, a portion of a program is symbolically simulated and the results are shown. As can be seen from the figure, expressions for each statement are represented as subgraphs, and they are shared as much as possible. Conditional statements, such as if statements, need branches for then part and else part when performing symbolic simulation. This means there can be exponentially many execution paths with respect to the number of conditional statements.

Fig. 14.3 Symbolic simulation results represented by a shared graph



```
x0=a+b;
if x0<0 then
   x1 = -x0;
   y1 = y0;
else
   x1 = x0;
   y1 = y0+x0;
```

Table 14.1 Equivalence checking results for AES encryption circuits

Design	Time for equivalence check (min)	Variables in SAT problem instance	Clauses in SAT problem instance	Number of symbolically simulated statements
AES1	130	277,270	1,271,456	6,705
AES2	431	554,432	2,870,778	13,358

In order to avoid that symbolic simulation results of the then part and the else part of an if statement are merged as shown in the figure. With this merging, the size of the shared graphs grows only linearly with respect to the number of statements symbolically simulated. If the goal is to just symbolically simulate the descriptions, millions of lines can be simulated within a couple of minutes. However, for equivalence checking, the results of symbolic simulation must be compared with SAT/SMT solvers, and so the performance of the equivalence checking is determined by how large formulas or expressions can be processed by SAT/SMT solvers.

An experiment is performed in order to understand how many symbolically executed statements can be checked for equivalence with the state-of-the-art SAT/SMT solvers. The example design is an AES encryption design which has around 200 lines of C codes. It is commonly and widely used for high-level synthesis benchmarks, and the synthesized ones are actually used in some products. The synthesized hardware by a high-level synthesis tool and a logic synthesis tool has 174,810 gates. Although this has only 200 lines of codes, there are a number of for-loops inside, and consequently, the number of total executed statements are in the order of tens of thousands. As said before, equivalence is checked with a bounded number of executed statements. By manually changing the number of iterations of for-loops inside AES designs, two equivalence checking are performed; one is with 6,705 executed statements and the other is with 13,358 ones. For the analysis of symbolic execution results, miniSAT solver [1] is used. As this design has a lot of bit-level operations, SMT solvers generally show similar or poorer performance than SAT solvers. The results are shown in Table 14.1.

All experiments shown in this chapter are based on the following machine or computationally similar environments: Corei7-3770 (3.4 GHz) and 16 GB of memory under Linux Kernel 4.4.

State-of-the-art SAT solvers can generally process problems having several millions of variables and clauses, and the AES2 is approaching those limits. This indicates that around a couple of tens of thousands of symbolically executed statements is a sort of maximum for equivalence checking if we simply apply SAT/SMT solvers to the symbolic simulation results.

For larger designs, methods in which the true difference between the two designs are extracted and analyzed have been proposed [9–12]. As is the case of C-based designs shown in Fig. 14.2, most of the two descriptions to be compared are textually or structurally the same. There are a number of small portions where the two

Table 14.2 Experimental results on MPEG4 and elevator controller designs

Design 1	Design 2	Result	Time	No. of extensions
MPEG4_org	MPEG4_rev1	Equivalent	3.3 s	0
MPEG4_org	MPEG4_rev2	Inequivalent	13.2 s	80
Elv_org	Elv_rev1	Equivalent	1.8 s	1
Elv_org	Elv_rev2	–	>12 h	4

designs are actually described in different ways. By extracting such difference first, symbolic simulation can be applied only to that difference part, which results in dramatic reduction in the number of statements to be symbolically simulated. This method is applied to a couple of benchmark/industrial designs which are step-by-step refined for a high-level synthesis tool. The results are shown in Table 14.2. The example designs are an MPEG4 decoder (6,329 lines in C) and an elevator controller (3,349 lines in C). Following the refinement steps for better high-level synthesis, constant propagating and constant folding are applied to these designs, which generate MPEG4_rev1, MPEG4_rev2, Elv_rev1, and Elv_rev2. With these refinements, the resulting designs by high-level synthesis become significantly smaller and faster. So these are kinds of necessary steps for better designs. As can be seen, the time for equivalence checking remains very small. Please note that if we apply the method which simply performs symbolic simulation on the entire designs without the extraction of the actual difference, SAT/SMT solvers cannot finish their analysis.

Once the different portions are extracted, they are checked to be equivalence with symbolic simulation. One point to be noted here is that even if the different portions are not equivalent, the entire descriptions can be equivalent as a whole. Therefore, it is necessary to extend the portions to be checked for equivalence if the current ones are not equivalent. The last column in Table 14.2 shows the numbers of such extensions.

There is one problem with the equivalence checking method based on extraction of difference in two designs. If the two designs are actually equivalent, which are the first and third cases of Table 14.2, the method finishes and shows the equivalence very quickly. On the other hand, as can be seen in the last result in Table 14.2, if the two designs are actually nonequivalent, it may not finish, since in the worst case, it has to symbolically simulate entire designs. So practically, we may have to conclude that if the equivalence checking method with the extraction does not finish within a pre-specified time, we temporarily conclude that they are not equivalent and switch to simulation/emulation to look for counter examples.

14.2.2.2 Equivalence Checking Between Designs in C and RTL/Gate-level

In this case, we can apply symbolic simulation to the designs in C and RTL/gate level, and then compare the results by SAT/SMT solvers just like the same way discussed above. However, the problem is much harder than the above, as the two descriptions to be compared are very different in general. In most cases, in terms of descriptions, most portions are different in the two designs, therefore, almost entire designs must be symbolically simulated, which results in poor performance as equivalence checking. The number of simulated statements to be analyzed by SAT/SMT solvers cannot become larger than 100,000 statements or so, according to the experiments above. In general, the number of lines of codes in RTL/gate level can be more than 10 times larger than the ones in C, as RTL/gate-level designs are specifying all activities of the hardware for every clock cycle. Therefore, the number of symbolically simulated statements can easily become more than 100,000.

Therefore, it is essential to identify the real difference between the two designs in C and RTL/gate level before applying symbolic simulation. Unfortunately, they are textually very different descriptions, and it is very hard to automatically recognize the correspondence of internal signals between a design in C and one in RTL/gate level since their order of executions and even the ways of computing can be very different. In order to deal with larger designs, information on the relationships among internal signals between the two designs must be available. With those information, the equivalence checking problem can be decomposed into much smaller ones, although automatic extraction of the information is still a challenging problem. Therefore, the existing equivalence checking methods work well only if such information on relationships among internal signals are given by designers and others. Some commercial tools are actually doing this by having an alliance with high-level synthesis companies to get such information directly from the high-level synthesis tools.

As information on internal signal correspondence may not be easily available, another approach to the equivalence checking problem is better to be explored. One approach is to automatically generate C descriptions from the RTL/gate-level designs. If this is feasible, the equivalence checking problem between designs in C and RTL/gate level becomes the one between two designs in C, and the methods discussed in Sect. 14.2.2.1 including the difference extraction may be applied. In general, it is hard to automatically generate corresponding C designs from RTL/gate-level designs from the scratch. Moreover, if the generated C descriptions are very different from the original C description, the equivalence checking between them still remains very hard.

However, it may be feasible if most of the C designs corresponding to the RTL/gate-level designs can be manually predetermined and the problem is to generate the missing portions automatically. One such situation is the case where the generated design in C from RTL/gate level is very close to the original design in C. When that is the case, the design in C which corresponds to the RTL/gate level can be automatically generated by slightly modifying the original design in C. First, a set of small number of statements from the original design in C are selected, and they are replaced with statements having symbolic variables which correspond to variables, operations, and constants in the designs. This is called parameterized design in C. Then, the generation problem is to find appropriate variables, operations, and constants for the symbolic variables by which the resulting C description behave equivalent to the RTL/gate-level designs. This problem can be formulated as Quantified Boolean Formula (QBF) and can be solved by repeatedly applying SAT/SMT solvers. The basic algorithm is the same as the one used in the debugging methods discussed in Chap. 11. If we can generate the design in C from RTL/gate level, that is compared with the original design in C by the method discussed in Sect. 14.2.2.1. As the difference between the two designs is now very close, scalable equivalence checking can be expected. We have applied the generation method to the gate level designs which are high level synthesized from the AES designs in Table 14.1. There are around 100,000 gates in the gate-level designs. It takes around 2–5 min to generate the designs in C starting with the parameterized designs in C which are provided by designers. The equivalence checking time is very quick and is in the order of several seconds with the method which is an extended one from the one shown in Sect. 14.2.2.1 for C descriptions. This is a very preliminary result and more experiments are to be performed.

14.2.2.3 Evaluation with Industrial Designs

The above methods were evaluated with industrial designs to see how widely they can be applied practically. The example design is a custom floating point unit which may be used in various VLSI chips as IP (Intellectual Property) and has hundreds of thousands of gates once it is logically synthesized to gate level. First, we tried to apply the equivalence checking methods to their C and RTL designs, but it failed simply due to too many numbers of lines in Verilog or VHDL RTL codes. Symbolic simulation results are too complicated even for the state-of-the-art SMT solvers, such as [2]. For these kinds of designs having many number of lines in HDL, information on the relationships among internal signals is essential for the entire design to be decomposed into a number of much smaller sub-designs. Once they are decomposed, they may be equivalence checked one by one independently. Unfortunately, that kind of information on the relationships among internal signals is not available for this experiment.

Therefore, we switched to the equivalence checking problems between two designs in C. This example has a series of small steps of refinements in order to generate high-quality circuits by high-level synthesis tools. One such refinement example is shown in Fig. 14.4. As shown in the figure, scalar multiplication, “val = val * 10” is replaced with a set of statements of shift and add operations. It is well known that in most cases, implementing scalar multiplication with shift and add operations are much more efficient in hardware, and so this kind of design refinements are very common.

The extraction tool which generates the true difference between the two C designs generates the C descriptions shown inside the boxes in the figure. As you can see these can be quickly or immediately proven to be equivalent with symbolic simulation followed by SAT/SMT analysis. Please note that this equivalence checking is very quick regardless of the number of lines of C descriptions in the entire designs to be compared. So this is a very scalable verification method if the extraction process ever works. For the comparison between two C designs, there have been developed several methods by which such extraction can be automated. However, as stated before, it is still hard to develop such extraction methods for the equivalence checking problems between designs in C and RTL/gate level.

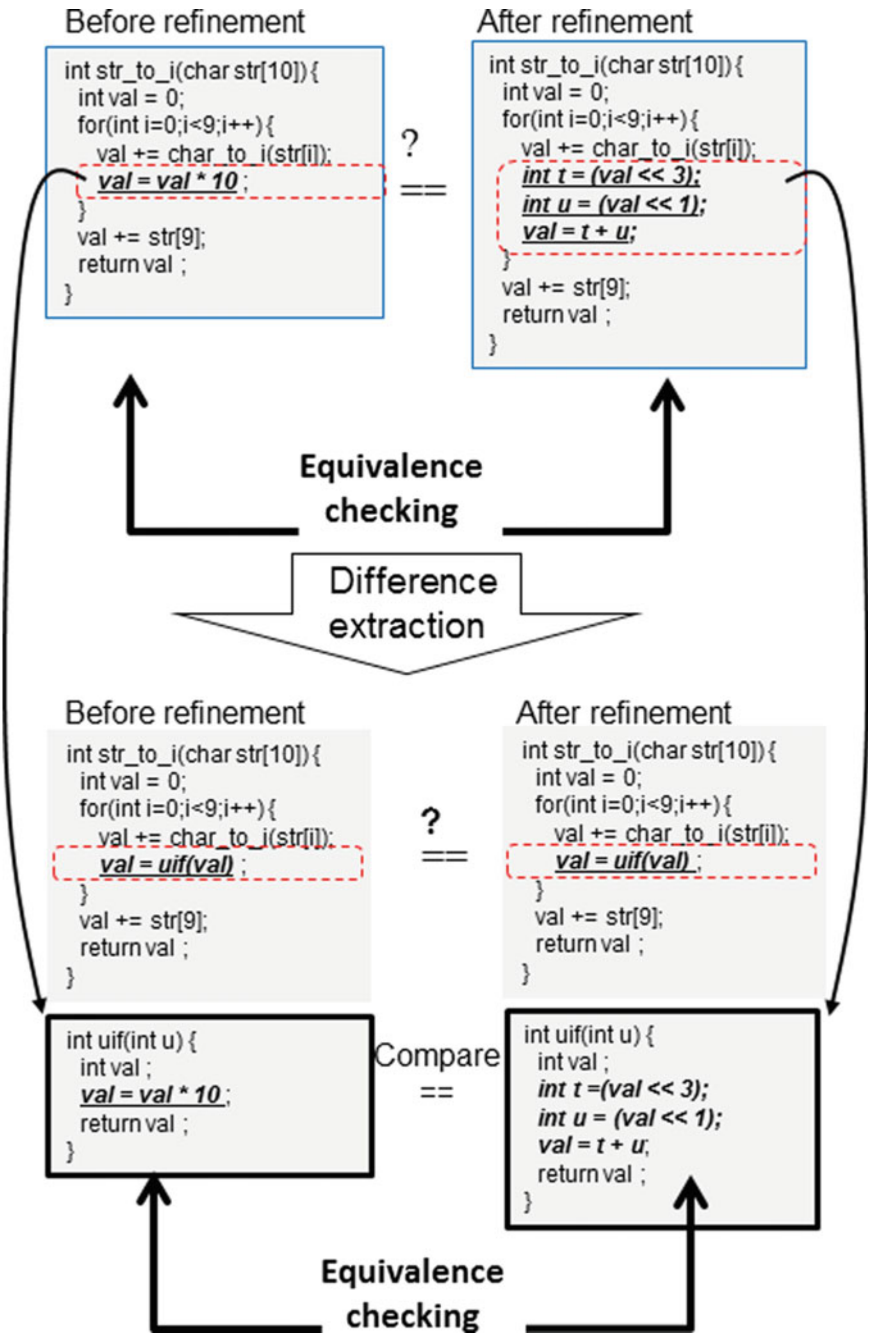
14.3 Logic Debugging with Formal Analysis

The basic problems, algorithms, and experimental results including the designs from industry are shown in Sect. 11.2. Here, we overview the problems and their associated debugging methods including a new method which can debug all of the industrial buggy designed we obtained. Logic debugging consists of two phases. The first phase tries to understand which portions of the buggy designs are actually the cause of the errors. For that, path tracing and its extension to SAT formulation are the state-of-the-art methods. The second phase actually tries to correct the buggy designs based on the results of the first phase. In this section, we only discuss the latter phase as there are still lots of room to be improved for dealing with that phase of the logic debugging. This phase of the logic debugging problems are classified into three situations: correction can be made by changing only the functions of the gates, correction can be made by changing both the functions and inputs of the gates locally, and correction can only be made by changing both the topologies of circuits globally and also functions of gates. The three situations are illustrated in Fig. 14.5b–d. Figure 14.5a is the original buggy circuit. In Sect. 11.2, the method works for the first two situations, (b) and (c), are presented and evaluated. Here, we briefly review them with industrial evaluation, and then show a new method targeting the third situation, (d), with preliminary industrial experimental results.

14.3.1 Correction by Changing the Functions of Gates

This corresponds to the case of (b) in Fig. 14.5. As can be seen from the figure, the functions of a set of gates (in the figure, two gates) are changed to other functions (one is from OR to EOR, and the other from AND to OR) due to logical bugs. Clearly, these bugs can be corrected by transformations on types of logic gates. The problem to be solved can be formulated as Quantified Boolean Formula (QBF) and can be solved by repeatedly applying SAT solvers, as shown in Sect. 11.3.2 of Chap. 11.

The method has been evaluated by benchmarks as well as several industrial designs. The bugs inserted into benchmark circuits are somehow artificial in the sense that the designs are modified to have logical bugs which can be corrected by



```
int str_to_i(char str[10]){
  int val = 0;
  for(int i=0;i<9;i++){
    val += char_to_i(str[i]);
    val = val * 10 ;
  }
  val += str[9];
  return val ;
}
```

```
int str_to_i(char str[10]){
  int val = 0;
  for(int i=0;i<9;i++){
    val += char_to_i(str[i]);
    int t = (val << 3);
    int u = (val << 1);
    val = t + u;
  }
  val += str[9];
  return val ;
}
```

```
int str_to_i(char str[10]){
  int val = 0;
  for(int i=0;i<9;i++){
    val += char_to_i(str[i]);
    val = uif(val) ;
  }
  val += str[9];
  return val ;
}
```

```
int str_to_i(char str[10]){
  int val = 0;
  for(int i=0;i<9;i++){
    val += char_to_i(str[i]);
    val = uif(val) ;
  }
  val += str[9];
  return val ;
}
```

```
int uif(int u) {
  int val ;
  val = val * 10 ;
  return val ;
}
```

```
int uif(int u) {
  int val ;
  int t =(val << 3);
  int u = (val << 1);
  val = t + u;
  return val ;
}
```

Fig. 14.4 Floating point unit designs whose refinements can be formally equivalence checked through extraction of the difference

changing only functions of a set of gates, and so those bugs are guaranteed to be correctable by changing the functions of the gates. These examples are helpful in understanding the performance of the method or how scalable the method is. The experimental results show that circuits having around 100,000 gates can be automatically corrected in several minutes.

In order to see the actual performance of the correction method for real designs, several buggy circuit examples are obtained from industry. The designs are mostly for communication chips and their sizes range from several hundreds to several thousands of gates. Therefore, in terms of circuit sizes, the method should work well. If we apply the bug correction method based on changes of the functions of the gates, around 50% of bugs in industrial buggy designs are corrected, but the remaining 50% bugs cannot be corrected only with this correction method. This is because for the remaining 50% of the bugs, not only the changes of the functions of the gates but also the changes of the inputs to the gates must be taken into consideration.

14.3.2 Correction by Changing the Functions and Inputs of Gates

In order to change the inputs to the gates, a simple way is to add multiplexers to the inputs of the gates, which is shown in Fig. 14.5c. Depending on the values of control inputs of the multiplexers, different signals are connected to the inputs of the gates, and so effectively we can change the inputs of the gates as well as the functions of the gates. The details are shown in Sect. 11.2.

However, there is a problem: which signals should be connected to the multiplexers. There are lots of candidate signals in the circuits that can be connected, and it is

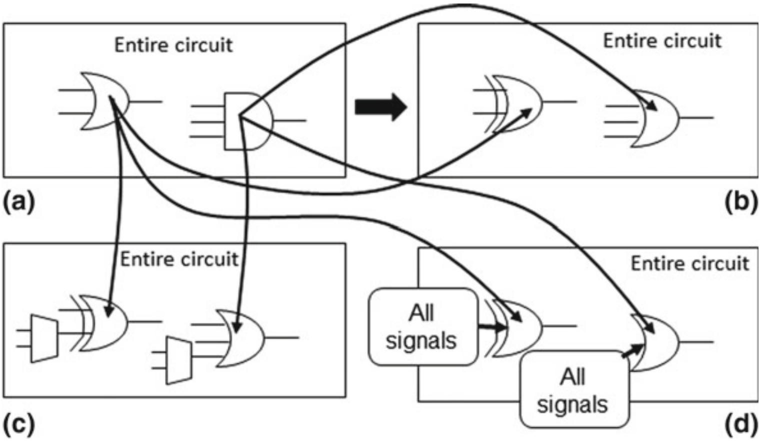


Fig. 14.5 Three situations happening when correcting the buggy designs

not easy to see which one works and which one does not work. Therefore, we have to try many connections, which can be too time-consuming. Although, theoretically all of the bugs in the industrial buggy circuits should be able to be corrected by this method, practically it cannot correct around half of the remaining bugs due to too many choices of signals to be added to the gates. Therefore, a completely new method which can efficiently and globally search for signals to be added to the inputs of the gates is required. The next section gives one such method.

14.3.3 A Method to Search for Good Inputs of the Gates

Here, the problem is the one shown in Fig. 14.5d. We can not only change the functions of the gates but also change the inputs of the gates to any sets of signals, and the signals to be added to the gates must be searched globally in the circuits. This is a new debugging problem, and there is a new approach [13] in the sense that it focuses only on finding the appropriate inputs for the selected gates, rather than trying to identify the appropriate functions of the gates. It does not generate the required functions of the gates, and it generates only the appropriate inputs of the gates guaranteeing that there exist functions for the gates under which the entire circuits become correct.

As shown in [13], this problem can be solved by iteratively applying SAT solvers, and so large problems can be efficiently solved. The candidate signals can be all primary inputs and internal signals, therefore, all of the remaining bugs in the industrial buggy designs can be corrected with this method. This is efficient in the sense that it does not search for the functions of the gates. Instead, it just guarantees the existence of the functions of the gates which make the entire circuit correct.

As this is a newly found method, we are exploring other applications of the method than the logic debugging, such as logic optimization. Because the method can dramatically change the circuit topology guaranteeing the correctness of the entire circuits, it could be a very powerful logic optimization method.

14.4 Conclusion and Future Perspectives

We have presented and summarized the performance of the equivalence checking methods associated with C-based design methodologies, and logic design debugging methods with formal approaches, by showing the experimental results on industrial designs as well as benchmark circuits.

As for the equivalence checking, if the two designs to be compared are close in terms of descriptions, fairly large designs can be processed. On the other hand, when the two designs are very different in descriptions, which is mostly the case of comparison between designs in C and RTL/gate level, unless information on relationships among internal signals are given, the equivalence checking problem remains very hard. A new method which tries to generate C designs from RTL/gate level automatically is introduced in order to convert the equivalence checking between designs and RTL/gate level into the one between designs in only C. A preliminary promising experimental results are shown.

In order to deal with larger designs, some kinds of modular verification, which tries to verify each function one by one rather than analyzing the entire descriptions all at once, is necessary. One way for such direction is to use the idea of scope bounding shown, for example, in [14]. With the scope bounding methods, the pre- and post-condition of the function execution can be automatically extracted from the entire descriptions, and so each function could be analyzed more independently, and consequently, we can expect more scalability even if the entire designs in C are very large. We are working on this direction with industrial designs as example.

As for logic debugging, more specifically on the correction phase of debugging, methods for the three situations shown above has been discussed with preliminary experimental results including the application to industrial designs, and a new logic debugging method which have covered all the logical bugs found in industrial designs. This method is to be further explored and evaluated.

Some of the developed methods, mostly the ones for logic debugging, have been implemented in the logic verification and synthesis tool, ABC, from University of California, Berkley [15]. They are available under the standard distribution of ABC. As the tool ABC is now used in industries, more industrial evaluations by various people and companies can be expected.

References

1. http://minisat.se/
2. https://z3.codeplex.com/
3. E. Clarke, O. Grumberg, D. Peled, Model Checking, MIT Press, Cambridge, Massachusetts (1999), ISBN: 9780262032704
4. A. Mathur, M. Fujita, E.M. Clarke, P. Urard, Functional equivalence verification tools in high-level synthesis flows. IEEE Design Test Comput. **26**(4), 88–95 (2009)
5. M. Fujita., I. Ghosh, M. Prasad, Verification Techniques for System-Level Design, Morgan Kaufmann, Burlington, Massachusetts (2007), ISBN: 9780123706164
6. http://www.systemc.org/
7. SpecC: Specification language and design methodology. Kluwer Academic Publishers
8. M. Fingeroff, High-level synthesis blue book, Xlibris, Bloomington, IN (2010), ISBN: 9781450097246
9. T. Matsumoto, H. Saito, M. Fujita, An equivalence checking method for C descriptions based on symbolic simulation with textual differences. IEICE Trans. **88-A**(12), 3315–3323 (2005)
10. T. Matsumoto, H. Saito, M. Fujita, equivalence checking of c programs by locally performing symbolic simulation on dependence graphs, in *International Symposium on Quality Electronic Design (ISQED)* (2006), pp. 370–375
11. T. Nishihara, T. Matsumoto, M. Fujita, Word-level equivalence checking in bit-level accuracy by synthesizing designs onto identical datapath. IEICE Trans. **92-D**(5), 972–984 (2009)
12. H. Yoshida, M. Fujita, Improving the accuracy of rule-based equivalence checking of system-level design descriptions by identifying potential internal equivalences, in *International Symposium on Quality Electronic Design (ISQED)* (2009), pp. 366–370

13. A.M. Gharehbaghi, M.Fujita, A new approach for debugging logic circuits without explicitly debugging their functionality, in *Asian Test Symposium (ATS)* (to appear in Nov 2016)
14. F. Ivancic, G. Balakrishnan, A. Gupta, S. Sankaranarayanan, N. Maeda, T. Imoto, R. Pothengil, M. Hussain, Scalable and scope-bounded software verification in Varvel. Autom. Softw. Eng. **22**(4), 517–559 (2015)
15. R. Brayton, A. Mishchenko, ABC: an academic industrial-strength verification tool. Comput. Aided Verif. **6174**, 24–40 (2010)

Chapter 15
Virtualization: System-Level Fault Simulation of SRAM Errors in Automotive Electronic Control Systems

Shigeru Oho, Yasuhiro Ito, Yasuo Sugure, Yohei Nakata, Hiroshi Kawaguchi and Masahiko Yoshimoto

Abstract In the coming age of self-driving cars, system-level testing of electronic control will become much more important to ensure dependable operation of automated functions. Modern VLSI devices are not always totally reliable. They can fail due to aging, electromagnetic excitation and many other reasons as described in the other chapters in this book. Therefore, dependable electronic systems must be tested against possible VLSI device failures. This may not be a common practice for meeting the ISO 26262 functional safety standard today, but deemed necessary for full-fledged self-driving cars in future. In this chapter, we demonstrate system-level simulation of SRAM errors and their impact on the design of electronic control. Automotive engine control is chosen as a test bed for this study. Model-based development techniques for automotive control systems are described first as the background and virtual electronic control units are introduced. A dependable SRAM architecture is proposed, and to test it in a practical use, a multilayer simulation modeling of an electromechanical system, its control software, and the SRAM design built-in microcontroller are discussed. To run a fault injection analysis in the SRAM chip at a large scale, a public cloud computing is used. The virtual computer machines in the cloud computing carry out the virtual engine control system simulation in which an instruction set simulator for the microcontroller executes the control software code step by step. The simulation system traces the outcome of the engine control system behavior upon a fault injection into SRAM to evaluate the dependable SRAM design. The large-scale

S. Oho (✉)
Nippon Institute of Technology, Minami-Saitama, Saitama, Japan
e-mail: oho@nit.ac.jp

Y. Ito · Y. Sugure
Hitachi Central Research Laboratory, Kokubunji, Japan

Y. Nakata · H. Kawaguchi · M. Yoshimoto
Kobe University, Kobe, Japan

S. Asai (ed.), *VLSI Design and Test for Systems Dependability*,
https://doi.org/10.1007/978-4-431-56594-9_15

fault analysis proposed here allows us to evaluate quantitatively the impact of the quality design of components on the entire system failure rate.

Keywords Electronic control unit (ECU) • Model-based development (MBD) Functional safety • Fault injection • Cloud computing

15.1 Automotive Control Systems and Model-Based Development

Modern automobiles are equipped with dozens of electronic control systems to achieve such functions as engine–power train management, anti-lock braking, electric power steering, vehicle stability control, and many more. In these systems, electronic control units (ECUs) play a central role in control operations with its built-in microcontrollers and control software. As automotive control advances, the electronics, and software of ECUs are becoming larger and more complex. Then, design and test of ECUs have also become time-consuming and costly. Automobiles are expected to evolve into autonomous self-driving cars. Validating control electronics of such robotic vehicles will be a great challenge to ensure the highest reliability and safety.

To cope with increasing complexity of electronic controls, automotive industry has been adopting model-based development (MBD) approaches, i.e., design and testing methods with computer simulation. Typically, automotive control systems consist of electromechanical components (physical plants), control algorithms to drive the mechanism, and ECUs to execute the control operations. To apply MBD techniques, these elements are formulated as mathematical, physical, and logical models as shown in Fig. 15.1. Commercially available modeling languages to describe the models include Matlab®, Modelica®, and VHDL-AMS [1], to name a few. They are chosen according to its engineering domains and users' preference. Regardless of the modeling methods and languages, the models are executed on computers and often called "virtual" systems.

By combining the virtual and real components, numerous MBD techniques have been invented and utilized in each phase of V-cycle of control system development as depicted in Fig. 15.2. Model-in-the-loop simulation (MILS) uses both virtual models of physical plants and control algorithms and verifies basic control system designs. When the control software is written with C-code, MILS turns to be software-in-the-loop simulation (SILS) and SILS can include detailed software functions. Rapid control prototyping (RCP) drives an actual hardware plant, executes the control algorithms real time, and proves the control strategy experimentally. Hardware-in-the-loop simulation (HILS) replaces physical plants with virtual model and verifies the control software installed in ECUs. Simulated processor-in-the-loop simulation (SPILS) uses a model of microcontroller to build a

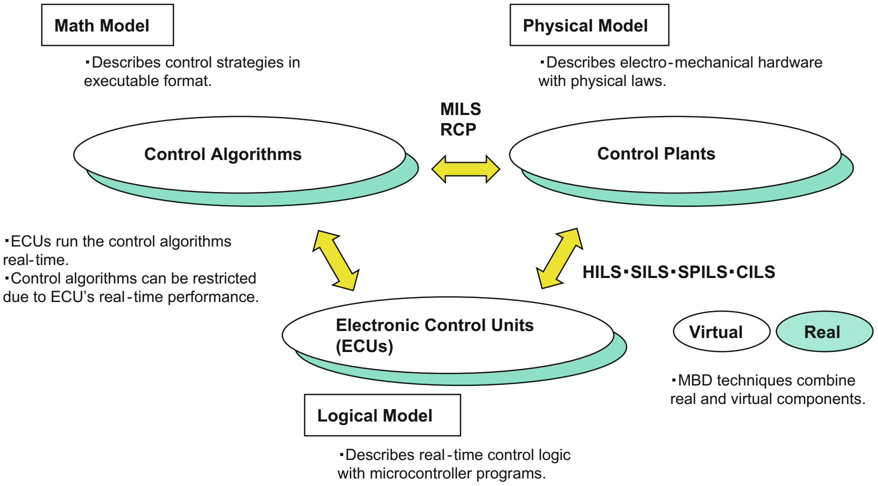

Math Model
•Describes control strategies in executable format.
Physical Model
•Describes electro-mechanical hardware with physical laws.
MILS
RCP
Control Algorithms
Control Plants
•ECUs run the control algorithms real-time.
•Control algorithms can be restricted due to ECU's real-time performance.
HILS•SILS•SPILS•CILS
Electronic Control Units (ECUs)
Virtual
Real
•MBD techniques combine real and virtual components.
Logical Model
•Describes real-time control logic with microcontroller programs.

Fig. 15.1 Modeling of automotive control systems

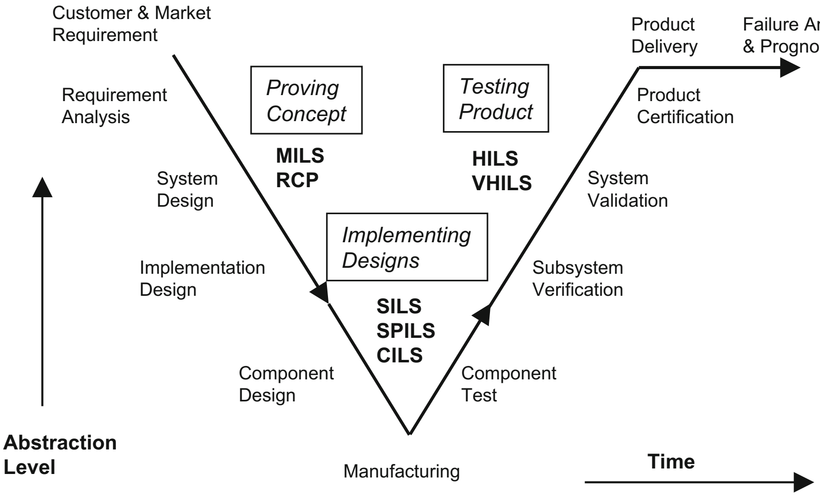


Fig. 15.2 Model-based development techniques in V-cycle development phases

virtual ECU and looks into the details of control software execution with the virtual ECU connected to a plant model.

As described above, MBD techniques cover wide ranges of system development phases and different system abstraction levels. Among them the SPILS, i.e., virtual ECU focuses on microcontroller operations in the lowest abstraction. To investigate the influence of faults in LSI hardware on control system behavior, we apply the virtual ECU to control system analysis. We call this approach as chip-in-the-loop simulation (CILS) to emphasize that the method evaluates a VLSI device design in application systems.

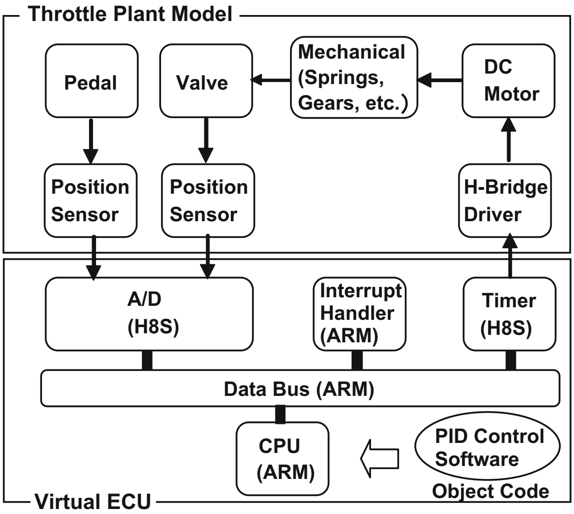
15.2 Virtual ECU and Its Applications

Virtual ECUs are built with a microcontroller model that simulates the executions of CPU instructions and peripheral functions of an actual microcontroller. The instruction set simulator (ISS) runs the exactly same binary codes of control software as the ones programmed in mass production ECUs. Therefore, the virtual ECUs provide an ultimate means of ECU testing in MBD approaches. The cycle accuracy of instructions and fidelity of peripheral behavior of a microcontroller model may restrict the accuracy of control system simulation. Even so, the complete transparency of microcontroller execution yields a lot of benefits in control system designs and verification.

Virtual ECUs have been applied to electronics throttle control [2, 3], engine control [4–7], power window control [8, 9], and adaptive cruise control systems [10]. Their applications include real-time code analysis, ECU fault analysis, and virtual HILS [10], a replacement of conventional HILS, and so forth.

A use case of virtual ECU is shown in Fig. 15.3, where an electronic throttle control system is built with plant and microcontroller simulators (in this case they are Saber® and CoMET®). The controller model here adopts the ISS for ARM®

Fig. 15.3 Virtual ECU applied to electronic throttle control



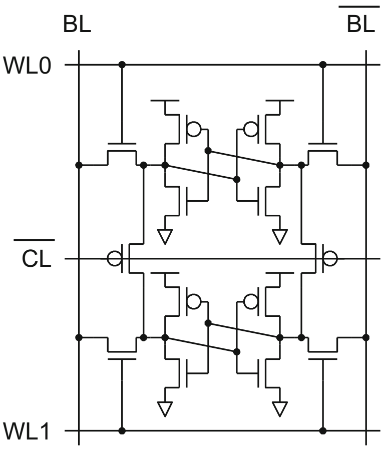
microprocessor core and ARM’s data bus, and interrupts handler architecture, while the analog-to-digital (A/D) converter and the timer unit are derived from Renesas H8S® microcontroller. Therefore, the virtual microcontroller in Fig. 15.3 does not exist as a real physical chip. Even so, it can run the object code of the PID control software for throttle operation to examine if the control algorithm is right, and to verify how effective the timer functions are. This is a typical case of CILS application mentioned above. CILS allows us to prove a new design concept before hardware manufacturing. This approach is applied to a new SARM design to evaluate its system benefits in this chapter.

15.3 Dependable SRAM

To ensure the operational safety of ever-advancing automotive controls, the new safety standard ISO 26262 “Road Vehicles—Functional Safety” was published in 2011 [11]. It defines four Automotive Safety Integrity Levels (ASILs) and automotive electronic control systems are classified into ASIL A through D accordingly with their safety risks upon system failures. Electronic stability control systems, for examples, are normally regarded as safety critical and classified as ASIL D. To comply with the ISO 26262 requirements, automotive microcontrollers have been updating their safety features, and latest products incorporate such functions as error check codes (ECC) and built-in self-test (BIST). Dual-core processors are also used in some microcontrollers to double-check the processor operation by comparing execution results.

If we seek the highest dependability of automotive electronic control in the cases of burst memory errors in microcontrollers used for non-stoppable systems such as brake and steering controls, the on-chip SARM itself needs to be improved further. A design approach to enhance SRAM’s dependability with the “7T/14T” scheme [12] is depicted in Fig. 15.4. In this design, the control input CL turns the operational mode of SRAM from “Normal” to “Dependable” and vice versa. In the dependable mode, the SRAM holds one-bit information with dual redundancy and becomes durable against bit errors, while in normal mode, it acts as a standard SRAM with a minimal increase in redundancy.

The dependable SRAM design should improve the reliability of the memory device. The important question is how often the dependable SRAM prevents a control system from malfunctioning. To justify the “7T/14/T”-dependable memory approach, we will apply the CILS technique and evaluate the memory design from system viewpoint in the following sections.



The dependable SRAM has a pair of conventional 6-transistor memory cell and two control transistors.

CL: Control Line
BL: Bit-select Line
WL: Write Line

Fig. 15.4 Dependable 7T/14T SRAM design

15.4 Multilayer Modeling of Dependable SRAM and Automotive Control Systems

When a device fails, the most crucial question is what happens next in the operation of control systems. When a bit data in SRAM corrupts, what is the impact on electronics control systems? The actual effect depends on the content of information stored in the SRAM; a corrupted control variable can result in erroneous control operation; an error in the CPU stack pointer most likely leads the microcontroller into total malfunction and system breakdown; an inversion in the least significant bit of a sensor data will be regarded as a minor noise and neglected. Automotive electronic engineers have been carefully managing the risk of SRAM errors. SRAM are tested when ECUs are switched on and important control data are stored redundantly. To prepare for the worst-case scenario of microcontroller malfunction, a backup processor stands by for “limp-home” mode operation in many ECUs.

As SRAM becomes more vulnerable and ECUs replace more human maneuvering, we need to seriously examine if the countermeasures to deal with possible SRAM errors really work as designed or backup means kicks-in timely. But injecting an error into SRAM at a specified point is practically impossible. Therefore, we investigate a method of fault injection into SRAM and apply the virtual ECU approach [12].

There is a long way to trace the cause-and-effect sequence from an SRAM error to vehicle control operation. SRAM itself has many reasons to corrupt. An error in SRAM somehow affects the microcontroller’s software execution. ECUs may deliver wrong signals to mechanical systems due to microcontroller malfunction. A control system can fail its vehicle maneuvering and the vehicle falls in critical situation. Top-down approach of modeling the multiple layers from vehicle motion to control system operation to ECU signals to microcontroller code execution to

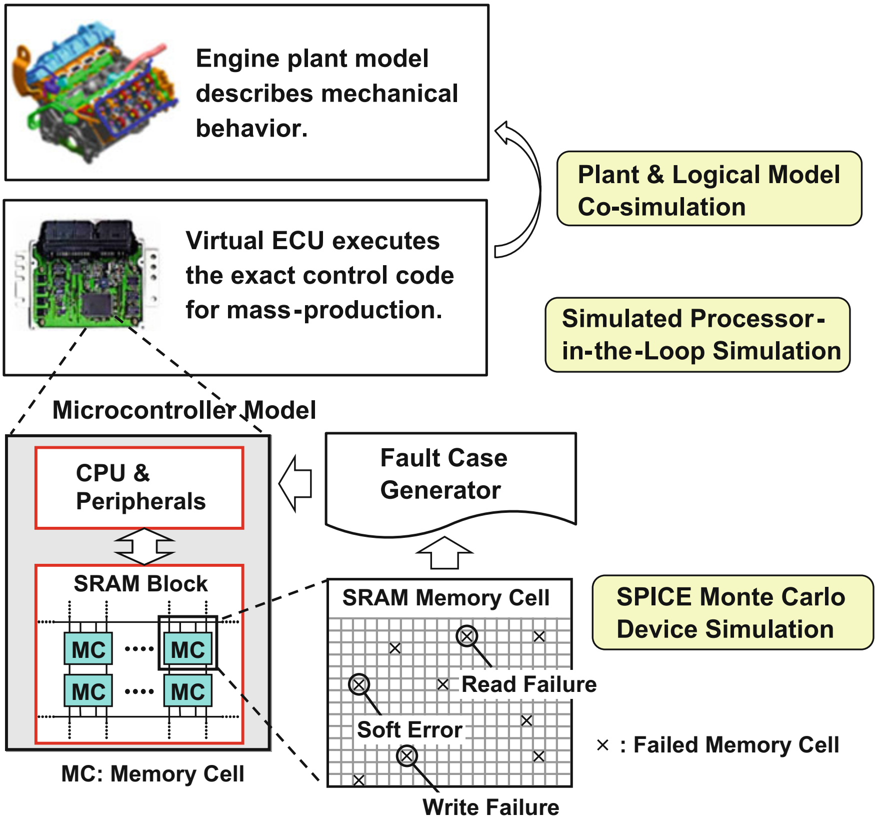

Engine plant model describes mechanical behavior.
Plant & Logical Model Co-simulation
Virtual ECU executes the exact control code for mass-production.
Simulated Processor-in-the-Loop Simulation
Microcontroller Model
CPU & Peripherals
SRAM Block
MC
MC
MC
MC
MC: Memory Cell
Fault Case Generator
SRAM Memory Cell
SPICE Monte Carlo Device Simulation
Read Failure
Soft Error
Write Failure
× : Failed Memory Cell

Fig. 15.5 Layered modeling of an automotive engine control system

SRAM device circuits and physics may be feasible. However, even with today's advanced computer performance, simulation of all of these processes will be an enormous task, and modeling works require huge multidisciplinary engineering.

We found a compromise here, and separated the SRAM device simulation from electromechanical modeling of vehicle control, and then connected them with the fault case generator (FCG) as shown in Fig. 15.5. The upper layer, i.e., the mechatronic system of automotive engine control adopted the SPILS approach discussed in previous sections. It includes an automotive engine simulator built with SIMULINK® and a virtual ECU that incorporates a Renesas SH-2A® microcontroller modeled with CoMET®. These simulators exchange their data periodically to achieve co-simulation. The virtual ECU also has a model of SRAM, and its contents are made to be manipulated from bit zero to one or vice versa at any SRAM addresses and at any timing of control execution.

In the lower layer, there is a device level simulation that describes the behavior of the SRAM cells. Here, we account for memory cell errors due to read/write margin failures and single event upsets (soft error). The margin failures reflect physical aspect of the memory cells, namely, process variations in semiconductor chip manufacturing, aging of the transistor devices, fluctuations in the supply voltage, and temperature dependency. The soft error is a temporary error and caused by such external excitation as neutron beams and electromagnetic radiation. Taking all of these parameters into account, we ran a Monte Carlo analysis with a SPICE device simulator and generated an SRAM bit error rate (BER) library as the summary for the memory error occurrence. The BER library lists a calculated probability of failures for a specified SRAM device. The dependable SRAM design with 7T/14T architecture described in Sect. 16.3 should yield a lower error probability than the conventional SRAM.

These numerals about error probability alone, however, do not clearly prove the benefit of the dependable SRAM for automotive control and ECU engineers. Therefore, the content of the SRAM BER library is fed into the upper layer of mechatronic simulator through the FCG. As shown in Fig. 15.6, the FCG inputs the design data and operational conditions of SRAM, looks up the BER information, and outputs the SRAM failure data pattern in a time sequence. The virtual ECU receives the BER data from the FCG and uses the supplied information for its system error simulation. The FCG bridges the upper and lower layers of mechatronics and device simulators. The validity of this two-layer approach depends on the accuracy of device error modeling for a large quantity statistics.

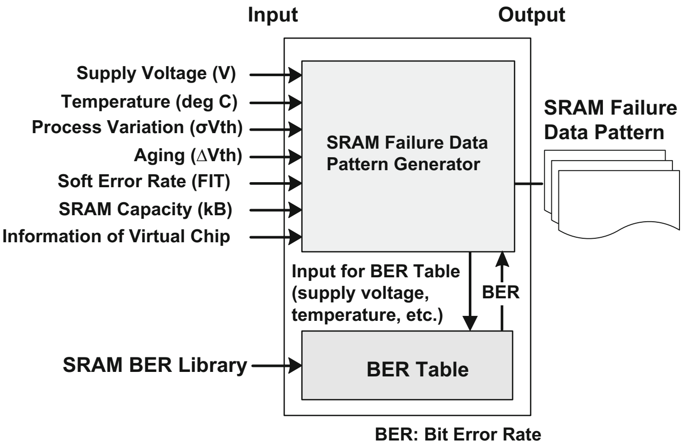


Fig. 15.6 Fault case generator

15.5 Large-Scale Fault Injection Testing with Cloud Computing [13–15]

To make the simulation scenario realistic, we assumed 65-nm fabrication process and determined the SRAM device parameters accordingly with the assumed process. The power supply voltage of the SRAM was set to be 0.4–0.8 V and the operating temperature to be −50 to +150 °C. Assuming a gate length of 60 nm and gate width of 120 nm, the variation of the threshold voltage was calculated to 40 and 30 mV for each of PMOS and NMOS transistors. The negative bias temperature instability (NBTI) of the PMOS transistor was set to be −24 mV assuming aging degradation over 10 years. The soft error rate was set to be 300 FIT in this simulation. These parameters are summarized in Table 15.1.

The control software for the engine control was built fairly simple; the SH-2A® microcontroller ran the OSEK® operating system, an industry standard microkernel code, and such basic input/output (BIOS) functions as analog-to-digital (A/D) converter, timers, and digital inputs and outputs (DIO). By using the OS and the BIOS, the ECU software achieved such engine control functions of airflow metering, fuel injection, ignition timing, and feedback control on the air-to-fuel ratio. The control software was periodically executed every 10 ms. The control code converted to object format was loaded onto the ROM area of the microcontroller model. The SRAM was 128 kB in size and used for OS functions, data storage of control variables, and a scratchpad area needed for the control operation.

Now, we are ready to integrate the SRAM model with the control software loaded on the virtual ECU. Using the multilayer modeling approach mentioned above, we ran a large-scale fault injection analysis on the SRAM device in order to examine the advantage of the dependable SRAM design described in Sect.16.3. Because of the anticipated computational demand, a public cloud computing environment (Amazon EC2®) was used as the computer platform as shown in Fig. 15.7.

In this experiment, 600 pieces of computational nodes were used for running the simulation models, while other several dozen computer nodes supervised the

Table 15.1 SRAM parameter settings for fault simulation

Number of virtual chips	6,000
Supply voltage range	0.4–0.8 V
Temperature range	−50 to +150 °C
Fabrication process	65 nm CMOS
Transistor gate size	Length: 60 nm Width: 120 nm
Standard deviation of threshold voltage	PMOS: 40 mV NMOS: 30 mV
PMOS threshold voltage change due to aging	−24 mV
Soft error rate	300 FIT

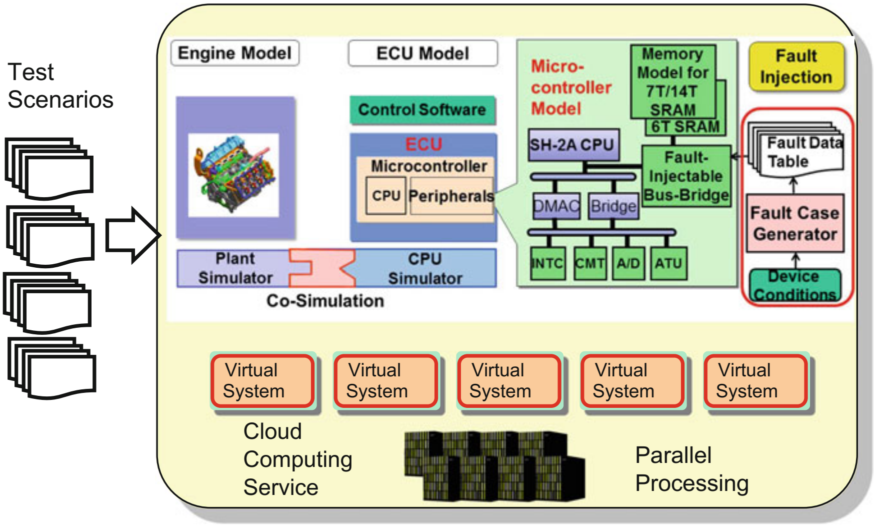
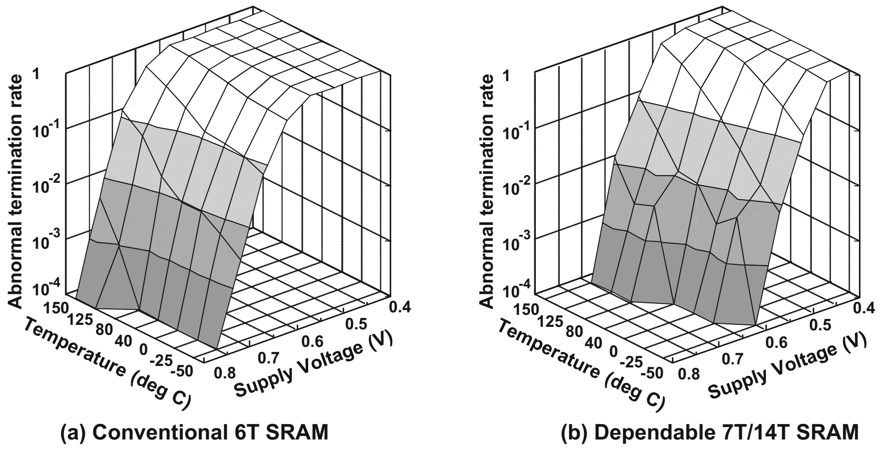


Fig. 15.7 SRAM fault injection test in cloud computing environment

execution of the simulation codes. Note because of the nature of cloud computing, these computational nodes were also virtual; they were Windows® virtual machines to mimic the PC platform. At first, the electromechanical simulation, virtual ECU, and SRAM device simulation were built and verified on actual stand-alone PCs, and then sent to the cloud environment. On the cloud side, there placed was the test case database that contains 672,000 cases of SRAM faults. (The two memory modes of 56 different fault scenarios for 6,000 "virtual" SRAM chips made the total of 672,000 test cases.) The supervisor nodes monitored the progress of each fault case simulation on the 600 computational nodes. Once a fault case was done on a computational node, the supervisor gave the node another fault case and let it begin a new simulation. Here, we adopted the data parallelism to accelerate the entire simulation, and all the computational nodes were kept busy. On the client side, there was a client PC to send parameter settings and simulation request to the cloud service, a license server to manage proprietary licenses of simulation tools, and logging files to receive the simulation results. The whole test cases were carried out overnight in about 12 h. In some cases of SRAM fault injection, the ECU control ended up in engine stalling, and in other cases, the engine was kept running. Figure 15.8 summarizes the result of the fault injection analysis; the occurrence rate of abnormal control termination, i.e., engine stall, was mapped with respect to temperature and supply voltage changes. The 3D graph in Fig. 15.8 compares the dependable SRAM design with the conventional one. The smaller volume of the 3D shape indicates the lower chance of system malfunctioning and proves the superiority of the 7T/14T dependable memory. Note in realistic control systems, there should be a backup means to prevent the engine from stalling. To illustrate the benefit of the dependable memory, no backup system is incorporated here.



(a) Conventional 6T SRAM

(b) Dependable 7T/14T SRAM

Fig. 15.8 Results of fault injection analysis into an engine control system

15.6 Future Directions

Automotive engineers have been improving the test method on ECUs to manage the ever-increasing complexity of the control systems. Failure mode and effect analysis (FMEA) and fault tree analysis (FTA) are the typical methods to verify the reliability of the ECUs and widely adopted. As the automotive control deals with such critical functions as braking and steering, these methods need to be updated. The ISO 26262 functional safety standard suggests an experimental evidence for fault cases and describes a model-based fault injection test as a possible replacement. Though FMEA tries to list up all the conceivable failures in system components, experimental effect analysis is not always easy to carry out. A solder bridge between LSI pins or a wiring short circuit to a ground may be doable fairly easily as fault injections. SRAM errors, however, are very difficult to deal with as a system experiment due to its nature of error mechanism.

Virtual ECU working group (vECU-WG) [16] in Japan, an industrial collaboration among automotive manufacturers, ECU suppliers, semiconductor vendors, simulation tool developers, and information technology companies, have been developing use cases of virtual ECUs. Currently, they are focussing on:

- Modeling multiple ECUs in order to realize an integrated virtual HILS that can simulate an entire vehicle control system connected to a communication network,
- Virtual FMEA [8] to achieve extensive fault injection in all system components and its automated effect analysis, and
- Advanced SILS with microcontroller peripheral models to reflect the microcontrollers' feature designs in system simulation and to ease the load of accurate ISS modeling.

The vECU-WG uses a power window control system as a common use case to share and some of their results have been published (mostly in Japanese). In the case of power window control with a single ECU, the mechanical motion of the window, the motor's up/down rotation, the power MOSFETs circuit current to drive the motor, the control logic signals to turn on/off the MOSFETs, sensor signals to be taken into a microcontroller, and the execution of control software code are all visible together [9].

The goal of the vECU-WG activities is to improve the method for design and test of highly dependable automotive control systems. If future VLSIs will become more vulnerable, the virtual ECU approach should help the automotive engineers to test it in control systems. If VLSI designers want to propose a new idea of device functions or dependable architecture, they may apply the virtual ECU or chip-in-the-loop approach to its concept proving. Then, they can obtain feedbacks on the device features from its potential users prior to mass production. System-on-chip (SoC) design methods have been well established for such electronic systems as cell phones. Automotive and robot systems are far more complex and should require the experiences of VLSI designs for the virtual ECU and chip-in-the-loop simulations.

References

1. IEEE Standard Association, http://standards.ieee.org/findstds/standard/1076.1-1999.html
2. G. Saikalis et al., Virtual embedded mechatronics system. SAE Technical Paper 2006-01-0861, SAE Trans. J. Passeng. Cars Electron. Electr. Syst. **115**(7), 407–413
3. S. Oho et.al., Model-based implementation design of automotive controllers, in *Proceedings of 17th IFAC World Congress (IFAC 2008)* (2008), pp. 1068–1069
4. M. Ishikawa et al., CPU model-based hardware/software co-design for real-time embedded control systems. SAE Technical Paper 2007-01-0776. SAE Int. J. Passeng. Cars Electron. Electr. Syst. **116**(7), 211-218
5. M. Ishikawa et al., CPU model-based hardware/software co-design, co-simulation and analysis technology for real-time embedded control systems, in *13th IEEE Real Time and Embedded Technology and Applications Symposium*, April 2007
6. M. Ishikawa et al., CPU model-based mechatronics/hardware/software co-design technology for real-time embedded control systems, IEICE Trans. Electron **E90-C**(10), 1992–2001
7. Y. Sugure et al., Virtual engine system prototyping with high-resolution FFT for digital knock detection using CPU model-based hardware/software co-simulation. SAE Technical Paper 2009-01-0532. SAE Int. J. Passeng. Cars Electron. Electr. Syst. **1**(2), 177–185
8. Y. Sugure et al., Failure modes and effects analysis using virtual prototyping system with microcontroller model for automotive control system, in *7th IFAC Symposium on Advances in Automotive Control*, Sept 2013
9. S. Shimada et al., Virtual development of automotive control system, in *7th IFAC Symposium on Advances in Automotive Control*, Sept 2013
10. Y. Ito et al. VIRTUAL HILS: a model-based control software validation method.SAE Technical Paper 2011-01-1018. SAE Int. J. Passeng. Cars Electron. Electr. Syst. **4**(1), 142–149
11. ISO 26262 Road Vehicles—Functional Safety (2011)

12. Y. Nakata et al., Model-based fault injection for failure effect analysis—evaluation of dependable SRAM for vehicle control units, in *IEEE International Conference on Dependable Systems and Networks Workshops*, June 2011
13. Y. Nakata et al., Model-based fault injection for large-scale failure effect analysis with 600-node cloud computers, in 1st *RIIF DATE Workshop*, March 2013
14. Y. Takeuchi et al., SRAM failure injection to a vehicle ECU and its behavior evaluation, in *1st RIIF DATE Workshop*, Mar 2013
15. Hitachi News Release, Cloud-based verification simulation technology to analyze the effect of semiconductor memory error on industrial equipment and vehicular control, http://www.hitachi.com/New/cnews/111202.htmlarticl
16. vECU-MBD Working Group, http://www.vecu-mbd.org/en/

Chapter 16
DART—A Concept of In-field Testing for Enhancing System Dependability

Kazumi Hatayama, Seiji Kajihara, Tomokazu Yoneda, Yuta Yamato, Michiko Inoue, Yasuo Sato, Yukiya Miura and Satoshi Ohtake

Abstract LSIs may degrade over time even if they are properly manufactured. The decrease of delay margin caused by the degradation increases the risk of malfunction due to noises or environmental changes as a result, and thus becomes a serious issue for system dependability in field. Therefore, advance detection of failures caused by the degradation of LSIs should be implemented as a key element for preventive maintenance to avoid sudden system down. This chapter gives the essence of the DART (Dependable Architecture with Reliability Testing) technology which enhances the dependability of electronic control systems by detecting in-field aging of LSIs. The DART technology utilizes a sophisticated in-field test capability, especially in-field BIST (Built-In Self-Test), of LSIs, and measures the delay margin of paths all over the chip to alert the occurrence of system down for preventive maintenance. For proofs of the capability of the DART technology, a case study for an industrial circuit, some test chip evaluations, and a FPGA implementation are also given in this chapter. The DART technology itself and its supporting element technologies, including temperature and voltage monitor (T-V monitor), thermal-uniformity-aware test, partitioned rotating test, high-quality delay test, and low power BIST, have been examined by several corporations, some of which have used or are going to use a part of key technologies in practice. The compatibility of DART implementation workflow with a general LSI design flow is also verified by "DART Implementation Guideline".

K. Hatayama (✉)
Gunma University, Kiryu, Japan
e-mail: hatayama@gunma-u.ac.jp

S. Kajihara · Y. Sato
Kyusyu Institute of Technology, Kitakyusyu, Japan

T. Yoneda · Y. Yamato · M. Inoue
Nara Institute of Science and Technology, Ikoma, Japan

Y. Miura
Tokyo Metropolitan University, Hino, Japan

S. Ohtake
Oita University, Dannoharu, Japan

S. Asai (ed.), *VLSI Design and Test for Systems Dependability*,
https://doi.org/10.1007/978-4-431-56594-9_16

Keywords In-field BIST • Delay margin degradation • Advance detection
System dependability • Preventive maintenance

16.1 Introduction

This chapter describes the outline of DART technology [1–3] as a key electronic control technology for enhancing system dependability by preventive maintenance to avoid sudden system down using in-field test of VLSIs. Some related technologies are given in Sects. 5.3, 6.3, 11.3, 11.4, and 12.4.

16.1.1 Background

Advances in semiconductor process technology have brought up various aging-caused degradation issues in field operation of LSIs. There are many aging mechanisms, such as BTI (Bias Temperature Instability), HCI (Hot Carrier Injection), TDDB (Time Dependent Dielectric Breakdown), EM (Electromigration), and SM (Stress Migration) [4–6]. Figure 16.1 is based on an example of real measurement data of operational frequency degradation by NBTI (Negative BTI) [7] which is a shift of transistor characteristics caused by stresses from high temperature and negatively biased voltage. From this figure, it is clear that the delay increase caused by NBTI results in frequency degradation over time. It is, however, noted that the amount of increased delay is hard to estimate accurately since its measurement depends on environmental parameters, such as temperature and voltage, and operating status, such as PMOS active ratio.

In order to avoid system failure caused by degradation, recent designs usually accommodate a certain amount of margin on operational frequency. However, some applications may require very large, say 5–15%, margin since it is determined based

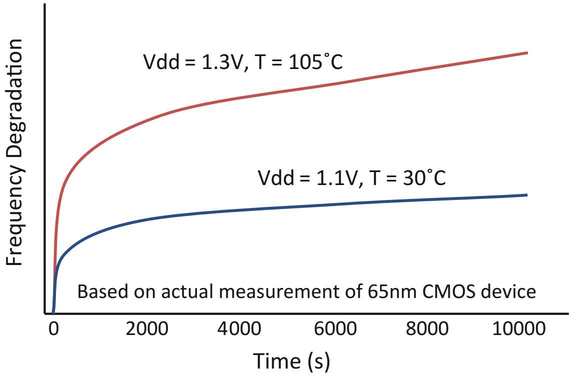


Fig. 16.1 Trend of operational frequency degradation over time by NBTI

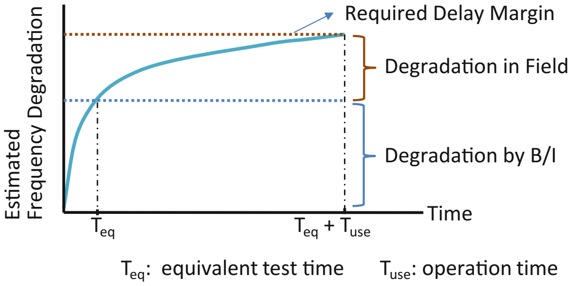


Fig. 16.2 Required delay margin for reliability-aware design

on the worst case condition of process variations, operational environment, expected lifetime, and so on. In such cases, LSI performance will be sacrificed. Figure 16.2 shows an example of frequency degradation caused by NBTI, which requires reliability-aware design with large margins. As shown in Fig. 16.2, the amount of frequency degradation is usually estimated by the evaluation of TEG (Test Element Group) where the amount of degradation by burn-in (B/I) and in field should be also taken into account. So such reliability-aware design may sacrifice a great deal of operational frequency for delay margins.

The utilization of online testing to monitor circuit outputs and internal signals in operation is often used as another solution to avoid system failure. There are several well-known methods, such as, parity checking, and stability checking using dedicated flip-flop, for monitoring soft errors, noises, and other temporary failures. However, the dedicated flip-flop requires large area overhead, that is, its area is more than the triple of ordinary flip-flop, and so, it can be used only for a part of all flip-flops. As a result, it is difficult to guarantee the field reliability of the whole circuit by the utilization of such flip-flops. Moreover, these monitoring methods often cause large repair time, since they only detect faults after some abnormal outputs are observed in operation.

In order to overcome these issues, high level reliability assurance, such as a high-quality test of whole circuit, the detection of aging progression, the prediction of system failure, and so on, should be realized.

16.1.2 Objective

The objective of the field test technology, DART, described in this chapter is the assurance of high level reliability by quick high-quality test for a shipped LSI, or a part of it, in its test mode. As shown in Table 16.1, there are various test constraints, such as operational environment, test data volume, test application time, and so on, in field test, depending on its application. For example, the operation period of network servers is less than 10 years while that of plant control or social

Table 16.1 Application systems and field test constraints

Constraints	Automobile, medical systems	Plant control systems, social infrastructure, etc.	Network server, etc.	Ordinary LSI manufacturing test
Operation period	Long (~20 years)	Very long (~30 years)	Medium (~10 years)	N.A.
Field test timing	Power-on	Periodical test mode in operation	In operation (nonstop)	N.A.
Test resource (memory size, etc.)	Low pin count, small memory size	Constrained (redundant design, etc.)	Constrained (aging data memory, etc.)	A few constraints (on ATE)
Test time	~10 ms	~100 ms (related to frequency)	50–500 ms	Physically few (some on cost)

infrastructure systems is required to be as long as 30 years. This chapter gives elemental technologies corresponding to these constraints and also an integrated self-test technology to implement field testability function to application systems for realizing highly dependable systems using these elementary technologies.

16.2 Outline of DART Technology

16.2.1 What's DART Technology

As an approach for field testability, we are developing a circuit and system architecture, called DART, for advance degradation detection and fault detection utilizing self-test and self-diagnosis of LSIs at system unoccupied time, such as power-on, power-off, and idle time or dedicated maintenance time. For the DART technology, the following four targets are considered not only for elemental technology development but also for feasibility study and system integration.

D (Degrade factor)	advance detection of degradation in SoC/NoC/FPGA
A (Accuracy)	high accuracy detection
R (Report)	report of degradation information in field
T (Test coverage)	realization of high test coverage.

The basic concept of the DART technology is shown in Fig. 16.3. The DART technology calculates the amount of degradation of a chip by comparing measured delay with the initial value before shipment and issues an alarm to the system before the longest path delay of the chip exceeds allowable delay limit for prompting a preventive maintenance action to avoid sudden system down. Thus, we can reduce not only the failure rate of the system but also its repair time.

Figure 16.4 shows the conceptual diagram of the DART technology application. The DART technology requires a DART test controller for field test operation. The

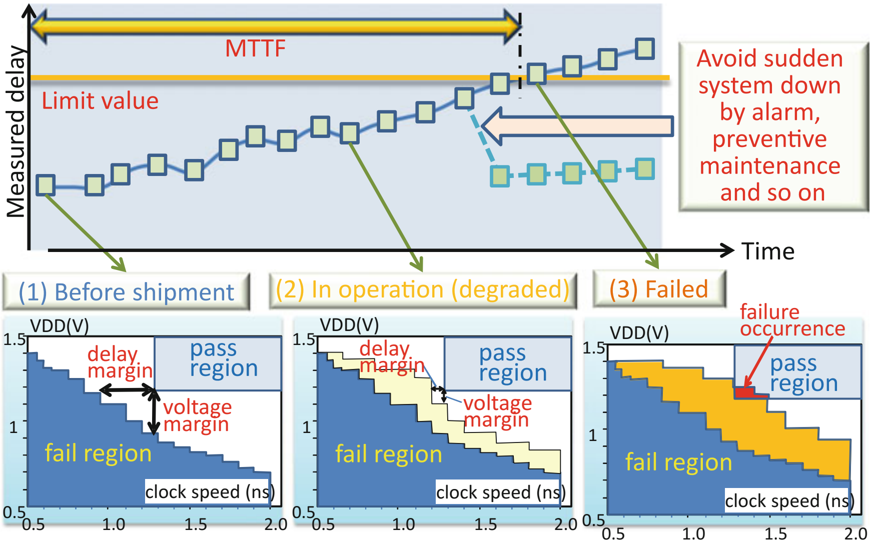


Fig. 16.3 Basic concept of DART technology

test controller for DART communicates with manufacturing test controllers, such as logic BIST (Built-In Self-Test) controller and memory BIST controller, to realize field test of each IP core on the chip. Test patterns for field test are stored in ROMs or nonvolatile memories. The logs of field test results are also stored in nonvolatile memories. The DART test controller and these memories can be located on-chip or

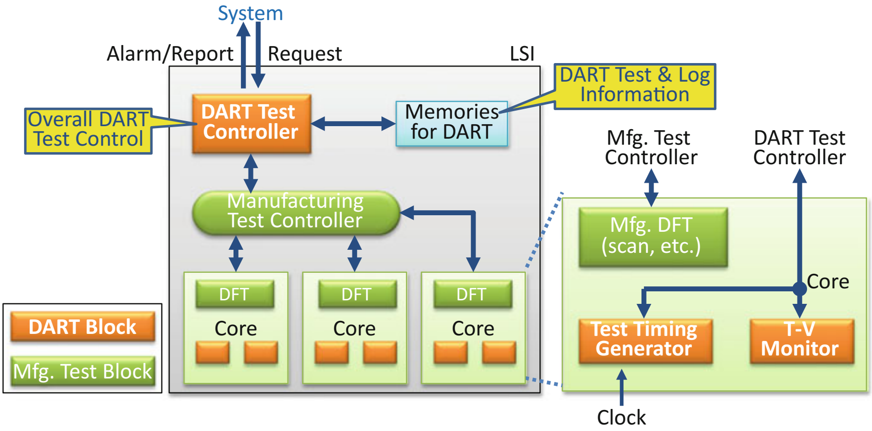


Fig. 16.4 Conceptual diagram of DART technology application

Table 16.2 Range of detectable failures by DART

Cause of failure	Appearance	System multiplication[a, b]	Online test (monitor, etc.)[b]	In-field BIST[b]	DART
Stuck fault	Sudden stuck (random)	Very high	Low–medium (inexhaustive)	Very high	Very high
EM/SM					
HCI/NBTI/PBTI	Gradual delay increase (systematic)	Low–medium (CCF)	Low–medium (inexhaustive)	Very high (posteriori)	Very high (in advance[c])
TDDB	Delay increase → gate open (random)	Very high	Low–medium (inexhaustive)	Very high (posteriori)	Very high (posteriori) Medium–high (in advance[c])
Noise	Marginal (temporary)	Very high	Low–medium (inexhaustive)	Low	Medium–high (in advance[c])
Soft error	Temporary (nonrecurring)	Very high	Low–medium (inexhaustive)	Low	Low

[a] Hard to detect common cause failures (CCFs)
[b] Only posteriori detection
[c] DART only feature

off-chip. Though the test operation for each core is controlled by a certain core test controller, the DART test controller specifies the test timing based on the information obtained from temperature and voltage (T-V) monitor for accurate detection of the degradation of circuits in the core.

The DART technology has a good possibility to enhance functional safety of a system. Table 16.2 shows the range of detectable failures by DART and other existing approaches [8–20]. It is noted that system multiplication approaches, such as duplication, majority voting, and so on, can provide very high detectability for most failures, but they are hard to detect common cause failures (CCFs) brought by aging. It is also noted that existing approaches can provide only posteriori detection, that is, they cannot detect failures caused by degradation in advance of real failures, while DART has a capability of advance detection of degradation appearing as delay increase.

Figure 16.5 shows an example of product development flow to implement the DART technology to a system. Following this flow, system dependability can be enhanced by implementing the DART technology on LSIs in system design and LSI design phases and utilizing the implemented DART technology for field test phase.

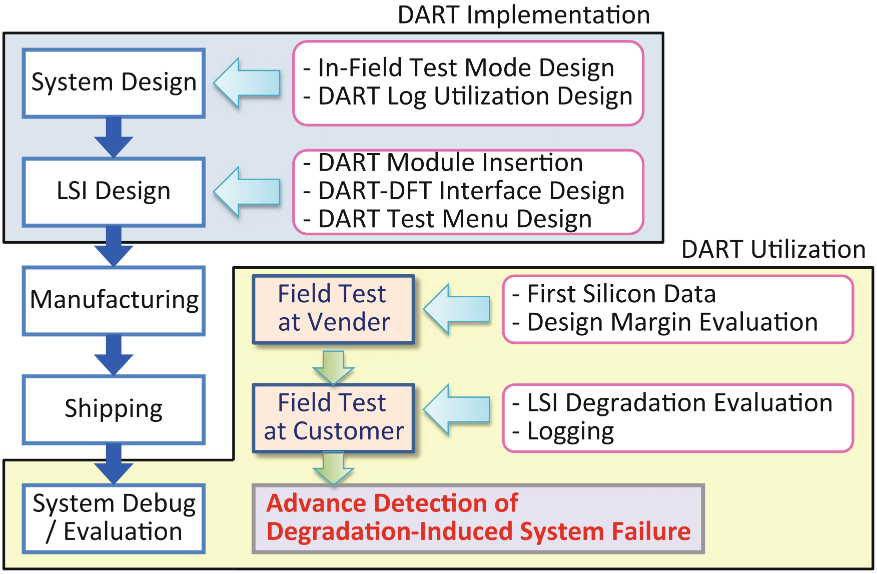

DART Implementation
System Design
- In-Field Test Mode Design
- DART Log Utilization Design
LSI Design
- DART Module Insertion
- DART-DFT Interface Design
- DART Test Menu Design
Manufacturing
Shipping
System Debug / Evaluation
DART Utilization
Field Test at Vender
- First Silicon Data
- Design Margin Evaluation
Field Test at Customer
- LSI Degradation Evaluation
- Logging
Advance Detection of Degradation-Induced System Failure

Fig. 16.5 Product development flow with DART implementation

16.2.2 *Specifications of DART Technology*

Based on the DART technology given in the previous section, we define four issues for establishing the DART technology and breakdown the issues to target specifications as shown in Table 16.3.

The first issue is accurate delay measurement, which requires to measure circuit delay accurately in field. The DART technology utilizes self-test and self-diagnosis to measure path delays in the circuit and predicts or detects the occurrence of fault due to aging. It realizes delay measurement in an accuracy one or two order finer than system clock cycle, then judges the level of degradation from the increase of measured delays, and predicts the occurrence of system failure due to aging in advance.

The second issue is test constraints consideration, which requires the satisfaction of dedicated constraints on test time, test data volume, and so on, for each application system. Though the target values shown in Table 16.3 are very severe comparing with those for manufacturing test, the DART technology can reduce the impact of its implementation on the system by establishing these targets.

The third issue is efficient implementation, which requires realization of in-field test functionality. Obviously, the implementation of the DART technology becomes more attractive by establishing these targets.

The fourth issue is practical application of the DART technology, which requires a guideline for DART implementation, called *DART Implementation Guideline*, to promote evaluation and implementation of the DART technology in wide range of

Table 16.3 Issues and target specifications

No.	Issue	Target specification	Remarks
1	Accurate delay measurement	Delay measurement error ≤ 50 ps (for 300–500 MHz circuits)	Digital measurement of temperature and voltage variation
		Temperature variation ≤ 5 °C	To reduce error due to temperature variation
2	Test constraints consideration	Fault coverage ≥ 95%	To ensure test quality
		Test data volume ≤ 1/3000	To embed in on-chip memory
		Test time per chance: 10–200 ms	To avoid impact on system performance
3	Efficient implementation	Logic BIST based implementation	To reduce area overhead by utilizing existing test circuits and to reduce test data volume and power
		Asynchronous circuit support	To apply to NoC
		Test record utilization	To enhance degradation detectability and diagnosis efficiency
4	Practical application	Guideline for DART implementation	To promote wide evaluation and implementation
		Feasibility study for effectiveness validation	To validate practical applicability on performance, accuracy, field data acquisition and performance/environment monitoring in operation, by real chip, TEG or simulation
		Standardization for functional safety	To propose to add DART technology to conditions for IEC61508 [21] SIL

potential application systems. Figure 16.6 shows the image of DART implementation workflow. *DART Implementation Guideline*, defining DART implementation works at each LSI design phase, can make it easy to implement the DART technology on LSIs. Moreover, the effectiveness of the DART technology on system dependability can be illustrated by validating the capability of efficient data acquisition and analysis of internal circuit delays by field test of DART implemented LSIs.

16.2.3 Key Enablers of DART Technology

Several technologies for advance detection of degradation and failure detection utilizing in-field LSI self-test are developed as elemental DART technologies. Four key items shown in Table 16.3 are broken down into target requirements and elemental technologies covering these target requirements as shown in Fig. 16.7 are developed.cir

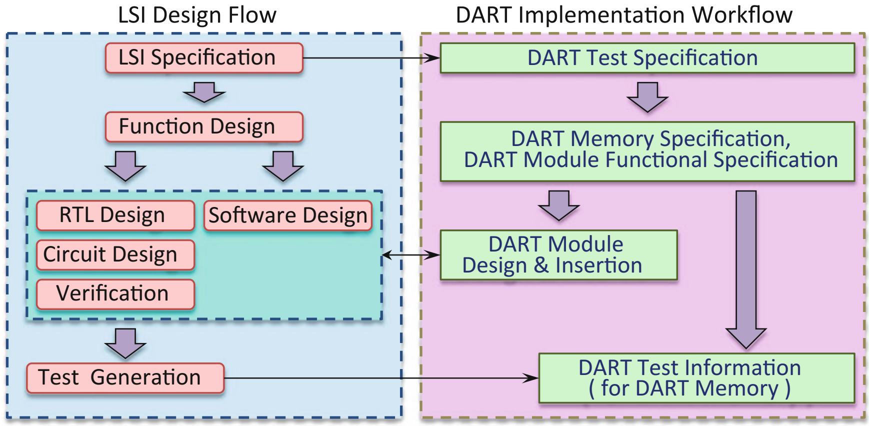


Fig. 16.6 DART implementation workflow

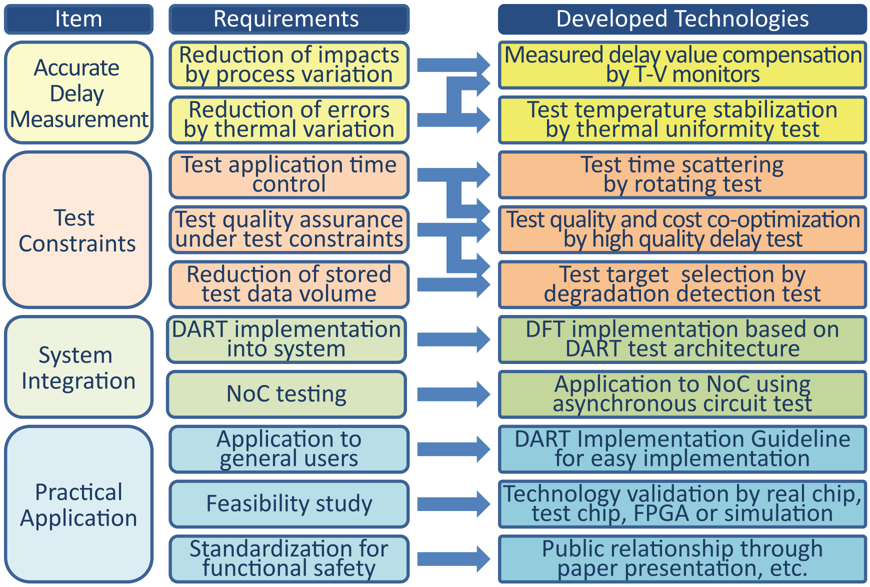

Item
Requirements
Developed Technologies
Accurate Delay Measurement
Reduction of impacts by process variation
Reduction of errors by thermal variation
Measured delay value compensation by T-V monitors
Test temperature stabilization by thermal uniformity test
Test Constraints
Test application time control
Test quality assurance under test constraints
Reduction of stored test data volume
Test time scattering by rotating test
Test quality and cost co-optimization by high quality delay test
Test target selection by degradation detection test
System Integration
DART implementation into system
NoC testing
DFT implementation based on DART test architecture
Application to NoC using asynchronous circuit test
Practical Application
Application to general users
Feasibility study
Standardization for functional safety
DART Implementation Guideline for easy implementation
Technology validation by real chip, test chip, FPGA or simulation
Public relationship through paper presentation, etc.

Fig. 16.7 Elemental technologies for DART

For accurate delay measurement, a statistical approach is used to reduce quantization error. In the DART technology, a circuit delay is measured by LSI self-test in field, however, the circuit delay depends not only on degradation by aging but also on environmental conditions such as circuit voltage, temperature variation, and so on. Therefore, we are developing technologies for delay value compensation using circuit monitoring using T-V monitors [22] and test temperature stabilization by thermal-uniformity-aware test [23, 24].

For satisfying test constraints on test application time, test data volume, and so on, which may differ from application to application, we are developing three techniques, that is, rotating test, high-quality delay test set generation, and degradation detection test. The rotating test technique scatters test set for whole chip in multiple test chances to reduce test application time and test data volume for each test chance [25]. The high-quality delay test set generation technique co-optimizes delay test quality and test cost under the test constraints [26–31]. The degradation detection test technique narrows down the test target considering aging mechanism and optimizing test for the aging mechanism to reduce test application time and test data volume [32]. Furthermore, we are working for improving BIST technologies for manufacturing test to reduce test data volume or power consumption during test [33–35].

For system integration, DART realizes test architecture for in-field test utilizing existing DFT frameworks, such as scan, logic BIST, and so on, for manufacturing test and in cooperation with proposing monitor circuits, test logging function, and so on [36]. The reuse of manufacturing DFT frameworks makes it possible to achieve high test quality in low hardware overhead.

For practical application, we are reviewing the developed technologies from the viewpoints of generalization and standardization, and provide a guideline for realizing them as DART modules. Furthermore, as a feasibility study, we are going to show the DART technology can be practically applicable by implementing the DART technology in real systems in cooperation with some companies and illustrating the target delay measurement accuracy can be achieved in realistic hardware overhead, test application time, and test data volume. For the developed technologies which are not embedded in the real system, we will validate them by test chip or by simulation. Moreover, we are going to work for the acceptance of the DART technology as a requirement for international standard of functional safety, IEC61508 [21], to show its advantage and effectiveness in a form which is easily recognized by users.

16.2.4 Advantages of DART Technology

The DART technology and its ideas have advantages on applicability, superiority, and originality as shown below.

The DART technology can realize field test utilizing scan design, logic BIST, and so on which are implemented for manufacturing test. Moreover, the DART technology can be used both for field online test during system operation and for off-line test during system development and system debug on system halt. At online test, it can contribute to enhance system dependability in field by detection of delay increase through periodical delay measurement. On the other hand, at off-line test, it can not only detect low reliability chip in advance by measuring delay margin and initial degradation amount of the chip, but also contribute to efficient system debug in field by reporting on-chip delay information. Furthermore, the DART technology can provide techniques for optimizing test quality under severe constraints of test application time and test data volume and test and DFT techniques for asynchronous circuits. These technologies are also used in manufacturing test, and so they can contribute to enhance the quality of LSI chips including synchronous circuits, asynchronous circuits and GALS (Globally Asynchronous Locally Synchronous) systems.

As shown in Table 16.4, the DART technology has a possibility to be used for many purposes both online and off-line.

The adoption of the DART technology may largely depend rather on cost acceptability than on technical applicability considering the target usages. The DART technology is mostly suitable for plant control systems and social infrastructure systems among the application systems shown in Table 16.1, where redundancy is required for assuring long-term reliability. Moreover, it is suitable for network devices and servers where performance binning is necessary. On the other hand, for automotive LSIs and consumer LSIs, which have severe cost constraints on LSI pins and silicon areas, it is difficult to use the DART technology in current products, but we think it will be a necessary technology for next generation and beyond.

The DART technology has the following advantages comparing with similar researches.

- It can be applied to various types of LSIs including SoCs, NoCs and multicores.
- It can be also applied to FPGA-based systems.
- It can utilize the same DFT framework as used for manufacturing test, and so its impact to system can be minimized and it can even contribute to the efficiency of manufacturing test and system debug.

Table 16.4 Target usages of DART technology

Target usage	Purpose	Functionality
Field test (online use)	Advance detection of system failure due to aging	Log data analysis for checking delay margin transition
	Diagnosis report on erroneous behavior	Report on tested paths and their delay margin
System debug (off-line use)	Monitoring of design margin and level of degradation	Acquisition of data on time passage, environmental effects, ordinary aging, accelerated aging, etc.
	System diagnosis report	Report on delay information for failure analysis
Manufacturing test (off-line use)	Chip quality improvement	Maximization of delay test quality under test constraints Testability enhancement for asynchronous circuits

The DART technology has high novelty on the following points.

- Highly accurate measurement of delay margin of logic circuits by;
  - compensation functionality of measured delay value by monitoring the temperature and voltage during the delay measurement
  - aging-tolerant ring oscillators using standard cell library
  - simultaneous control of test power and temperature.
- Flexibly adaptation to test constraints on test application time and test data volume by;
  - utilization of multiple test chances in field
  - effective test target selection.
- Recording functionality of measurement logs and the capability of its application to system diagnosis.

16.3 Outlines of DART Elemental Technologies

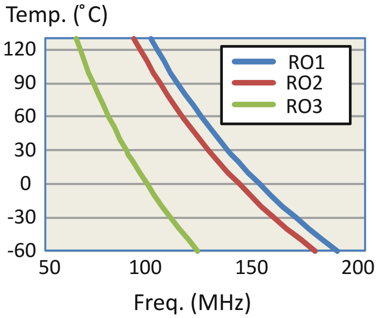
This section describes the outlines of some of DART elemental technologies, that is, temperature and voltage monitor (T-V monitor), thermal-uniformity-aware test, partitioned rotating test, high-quality delay test and low power BIST.

16.3.1 T-V Monitor

The DART technology uses temperature and voltage monitor to compensate environmental impact on circuit delay for accurate measurement. As shown in Fig. 16.8, temperature and voltage during test is estimated from the difference between initial and current count values of three ring oscillators (ROs), and then measured maximum frequency is compensated by the estimated temperature and voltage. It is noted that we can use aging-tolerant ROs [22] to avoid incorrect estimation.

16.3.2 Thermal-Uniformity-Aware Test

The DART technology provides thermal-uniformity-aware test method to reduce temperature variation in time and space during in-field testing. A dedicated X-filling method is used for spatial uniformity and a dedicated pattern ordering method is



$$\begin{bmatrix} Te \\ Ve \end{bmatrix} = \begin{bmatrix} a_1 & b_1 \\ a_2 & b_2 \end{bmatrix}^{-1} \begin{bmatrix} k_1\,F_{d1} - k_2\,F_{d3} \\ k_3\,F_{d2} - k_4\,F_{d3} \end{bmatrix} + \begin{bmatrix} c_1 \\ c_2 \end{bmatrix}$$

$$F_d(T,V) \equiv F(T,V) - F(T_0,V_0)$$

Fig. 16.8 High precision delay measurement by T-V monitor

used for temporal uniformity [24]. The techniques realize small thermal variation during test, which will result in small delay variation. See Sect. 11.4 for details.

16.3.3 Partitioned Rotating Test

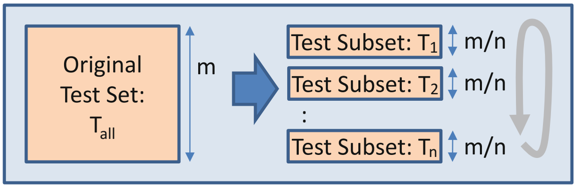
The DART technology uses partitioned rotating test, which divides the whole test set into several test subset and uses each test subset in a test chance by rotation as shown in Fig. 16.9, to satisfy test time constraint [25]. Adaptive change of test subsets can also be used to enhance degradation detection capability [36].

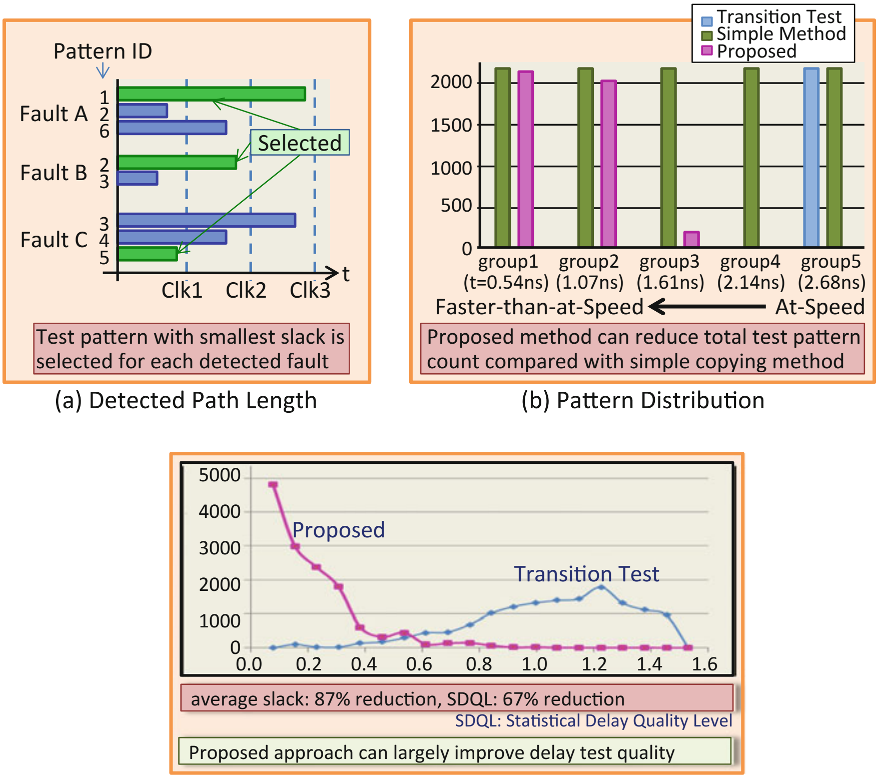
16.3.4 High-Quality Delay Test

Many delay test generation approaches are developed in the DART technology to improve test quality for small delay defects. Figure 16.10 shows one of the approaches, which utilizes faster-than-at-speed test and achieves better SDQL (Statistical Delay Quality Level) in less test patterns [29].

Moreover, we propose a high speed per cell IR-drop analysis method [30]. This enables an at-speed test taking account of the impact of IR-drop caused by power consumption during test, and contributes to high delay test quality. See Sect. 11.3 for details.

Fig. 16.9 Concept of partitioned rotating test





(a) Detected Path Length

(b) Pattern Distribution

(c) Slack Distribution

Fig. 16.10 High-quality delay test using faster-than-at-speed test

16.3.5 *Low Power BIST*

To avoid the change of path delay or propagated values caused by excessive heating and power noise, the DART technology can provide a low power BIST method for test power reduction or control. Test power can be classified into three elements, test pattern input (scan-in), test (capture), and test pattern output (scan-out) powers, each of which has different behavior. The proposed low power BIST method is a holistic approach to solve all types of test power issues. Our low power BIST can be implemented by adding power reduction circuits for each test power as shown in Fig. 16.11. Figure 16.12 shows results comparing with some existing approaches. These results show that our low power BIST is effective not only for test power reduction but also for test quality improvement [34, 35].

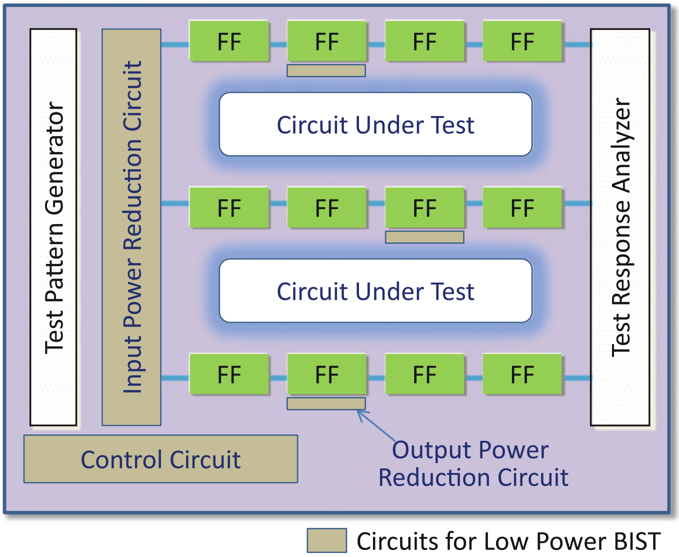

Test Pattern Generator
Input Power Reduction Circuit
FF
Circuit Under Test
Test Response Analyzer
Control Circuit
Output Power Reduction Circuit
Circuits for Low Power BIST

Fig. 16.11 Low power BIST architecture

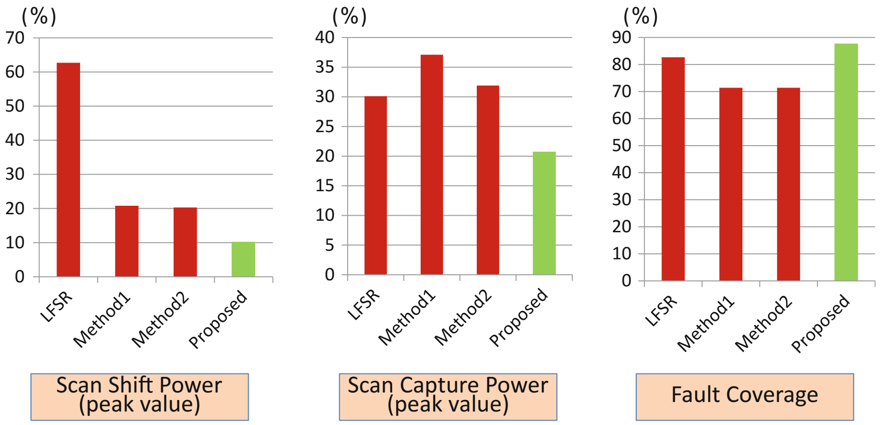


Fig. 16.12 Low power BIST results

16.4 Implementation of DART Technology

16.4.1 Case Study on Industrial Circuit

A case study of the DART technology on industrial circuit is given in this section [3]. Target circuit has 7.2M gates, 356k flip-flops, and 12 clock domains. It also has 264 memory blocks, including SRAMs and register files. Its DFT circuits for manufacturing test include not only scan circuits but also TPG (Test Pattern Generator) and TRA (Test Response Analyzer) for logic BIST, circuits for memory BIST, and TAPC (Test Access Port Controller) for boundary scan.

Figure 16.13 shows the design structure of the circuit with DART functionality. It embedded a test controller for DART, a test timing generator for delay measurement, an on-chip DART memory for storing DART test information and test logs, and temperature and voltage monitors (TVMs) [22] for the compensation of temperature and voltage impact on path delays. The DFT circuits, that is logic BIST circuits and memory BIST circuits, for manufacturing test are controlled through TAPC.

The results of this case study are as follows.

As shown in Table 16.5, the gate overhead for DART circuits is about 14k gates in total, which is less than 0.2% of whole circuit. It is noted that the on-chip DART memory is not included in the gate overhead since it can be used in common with work memory for ordinary function.

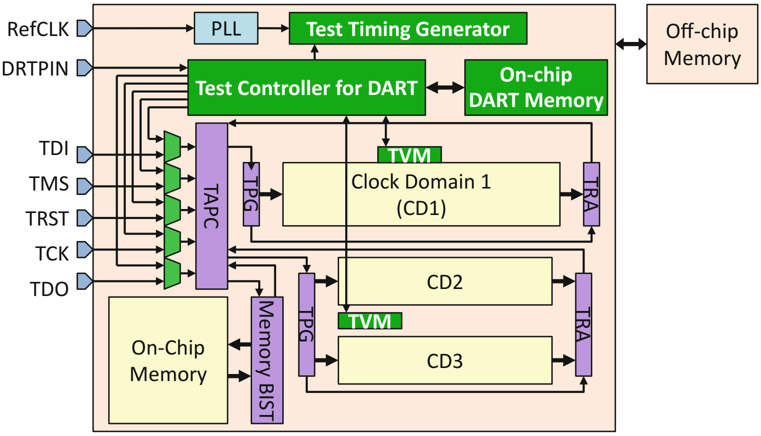


Fig. 16.13 Design structure with DART circuits

Table 16.5 Gate overhead of DART circuits

Item	# Cells	# Gates		
		Comb. circ.	Others	Total
For LBIST	1.1k	2.0k	0.2k	2.2k
For MBIST	1.1k	1.6k	0.2k	1.8k
Overall control	0.5k	0.2k	2.6k	2.8k
TVM	2.5k	6.8k	0.4k	7.2k
Total overhead	5.2k	10.5k	4.4k	13.9k

Table 16.6 Accuracy of temperature and voltage estimation by TVMs

				Temperature interval		
				−40 to 20 °C	20 to 80 °C	80 to 110 °C
Estimated temp.	Voltage interval	1.0–1.1 V	Error (min, max)	−2.6 to 2.4 °C	−2.6 to 2.4 °C	−1.3 to 2.0 °C
			Std. div.	1.2 °C	1.1 °C	0.8 °C
		1.1–1.2 V	Error (min, max)	−3.3 to 3.0 °C	−2.7 to 2.6 °C	−2.1 to 2.3 °C
			Std. div.	1.4 °C	1.3 °C	1.1 °C
		1.2–1.3 V	Error (min, max)	−2.8 to 1.9 °C	−1.8 to 1.9 °C	−1.3 to 1.9 °C
			Std. div.	1.2 °C	0.9 °C	0.7 °C
Estimated voltage			Error (min, max)	−13 to 8 mV	−15 to 8 mV	−8 to 5 mV
			Std. div.	5 mV	5 mV	3 mV

Table 16.6 shows the results on the accuracy of temperature and voltage estimation by TVMs. A two-stage estimation, that is interval estimation followed by precise estimation, is used to obtain the results of 0.7–1.4 °C standard deviation in temperature and 3–5 mV standard deviation in voltage.

In the experiments on the adjustability to test constraints (test data volume and test time) in field, not only all the 12 intra-domain circuits but also 52 inter-domain circuits are targeted for logic BIST. Two test constraints are considered, that is, 8 kB for test data volume and 200 ms for test time. The logic BIST for DART utilizes reseeding technique by multiple seed patterns for TPG to improve test quality. It is noted that the use of many seeds can improve test quality but it will increase test data volume. Table 16.7 shows the test data volume to test all target circuits at one test chance ($N_{TC} = 1$). Several cases of the number of seed for each intra-domain circuit and for each inter-domain circuit are evaluated, but even for the minimum case, that is, 1 seed for each intra-domain and 1 seed for each inter-domain, the test data volume exceeds the test constraint. On the other hand, for the cases where the whole test set are divided into 8 subsets and apply one subset at each test chance by rotating test [25] ($N_{TC} = 8$), more seed can be used within the test constraint as shown in Table 16.8. In general, intra-domains are larger than inter-domains, and so if the number of seeds for each intra-domain is maximized, 22 seeds can be used for each intra-domain. Test time for each case is evaluated similarly, and the results for $N_{TC} = 1$ and $N_{TC} = 8$ are shown in Tables 16.9 and 16.10, respectively. Detailed conditions are not shown here but the results illustrate the effectiveness of rotating test for keeping test constraints.

Other experiments are executed for showing the effect of test quality improvement by reseeding. Three clock domains (T0, T2, and T7) are used for intra-domain test and a seed selection method [28] is applied. Figure 16.14 shows the fault

Table 16.7 Estimated test data volume ($N_{TC} = 1$)

# Seeds		Test data volume (kB)
Intra-domain	Inter-domain	
1	1	10
2	1	11
2	2	17
3	1	12

Table 16.8 Estimated test data volume ($N_{TC} = 8$)

# Seeds		Test data volume (kB)
Intra-domain	Inter-domain	
1	1	4.8
2	2	5.6
5	5	8.0
22	1	7.9

Table 16.9 Estimated test time ($N_{TC} = 1$)

# Seeds		Test time (ms)
Intra-domain	Inter-domain	
1	1	229
2	1	271
2	2	459
3	1	313

Table 16.10 Estimated test time ($N_{TC} = 8$)

# Seeds		Test time (ms)
Intra-domain	Inter-domain	
1	1	29
2	2	57
5	5	143
22	1	174

coverage curves for each clock domain by random BIST (1 seed) and BIST reseeding (multiple seeds) with seed selection. It can be seen that BIST reseeding can achieve higher fault coverage than random BIST in less test patterns for all cases. Though these experiments do not consider the test constraints above, the results imply that appropriate selection of seeds and appropriate division of whole test set considering circuit structure may lead to enough test quality within given test constraints.

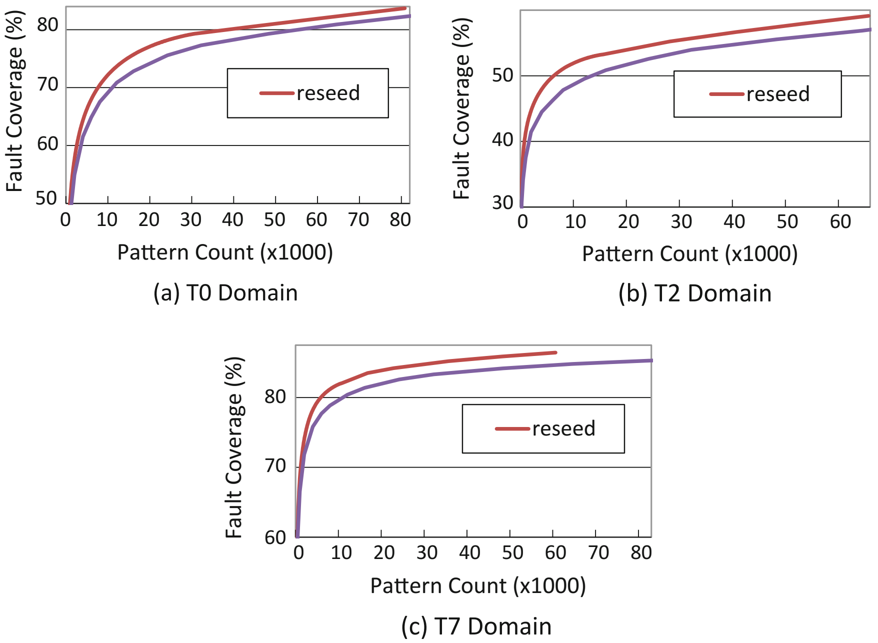


Fig. 16.14 Fault coverage improvement by seed selection

16.4.2 DART as Dependable FPGA Solution

The critical issue to apply DART technology to FPGA is the accurate delay measurement since it is not straightforward to assure accurate timing on FPGA efficiently. Therefore, three key components, that is the variable test timing generator for on-chip delay measurement, the T-V monitor for environmental impact compensation of circuit delay and the test pattern generator and test response analyzer for logic BIST, have been tuned for FPGAs.

A phase shift functionality of PLLs on FPGA is utilized for variable test timing generation [37] as shown in Fig. 16.15. An experimental result on FPGA, where normal test timing is set to 10 ns, shows 1–10 times phase shift, which means up to 960 ps delay shift can be realized by this approach. This result illustrates the possibility of the approach though we need further investigation to expand the delay shift size.

As for the implementation of T-V monitor on FPGA, a ring oscillator having special structure with specific input port assignment, as shown in Fig. 16.16, is developed to reduce NBTI-induced degradation [38]. Experimental result by

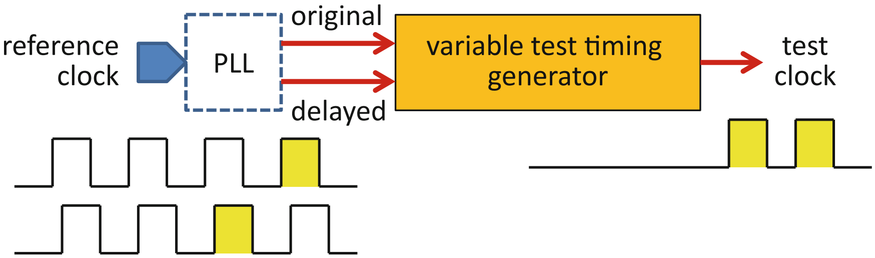


Fig. 16.15 Variable test timing generation on FPGA

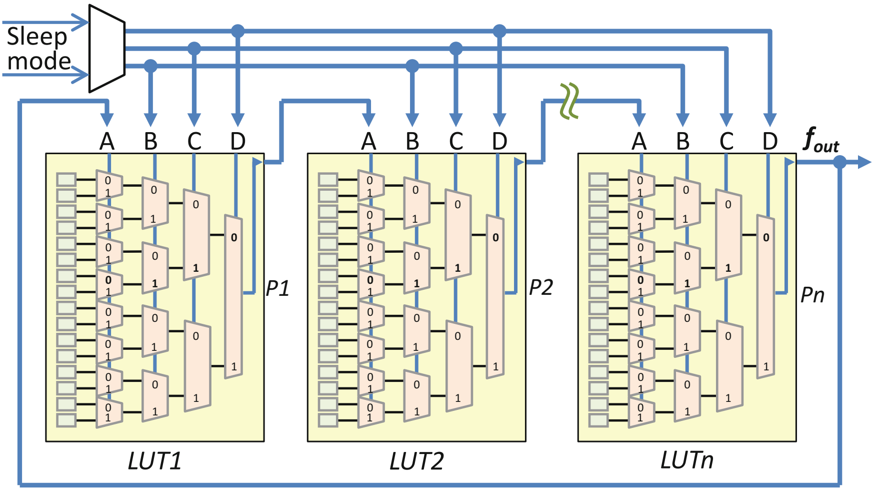


Fig. 16.16 Structure of ring oscillator for T-V monitor on FPGA

configuring several kinds of ring oscillator shows the developed one causes the lowest degradation. This result illustrates the merit of the DART technology as a dependable FPGA solution.

Dedicated test circuits for logic BIST, that is test pattern generator based on LFSR (Linear-Feedback Shift Register) and test response analyzer based on MISR (Multi-Input Signature Register), can be implemented on FPGA as general logic circuits but it may require large overhead since FPGAs are not scan-ready devices (no scan cell and no scan chain). To overcome this issue, an area-efficient architecture for LFSR/MISR using shift register configurations of memory blocks is used [39, 40]. It can flexibly assign BIST logics on memory block area or logic element area depending on the type of application circuit as shown in Fig. 16.17.

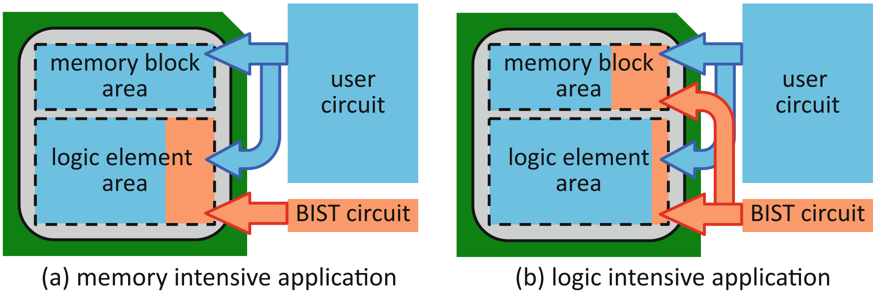


Fig. 16.17 Flexible assignment of BIST circuit

16.4.3 DART Implementation Guideline

To ease the implementation of the DART technology on LSI, we develop *DART Implementation Guideline* (DART Guideline, in short) based on the results of the above developed technologies. The DART Guideline defines DART modules, which are key components to realize DART. Each DART modules can be realized as a software module or a hardware module. Figure 16.18 illustrates the relation between DART modules and related modules shown in the DART Guideline.

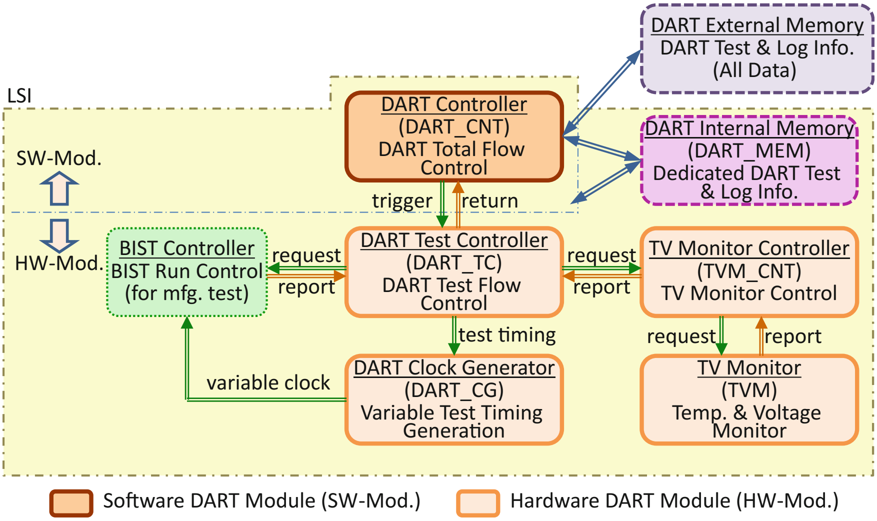


Fig. 16.18 DART modules and related modules

DART Controller (DART_CNT), which is provided as a software DART module, controls overall DART operation in field. DART_CNT accesses an external nonvolatile memory (called DART External Memory), which stores all information of DART test and a record of test log data, and an embedded work memory (called DART Internal Memory (DART_MEM)), which stores specific test execution information and the test result log data. Moreover, DART_CNT determines specific test contents and calculates estimated/corrected value of temperature, voltage, and circuit delay. Furthermore, DART_CNT triggers DART Test Controller (DART_TC) to start a DART test execution.

DART_TC, which is provided as a hardware DART module, controls all other hardware DART modules to execute a DART test. On the trigger from DART_CNT, DART_TC executes a DART test defined by the specific test execution information stored in DART_MEM by booting up a BIST (LBIST (logic BIST) or MBIST (memory BIST)) Controller for manufacturing test corresponding to a specified circuit under test (CUT). In case of LBIST, DART_TC updates test timing generated by DART Clock Generator (DART_CG) to measure the maximum operating frequency of the CUT. Both for LBIST and MBIST, DART_TC also boots up TV Monitor Controller (TVM_CNT) to execute measurement by TV Monitor (TVM) to estimate temperature and voltage during the test. At the end of test, DART_TC writes the test result log date in DART_MEM to pass the information to DART_CNT.

Some of the DART functionalities have already validated by the implementation on FPGA.

16.5 Other Activities

16.5.1 Activities for Standardization

There is a well-known international standard for functional safety, IEC61508 [21], related to system dependability in field. It defines “safety integrity level (SIL)” as a metric to express safety of electrical, electronic, or programmable electronic systems. There are four levels of SILs (SIL1-SIL4) and SIL4 is the highest level. IEC61508 Part2, Annex E gives a standard on on-chip redundancy, where the level of SIL3 is defined as follows.

β_{IC}: estimated susceptibility of IC with on-chip redundancy to common cause failures (CCFs)
initial value of $\beta_{IC} = 33\%$
→ increase based on Table E.1 and decrease based on Table E.2 [21]
→ if final $\beta_{IC} < 25\%$, then SIL3

An example of increasing factor is a monitoring by on-chip watchdog (5%), and an example of decreasing factor is a structure with isolating and decoupling physical locations (2–4%). The DART technology can provide functionalities for

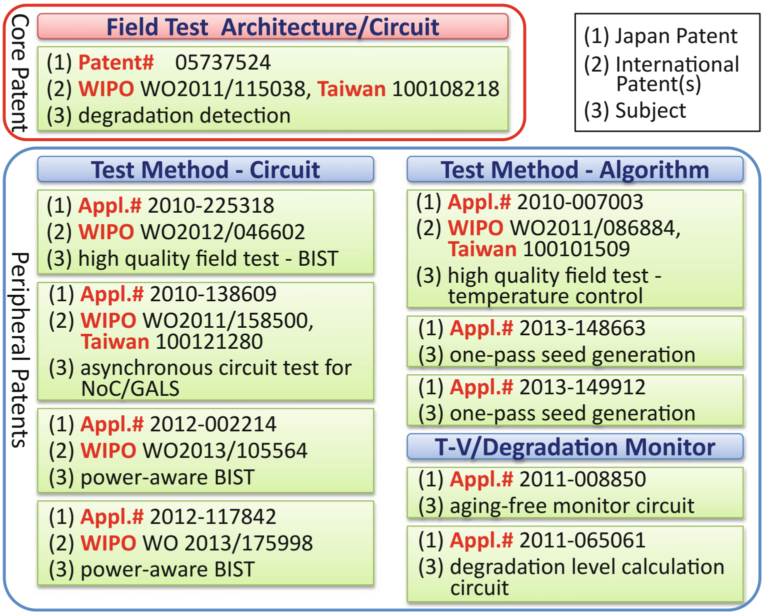

Core Patent
Field Test Architecture/Circuit
(1) Patent# 05737524
(2) WIPO WO2011/115038, Taiwan 100108218
(3) degradation detection
(1) Japan Patent
(2) International Patent(s)
(3) Subject
Peripheral Patents
Test Method - Circuit
(1) Appl.# 2010-225318
(2) WIPO WO2012/046602
(3) high quality field test - BIST
(1) Appl.# 2010-138609
(2) WIPO WO2011/158500, Taiwan 100121280
(3) asynchronous circuit test for NoC/GALS
(1) Appl.# 2012-002214
(2) WIPO WO2013/105564
(3) power-aware BIST
(1) Appl.# 2012-117842
(2) WIPO WO 2013/175998
(3) power-aware BIST
Test Method - Algorithm
(1) Appl.# 2010-007003
(2) WIPO WO2011/086884, Taiwan 100101509
(3) high quality field test - temperature control
(1) Appl.# 2013-148663
(3) one-pass seed generation
(1) Appl.# 2013-149912
(3) one-pass seed generation
T-V/Degradation Monitor
(1) Appl.# 2011-008850
(3) aging-free monitor circuit
(1) Appl.# 2011-065061
(3) degradation level calculation circuit

Fig. 16.19 DART patent map (as of June 5, 2016)

detection of delay increase and prediction of degradation, and so it has good potential to strengthen the countermeasures of CCFs and hence decrease β_{IC}. We will work for addition of these techniques to Table E.2 [21] and also we will target the inclusion of them in the requirement of SIL4.

16.5.2 Intellectual Property

We can actively license our patents shown in Fig. 16.19 to promote the practical application of the DART technology. Please contact crest(at)aries30.cse.kyutech.ac.jp for further information.

16.6 Conclusion

As shown in this chapter, we have developed an LSI test technology for supporting high system dependability in field. We also have performed some feasibility studies of the developed technologies, but we know the best way to validate the effectiveness of DART is collaborations to corporations who really apply it in practice. We appreciate your cooperation.

References

1. Y. Sato et al., A circuit failure prediction mechanism (DART) for high field reliability, in *Proceedings of the International Conference on ASIC (ASICON'09)* (2009), pp. 581–584
2. Y. Sato et al., Circuit failure prediction by field test (DART) with delay-shift measurement mechanism, in *Proceedings of Integrated Circuits and Devices in Vietnam (ICDV'10)* (2010)
3. Y. Sato et al., DART: dependable VLSI test architecture and its implementation, in *Proceedings of the International Test Conference (ITC'12), paper 15.2* (2012)
4. International Technology Roadmap for Semiconductors, 2011 edn. (2011), http://www.itrs2.net/
5. W. Wang et al., Compact modeling and simulation of circuit reliability for 65-nm CMOS technology. IEEE Trans. Device Mater. Reliab. **7**(4), 509–517 (2007)
6. J.B. Velamala et al., Physics matters: statistical aging prediction under trapping/detrapping, in *Proceedings of the Design Automation Conference (DAC'12)* (2012), pp. 139–144
7. Y. Cao, Modeling & simulation tools for resilient nanoelectronic design, in *Proceedings of the Workshop on Design for Reliability and Variability (DRV'08)* (2008)
8. M. Nicolaidis, Y. Zorian, On-line testing for VLSI-A compendium of approaches. J. Electron. Test. Theory Appl. **12**(1–2), 7–20 (1998)
9. H. Al-Asaad et al., Online BIST for embedded systems. IEEE Des. Test Comput. **15**(4), 17–24 (1998)
10. S. Dikic et al., BIST and fault insertion re-use in telecom systems, in *Proceedings of the international test Conference (ITC'01)* (2001), pp. 1011–1016
11. J. Braden et al., Use of BIST in FIRETM Servers, in *Proceedings of the International Test Conference (ITC'01)* (2001), pp. 1017–1022
12. D. Ernst et al., Razor: A low-power pipeline based on circuit-level timing speculation, in *Proceedings of the International Symposium on Microarchitecture (MICRO'03)* (2003), pp. 7–18
13. S. Mitra et al., Combinational logic soft error correction, in *Proceedings of the International Test Conference (ITC'06), paper 29.2* (2006)
14. T. Sakata et al., A cost-effective dependable microcontroller architecture with instruction-level rollback for soft error recovery, in *Proceedings of the International Conference on Dependable Systems and Networks (DSN'07)* (2007), pp. 256–265
15. Y. Li, S. Makar, S. Mitra, CASP: concurrent autonomous chip self-test using stored test patterns, in *Proceedings of the Design Automation and Test in Europe (DATE'08)* (2008), pp. 885–89
16. H. Inoue et al., VAST: virtualization-assisted concurrent autonomous self-test, in *Proceedings of the International Test Conference (ITC'08), paper 12.3* (2008)
17. J. Qian et al., Logic BIST architecture for system-level test and diagnosis, in *Proceedings of the Asian Test Symposium (ATS'09)* (2009), pp. 21–28
18. O. Khan, S. Kundu, A self-adaptive system architecture to address transistor aging, in *Proceedings of the Design Automation and Test in Europe (DATE'09)* (2009), pp. 81–86
19. Y. Li et al., Operating system scheduling for efficient online self-test in robust systems, in *Proceedings of the International Conference on Computer-Aided Design (ICCAD'09)* (2009), pp. 201–208
20. N. Kanekawa et al., *Dependability in Electronic Systems* (Springer, 2010), ISBN 978-1-4419-6714-5
21. International Electrotechnical Commission, IEC61508, Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems, Ed.2.0, 2010-4 (2010), http://www.iec.ch/functionalsafety/
22. Y. Miura et al., On-chip temperature and voltage measurement for field testing, in *Proceedings of the European Test Symposium (ETS'12)* (2012), p. 204

23. T. Yoneda et al., Thermal-uniformity aware x-filling to reduce temperature-induced delay variation for accurate at-speed testing, in *Proceedings of the VLSI Test Symposium (VTS'10)* (2010), pp. 188–193
24. T. Yoneda et al., Temperature-variation aware test pattern optimization, in *Proceedings of the European Test Symposium (ETS'11)* (2011), p. 214
25. S. Wang et al., A pattern partitioning algorithm for field test, in *Proceedings of the 2nd International Workshop on Reliability Aware System Design and Test (RASDAT'11)* (2011), pp. 31–36
26. M. Inoue et al., Optimizing delay test quality with a limited size of test set, in *Proceedings of the International Workshop on Reliability Aware System Design and Test (RASDAT'10)* (2010), pp. 46–51
27. M. Inoue et al., Test pattern selection to optimize delay test quality with a limited size of test set, in *Proceedings of the European Test Symposium (ETS'10)* (2010), p. 260
28. T. Yoneda et al., Seed ordering and selection for high quality delay test, in *Proceedings of the Asian Test Symposium (ATS'10)* (2010), pp. 313–318
29. T. Yoneda et al., Faster-than at speed test for increased test quality and in-field reliability, in *Proceedings of the International Test Conference (ITC'11), paper 2_2* (2011)
30. Y. Yamato et al., A fast and accurate per-cell dynamic IR-drop estimation method for at-speed scan test pattern validation, in *Proceedings of the International Test Conference (ITC'12), paper 6.2* (2012)
31. M. Inoue et al., Test pattern ordering and selection for high quality test under constraints. IEICE Trans. Inf. Syst. **95D**(12), 3001–3009 (2012)
32. M. Noda et al., On estimation of NBTI-induced delay degradation, in *Proceedings of the* european test *Symposium (ETS'10)* (2010), pp. 107–111
33. Y. Sato et al., Multi-cycle test with partial observation on scan-based BIST structure, in *Proceedings of the Asian Test Symposium (ATS'11)* (2011), pp. 54–59
34. Y. Sato et al., Low power BIST for scan-shift and capture power, in *Proceedings of the Asian Test Symposium (ATS'12)* (2012), pp. 173–178
35. S. Wang et al., A scan-out power reduction method for multi-cycle BIST, in *Proceedings of the Asian Test Symposium (ATS'12)* (2012), pp. 272–277
36. H. Yi et al., A failure prediction strategy for transistor aging. IEEE Trans. Very Large Scale Integr. (VLSI) Syst. **20**(11), 1951–1959 (2012)
37. Y. Sato et al., Variable test-timing generation for built-in self-test on FPGA, IEICE Technical Paper (in Japanese), DC2013-69 (2013)
38. Y. Sato et al., Reduction of NBTI-induced degradation on ring oscillators in FPGA, in *Proceedings of the Pacific Rim International Symposium on Dependable Computing (PRDC'14)* (2014), pp. 59–67
39. K. Ito et al., Efficient scan-based BIST architecture for application-dependent FPGA test, in *Proceedings of the Workshop on RTL and High Level Testing (WRTLT'13)* (2013)
40. K. Ito et al., Memory block based scan-BIST architecture for application-dependent FPGA testing, in *Proceedings of the International Symposium on Field-Programmable Gate Arrays (FPGA'14), paper 3.3* (2014)

Chapter 17
Design of SRAM Resilient Against Dynamic Voltage Variations

Masahiko Yoshimoto, Yohei Nakata, Yuta Kimi, Hiroshi Kawaguchi, Makoto Nagata and Koji Nii

Abstract This chapter deals with the design of SRAM cache resilient against dynamic voltage and temperature variations. The scaled CMOS SRAM suffers from a voltage margin reduction owing to the rising of the minimum operating voltage (Vmin), resulting in lower immunity against the dynamic voltage bounce on the power line. In order to solve this critical issue, the authors have proposed a resilient cache which is composed of a 256-KB 8-way cache memory array with 7T/14T bit-enhancing (BE) SRAM, voltage and temperature monitoring circuits, and an autonomous resilient cache controller. The autonomous controller detects degradation of the operating margin caused by the voltage and temperature fluctuation. If the margin is insufficient for stable operation, the controller changes the operating mode of 7T/14T bit-enhancing SRAM from 7T/bit normal operating mode to more reliable 14T/bit-enhancing mode. This adaptive control enables maintenance of the required voltage margin in the current operating condition. The experimental cache was designed and fabricated by 40 nm CMOS technology. The voltage variation tolerance of the resilient cache was evaluated using a voltage droop injection to the external power supply rail. Under 25 and 30% droop conditions, the failures increase linearly with droop duration length without the proposed scheme. Using the proposed scheme, the resilient cache does not fail irrespective of the droop duration length. The failure rate is improved by 91 times of that without the proposed scheme under 35% droop condition with 50 ms duration. The capacity decrease degrades processor performance only by 2.88% when all blocks operate in the enhancing mode.

Keywords Voltage droop · Minimum operating voltage · Autonomous resilient cache · Bit-enhancing SRAM · Online testing

M. Yoshimoto (✉) · Y. Nakata · Y. Kimi · H. Kawaguchi · M. Nagata
Kobe University, Kobe, Japan
e-mail: yosimoto@cs.kobe-u.ac.jp

K. Nii
Renesas Electronics, Tokyo, Japan

S. Asai (ed.), *VLSI Design and Test for Systems Dependability*,
https://doi.org/10.1007/978-4-431-56594-9_17

17.1 Introduction

Technology scaling increases the threshold–voltage (V_{th}) variation of MOS transistors mainly because of random dopant fluctuation. The minimum operating voltage (V_{min}) of SRAM cell increases as the V_{th} variation increases with technology scaling. Increase in the V_{min} degrades operating margin of processors. A processor with a shrinking operating margin is more susceptible to power supply noise, IR drops, and temperature fluctuations. Especially, electric control units in electric vehicles suffer large temperature fluctuation and large voltage fluctuation/droop caused by motor noise, EMIs, voltage surges, and sudden interruptions in wiring harness connections. It may cause malfunctions in processors inducing serious traffic accidents. Consequently, voltage variation and temperature variation-tolerant processors are strongly required for ECU s in electric vehicles.

Earlier designs [1–3] have addressed timing errors caused by a high-frequency (ca. 100 MHz) voltage droop. A tunable replica scheme [4] can reduce V_{min} of SRAM by 9% under 13% voltage droop. However, they cannot mitigate embedded SRAM margin failures caused by large amplitude (ca. 20% of V_{dd}) voltage droops. Dynamic variations strongly affect reliability, particularly in SRAM, because minimum-sized transistors are used in its design. Therefore, an on-chip cache, which is a large SRAM block, determines the V_{min} of the entire processor and a fault-tolerant cache is required to realize dynamic variation-tolerant processors.

Herein, we present a resilient on-chip cache memory that can perform sustained operations under a large amplitude–voltage droop.

17.2 Resilient Cache

The resilient cache (Fig. 17.1) the authors have proposed comprises a 256-KB 8-way cache memory array with 7T/14T bit-enhancing (BE) SRAM [5], voltage and temperature monitoring circuits [6], and an autonomous resilient cache controller. The autonomous resilient cache controller comprises an autonomous controller and an online testing controller with a test module and data transfer unit.

7T/14T bit-enhancing SRAM has a more reliable operating mode as well as a normal operating mode. The memory array is separated into eight memory blocks. A power supply of each memory block can be switched to the power supply for runtime operation ($V_{\mathrm{dd\_rt}}$) or the power supply for testing ($V_{\mathrm{dd\_test}}$) individually. The local power rails of the memory blocks are monitored by voltage monitoring circuits, which can obtain a precise supply voltage level at a testing time and monitor the voltage fluctuation during runtime. Furthermore, a temperature monitoring circuit can sense the on-chip temperature. The temperature information recorded at a testing time is used in a temperature correction of the V_{min}. The online testing controller can execute memory testing that is completely transparent to user accesses and which can obtain operating margin and V_{min}s of the memory blocks.

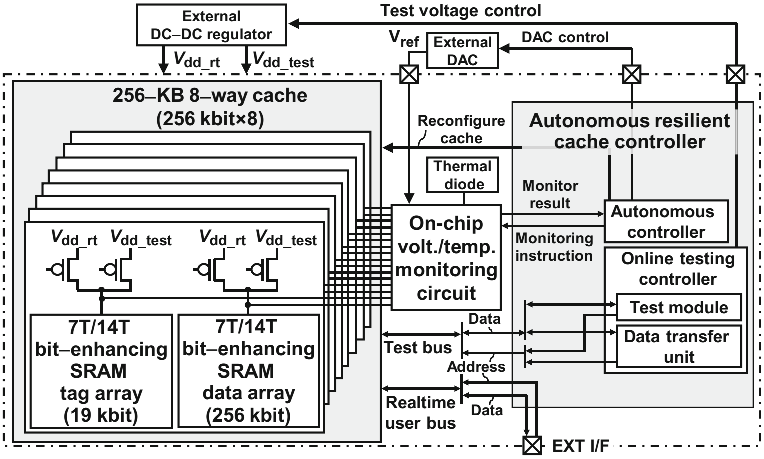


Fig. 17.1 Block diagram of the resilient cache

The autonomous controller controls a probing point of the voltage monitor and reference voltage (V_{ref}) using the external DAC. It receives monitoring results from monitoring circuits. The results are used for voltage droop detection and block-basis voltage droop control, as described in the remainder of this chapter.

17.2.1 7T/14T Bit-Enhancing SRAM

Each SRAM cell in the resilient cache comprises 7T/14T BE SRAM cell structure [5]. 7T/14T BE SRAM has an additional operating mode designated as the enhancing mode along with the normal mode. In the enhancing mode, 7T/14T BE SRAM features reliable operations especially at low voltages. The two operating modes of 7T/14T SRAM can be dynamically switched according to the required operating margin. The operating mode of 7T/14T BE SRAM is explained in detail in Sect. 6.4.2.

17.2.2 On-chip Monitoring Circuits

On-chip monitoring circuits, presented in Fig. 17.2, comprise a source follower (SF) and a latch comparator (LC) [6]. Supply voltage monitoring circuits measure the supply voltage fluctuation on power rails of each SRAM array. Temperature monitoring circuits sense thermal diodes placed near the center of the cache macro.

The voltages at the probing point and thermal diode are level-shifted by the SFs. The level-shifted voltage (V_{sfo}) is compared with the reference voltage (V_{ref}) by the

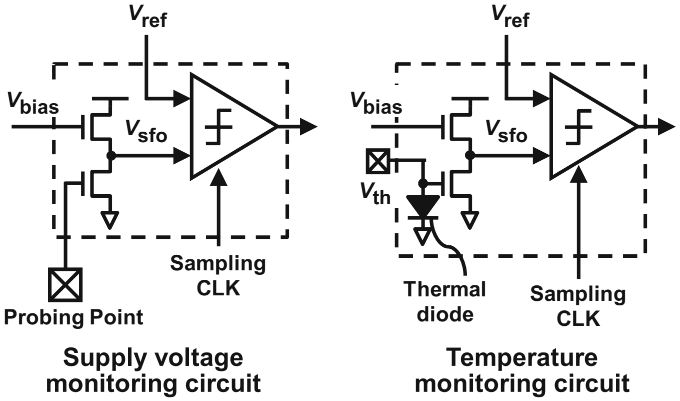


Fig. 17.2 Supply voltage/temperature monitoring circuits

LC in synchronization with a sampling clock. The LC outputs "1" or "0" corresponding to the comparison result.

The on-chip monitoring circuits are area-efficient and can sense accurate voltage level of the SRAM array, in addition to the cache temperature. Therefore, they are suitable for use in online built-in self-tests (BISTs) and voltage droop detection.

17.2.3 Block-Basis Online Testing

The online testing controller measures operating margin and V_{min}s of the memory blocks with current temperature. The adaptive control using the online testing result can deal with dynamic temperature fluctuation at operating time, but not during the boot time testing. Figure 17.3 shows the block-basis online testing scheme for the resilient cache. The online testing controller conducts memory testing on each

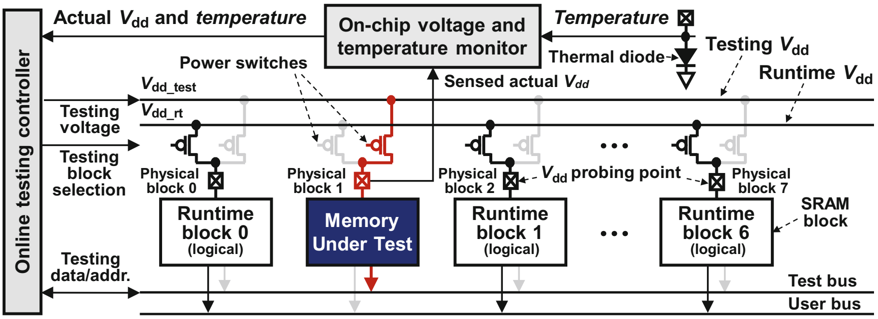
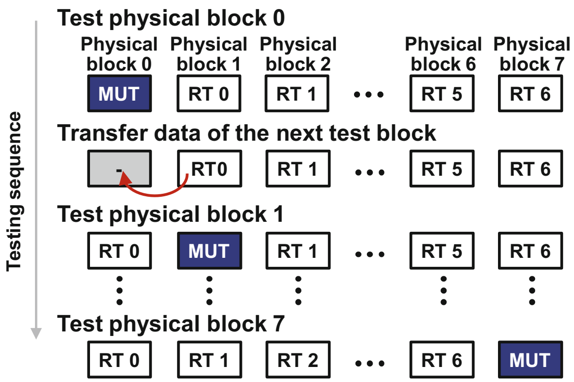


Fig. 17.3 Online testing architecture

Fig. 17.4 Block-basis online testing scheme

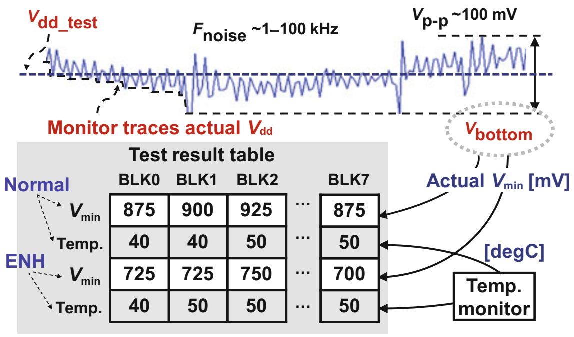


memory block in order of the physical block address. It decreases the supply voltage of the testing block gradually during the testing time. The controller records the testing voltage and temperature from the on-chip monitoring circuits with respect to each operating mode of 7T/14T BE SRAM at which the first failure is detected. The resilient cache still has cache lines to which data can be allocated even if memory testing is working because it is block-basis testing. The memory blocks, except the current memory under test (MUT) block, are still accessible. Thereby they can operate as runtime (RT) blocks. The testing does not disturb the processor operation because the testing controller uses the test bus separated from the user bus.

Operation of the data transfer unit is depicted in Fig. 17.4. First, physical block 0 is tested. Physical blocks of 1–7 operate as runtime blocks. Next, the data transfer unit transfers data from physical block 1 (next MUT) to physical block 0 (previous MUT). After the transfer, physical block 1 is tested. Physical block 0 and physical blocks 2–7 operate as runtime blocks. In this way, the MUT block moves among eight blocks without losing the memory contents.

An example of test results is presented in Fig. 17.5. The online testing controller has a test result table to record V_{min} corresponding to temperature. The recorded testing voltage is actual V_{min} of the memory array because the on-chip voltage

Fig. 17.5 Block-basis actual V_{min} and temperature recording



Test result table

		BLK0	BLK1	BLK2	···	BLK7
Normal	V_{min}	875	900	925	···	875
	Temp.	40	40	50	···	50
ENH	V_{min}	725	725	750	···	700
	Temp.	40	50	50	···	50

monitor probes the local power rails of the memory blocks. The voltage monitor traces the bottom level of the testing voltage (V_{bottom}) during the testing time to record an actual V_{min}. The test result table is used as a reference for the voltage–temperature variation adaptive control described later.

17.2.4 Voltage and Temperature Variation Adaptive Control

The autonomous controller detects degradation of the operating margin caused by the voltage and temperature fluctuation. If the margin is insufficient for stable operation, the controller changes the operating mode of 7T/14T bit-enhancing SRAM to the 14T enhancing mode. This adaptive control enables maintenance of the required voltage margin in the current operating condition.

To detect the voltage droop, reference voltages "high" ($V_{\mathrm{ref\_high}}$) and "low" ($V_{\mathrm{ref\_low}}$) are set to the proper level as shown in Fig. 17.6a. V_{dd} is monitored by the monitoring circuit using $V_{\mathrm{ref\_high}}$ and $V_{\mathrm{ref\_low}}$. When V_{dd} falls below $V_{\mathrm{ref\_high}}$, a timer starts to count. Then, as V_{dd} falls below $V_{\mathrm{ref\_low}}$, the timer stops to count and a gradient of the voltage droop is calculated. The autonomous controller estimates whether the V_{dd} drops below $V_{\mathrm{min\_normal}}$ or not using the gradient. If the gradient is greater than the threshold value, then the controller estimates that the V_{dd} crosses $V_{\mathrm{min\_normal}}$. If not, then the controller estimates that the V_{dd} does not cross $V_{\mathrm{min\_normal}}$ (shown in Fig. 17.6b). The resilient cache changes the operating mode to the 14T enhancing mode at the V_{dd} below $V_{\mathrm{min\_normal}}$.

This voltage variation adaptive control scheme is performed in a block-basis manner. Only blocks for which the V_{dd} drops below its $V_{\mathrm{min\_normal}}$ change the

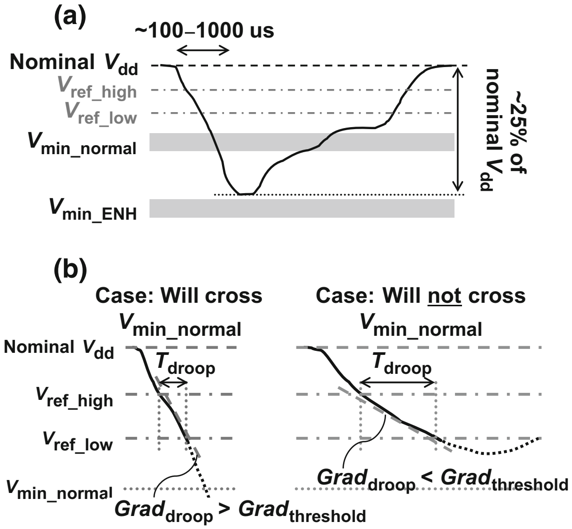
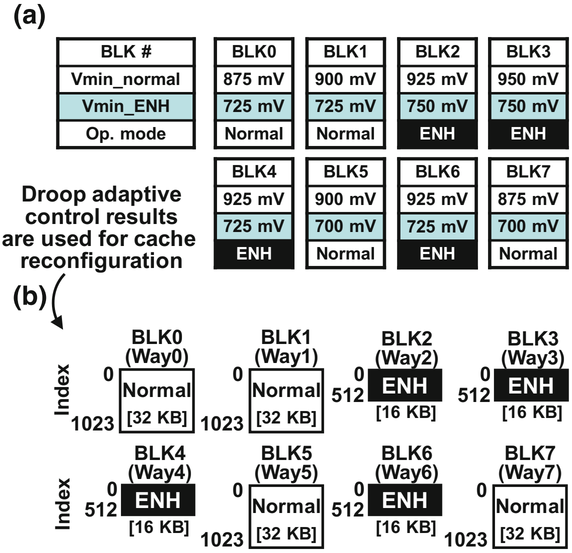


Fig. 17.6 **a** Example of voltage waveform. **b** Voltage droop detection scheme

operating mode to the 14T enhancing mode as presented in Fig. 17.7. The other blocks keep the operation mode as the 7T normal mode. If the V_{dd} is over $V_{\mathrm{ref\_high}}$ again, then the autonomous controller changes the operating mode of the blocks from the enhancing mode to the normal mode.

One-bit data in the enhancing mode block is made up of a pair of memory cells. Therefore, the capacity of the block is halved. In the resilient cache, only half indexes are activated in the enhancing mode block. To reconfigure the block, the tag array of the resilient cache must be modified. One bit is added to the tag bits in each cache line. The comparators for the tag comparison must be extended for the additional bit. The additional bit holds LSB of the index and is compared to the LSB of tag bits. Moreover, the decoder must be designed so as not to choose the half index. The LSB of the decoder input is fixed to “0” in the enhancing mode.

The V_{min} at runtime is corrected in response to the runtime temperature to compensate the temperature fluctuation (shown in Fig. 17.8). The autonomous controller obtains the current temperature using the on-chip temperature monitor and looks up V_{min} in the test result table. The V_{min} corresponding to the current temperature is calculated using these data. The coefficient data to compensate temperature difference between the testing time and current time are recorded in coefficient tables. The calculated V_{min} are collected in V_{min} tables. The V_{min} tables are used to determine the threshold of the gradient in the droop detection.



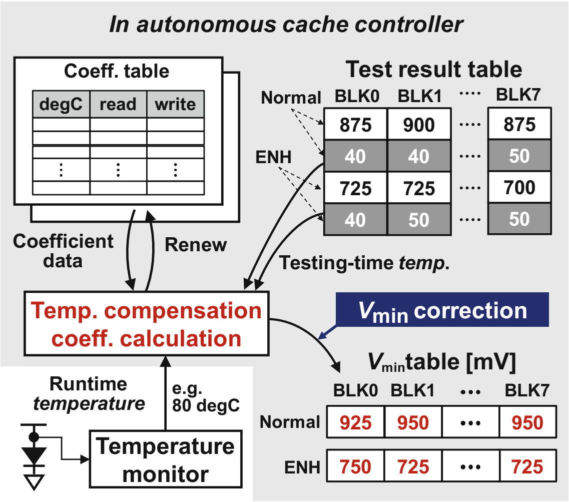
BLK #	BLK0	BLK1	BLK2	BLK3
Vmin_normal	875 mV	900 mV	925 mV	950 mV
Vmin_ENH	725 mV	725 mV	750 mV	750 mV
Op. mode	Normal	Normal	ENH	ENH

BLK #	BLK4	BLK5	BLK6	BLK7
Vmin_normal	925 mV	900 mV	925 mV	875 mV
Vmin_ENH	725 mV	700 mV	725 mV	700 mV
Op. mode	ENH	Normal	ENH	Normal

Droop adaptive control results are used for cache reconfiguration

Fig. 17.7 **a** Block-basis voltage droop control. **b** Cache configuration during voltage droop

Fig. 17.8 $V_{\min}$ correction responding to temperature variation



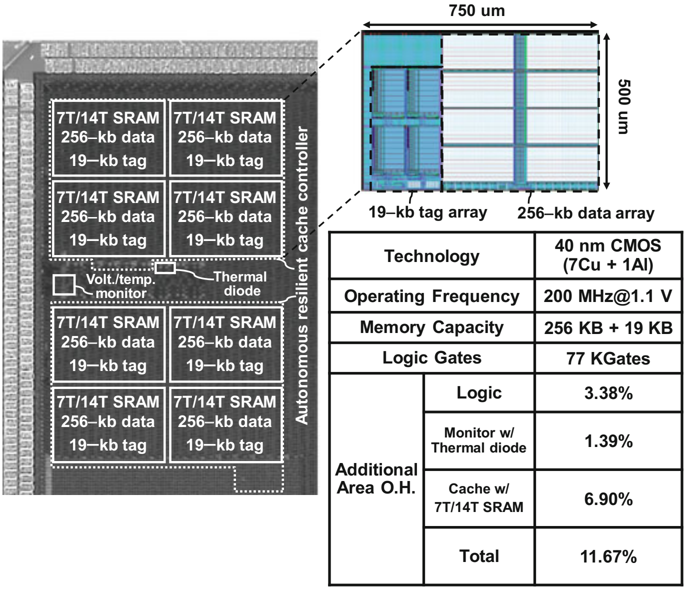
17.3 Measurement Results

Measurement results are obtained using a test chip fabricated in 40-nm CMOS (Fig. 17.9).

17.3.1 On-chip Voltage Droop Waveform and V_{min} of Memory Blocks

The voltage monitoring circuit measures the on-chip voltage droop waveform (Fig. 17.10). The upper waveform in Fig. 17.10 is the injected waveform from outside the chip. This waveform is measured at off-chip probing point on the global power rail. The lower waveform is acquired by measurement with the on-chip monitoring circuit, which probes the local power rail of each memory block. The on-chip measurement waveform shows a different shape from that of the injected waveform because of parasitic elements of the chip. The result shows that the on-chip monitoring circuit is necessary to obtain a precise voltage level.

Measured minimum operating voltage ($V_{\min}$) characteristics of the memory blocks are shown in Fig. 17.11. The $V_{\min}$s are acquired for 8 blocks of 11 chips at each operating mode of 7T/14T BE SRAM. The temperature at the measurement is normal (25 °C) and high (100 °C). The averages of the $V_{\min}$ of the worst block (i.e., $V_{\min}$ of the entire cache) for 11 chips are 1015 mV in the normal mode and 806 mV in the enhancing mode at 25 °C. At 100 °C, the average $V_{\min}$ in the normal and the enhancing modes are 1050 mV and 827 mV, respectively. Results show that changing the operating mode of 7T/14T BE SRAM to the enhancing mode



Technology		40 nm CMOS (7Cu + 1Al)
Operating Frequency		200 MHz@1.1 V
Memory Capacity		256 KB + 19 KB
Logic Gates		77 KGates
Additional Area O.H.	Logic	3.38%
	Monitor w/ Thermal diode	1.39%
	Cache w/ 7T/14T SRAM	6.90%
	Total	11.67%

Fig. 17.9 Micrograph and features of test chips

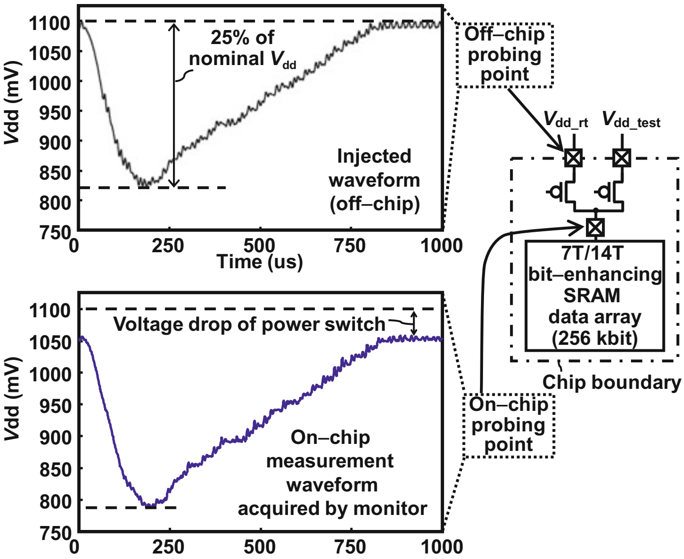


Fig. 17.10 Measured off-chip/on-chip voltage droop waveforms

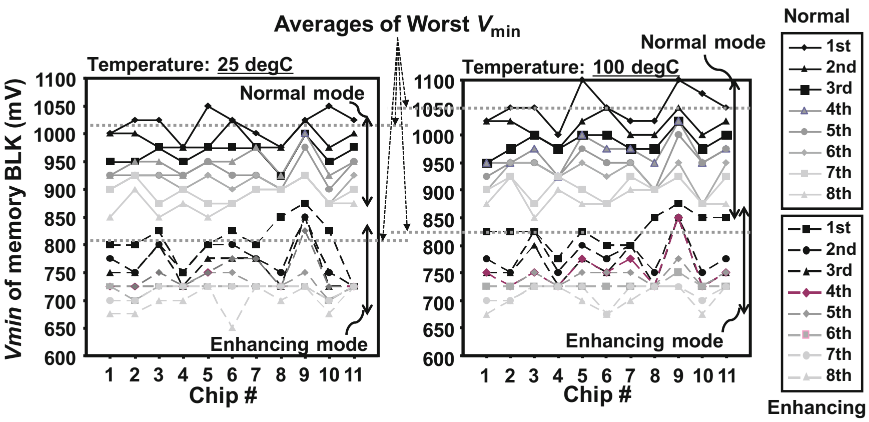


Fig. 17.11 V_{min}s of eight memory blocks of 11 chips (measured)

improves the operating margin by 205 mV at 25 °C and 223 mV at 100 °C, on average.

17.3.2 Voltage Variation Tolerance

The voltage variation tolerance of the resilient cache is evaluated using a voltage droop injection to the external power supply rail. During voltage droop injection, the trace of cache access is input to the resilient cache. Then, the accesses to fail bits are counted as the number of failures. Five cache traces were taken from SPEC 2006 [7]. The amplitudes of the voltage droop are assumed to be 25, 30, and 35% of V_{dd} as shown in Fig. 17.12a. The droop durations are 500 μs, 5 ms, and 50 ms. Evaluation results under 25, 30, and 35% droop condition are depicted, respectively, in Fig. 17.12b–d. Under 25 and 30% droop conditions, the failures increase linearly with droop duration length without the proposed scheme (no variation adaptive control and always in the normal mode). Using the proposed scheme (variation adaptive control and adopt switching to the enhancing mode), the resilient cache does not fail irrespective of the droop duration length. Under a severe 35% droop condition, failures without the proposed scheme increased numerically to about ten times those under a 25% droop condition. Using the proposed scheme, the failure rate is improved by 91 times of that without the proposed scheme under 50 ms droop duration.

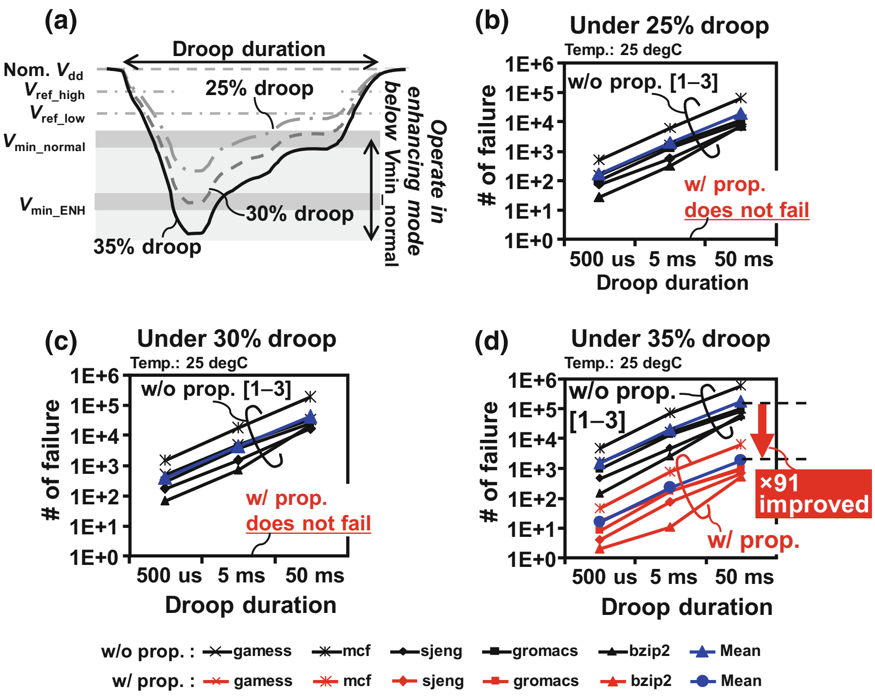


Fig. 17.12 Voltage droop tolerance and failure count evaluation: **a** droop waveform example, **b** 25% V_{dd} droop, **c** 30% V_{dd} droop, and **d** 35% V_{dd} droop

17.3.3 Processor Performance

We will now discuss how the cache reconfiguration affects the processor performance. The cache capacity decreases by 16 KB when one block changes its operating mode into the enhancing mode. The capacity decrease degrades processor performance since cache misses occur more frequently. Figure 17.13 shows the normalized instructions per cycles (IPCs) with respect to the number of the

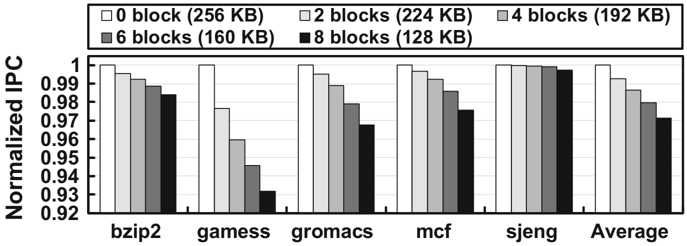


Fig. 17.13 Normalized IPCs with respect to the number of the enhancing mode blocks

enhancing mode blocks. The evaluation is conducted using gem5 simulator [8], with benchmarks selected from SPEC 2006 [7]. The average IPC loss is 2.88% when all blocks operate in the enhancing mode (128 KB cache capacity). The resilient cache operates in the enhancing mode only if the operating margin is insufficient and continues stable operation though processor performance degrades temporally.

17.4 Conclusion

In this chapter, we have described a resilient cache for dynamic voltage and temperature variation tolerance with 7T/14T bit-enhancing SRAM and on-chip diagnosis structures in 40-nm CMOS. 7T/14T bit-enhancing SRAM can dynamically change itself to the enhancing mode. The on-chip diagnosis structure uses on-chip voltage/temperature monitoring circuits and online memory testing scheme. The resilient cache dynamically reconfigures its operating mode using voltage/temperature monitoring result and testing result. Experimental results show that it does not fail under 25 and 30% droop of V_{dd} and it provides 91 times better failure rate under a 35% droop condition compared with the conventional design.

References

1. K.A. Bowman, C. Tokunaga, J.W. Tschanz, A. Raychowdhury, M.M. Khellah, B.M. Geuskens, S.L. Lu, P.A. Aseron, T. Karnik, V.K. De, All-digital circuit-level dynamic variation monitor for silicon debug and adaptive clock control. IEEE Trans. Circuits Syst. I **58** (9), 2017–2025 (2011)
2. K.A. Bowman, J.W. Tschanz, S.L. Lu, P.A. Aseron, M.M. Khellah, A. Raychowdhury, B.M. Geuskens, C. Tokunaga, C.B. Wilkerson, T. Karnik, V.K. De, A 45 nm resilient microprocessor core for dynamic variation tolerance. IEEE J. Solid-State Circuits **46**(2), 194–208 (2011)
3. J. Tschanz, N.S. Kim, S. Dighe, J. Howard, G. Ruhl, S. Vangal, S. Narendra, Y. Hoskote, H. Wilson, C. Lam, M. Shuman, C. Tokunaga, D. Somasekhar, S. Tang, D. Finan, T. Karnik, N. Borkar, N. Kurd, and V.K. De, Adaptive frequency and biasing techniques for tolerance to dynamic temperature-voltage variations and aging, in *Digest of Technical Papers of International Solid-State Circuits Conference* (Feb 2007), pp. 292–293
4. A. Raychowdhury, B. Geuskens, K. Bowman, J. Tschanz, S.L. Lu, T. Karnik, M. Khellah, V. K. De, Tunable replica bits for dynamic variation tolerance in 8T SRAM arrays. IEEE J. Solid-State Circuits **46**(4), 797–805 (2011)
5. H. Fujiwara, S. Okumura, Y. Iguchi, H. Noguchi, H. Kawaguchi, M. Yoshimoto, A 7T/14T dependable SRAM and its array structure to avoid half selection, in *Proceedings of International Conference on VLSI Design* (Jan 2009), pp. 295–300
6. K. Noguchi, M. Nagata, An on-chip multichannel waveform monitor for diagnosis of systems-on-a-chip integration. IEEE Trans. Very Large Scale Integrator (VLSI) Syst. **15**(10), 1101–1110 (2007)

7. Standard Performance Evaluation Corporation, The SPEC CPU 2006 Benchmark Suite, http://www.specbench.org
8. N. Binkert, S. Sardashti, R. Sen, K. Sewell, M. Shoaib, N. Vaish, M.D. Hill, D.A. Wood, B. Beckmann, G. Black, S.K. Reinhardt, A. Saidi, A. Basu, J. Hestness, D.R. Hower, T. Krishna, The gem5 simulator. ACM SIGARCH Comput. Archit. News **39**(2), 1–7 (2011)

Chapter 18
Design and Applications of Dependable Nonvolatile Memory Systems

Shuhei Tanakamaru and Ken Takeuchi

Abstract This chapter discusses how to build dependable nonvolatile memory systems that range from the SD card to high-performance enterprise storage. The nonvolatile memory systems are mainly composed of NAND flash memories because of their high bit density. However, the reliability of the NAND flash memory is degrading along with the memory-cell scaling. Therefore, the adoption of the highly reliable techniques is becoming increasingly important. On the other hand, storage-class memories (SCMs) are attracting much attention because of the higher performance than NAND flash memories. Since the cost is higher than the NAND flash memories, NAND flash/SCM hybrid configuration is developed. Therefore, some of the techniques introduced in this chapter are for the hybrid storage where SCMs are exploited as nonvolatile buffer. Dynamic codeword transition ECC and error-prediction (EP-) low-density parity-check (LDPC) schemes are the techniques related to the error-correcting codes (ECCs). Page-RAID, reverse mirroring (RM), and shift mirroring (SM) are described as redundant arrays of independent disks (RAID). Moreover, data preprocessing techniques such as asymmetric coding and stripe pattern elimination algorithm (SPEA) are introduced. Error recovery (ER) and error masking (EM) schemes are shown as the techniques which cannot be fit into the above classifications. To design dependable nonvolatile systems, techniques should be selectively applied from each layer (ECC, RAID, data preprocessing, and others) to satisfy the cost, performance, and reliability requirements of the application. Therefore, the storage overhead (cost), performance, and the acceptable bit error rate improvement (reliability) are compared among techniques in this chapter.

Keywords NAND flash memory • Storage-class memory (SCM)
Signal processing • Error-correcting code (ECC) • Redundant arrays of independent disks (RAID)

S. Tanakamaru · K. Takeuchi (✉)
Chuo University, Tokyo, Japan
e-mail: takeuchi@takeuchi-lab.org

S. Tanakamaru
e-mail: tanakamaru@takeuchi-lab.org

S. Asai (ed.), *VLSI Design and Test for Systems Dependability*,
https://doi.org/10.1007/978-4-431-56594-9_18

18.1 Introduction

NAND flash memory-based nonvolatile memory systems are significantly increasing demands because of their high performance, low power, and small form factor. Their applications are expanding extremely rapidly, from SD cards to ultrahigh-performance enterprise storage systems. However, as discussed in Sect. 6.2, the reliability of the NAND flash memory degrades as the memory-cell scaling, which causes the significant tradeoff between the cost (memory-cell size) and reliability. To drive the market adoption of NAND flash memories, their cost should be continuously decreased. As a result, the reliability of the memory system should be ensured by the system side.

On the other hand, storage-class memories (SCMs) are attracting much attention because SCMs can achieve faster operation and higher endurance than NAND flash with nonvolatility. According to the presentation slides of [1], the bit cost and the performance (latency) are in between DRAMs and NAND flash. Therefore, hybrid NAND flash/SCM storage is researched to achieve high performance with low cost overhead [2–5].

This chapter describes the off-chip reliability enhancement techniques and discusses the design and applications of dependable nonvolatile memory systems. Note that various on-chip dependable techniques are also implemented inside NAND flash memory, which cannot completely compensate the reliability degradation (see Sect. 6.2). Since the current nonvolatile memory systems are dominated by NAND flash memories, techniques in this chapter are applied to improve the reliability of NAND flash memories. Moreover, some of the techniques effectively use SCMs as nonvolatile buffer, not to degrade the storage performance or cost while attaining nonvolatility.

18.2 Background

Figure 18.1 shows the NAND flash-only SSD (Solid-State Drive) and NAND flash/SCM hybrid SSD. Basically, in any levels of nonvolatile memory system (SD cards to enterprise storage), NAND flash memories (and SCMs) are controlled by the controller. The controller manages the logical/physical address translation, wear leveling, interleaving, error correction, etc. [6]. The reliability enhancement techniques (some of which are introduced in this chapter) are also handled by the controller. NAND flash memories do not accept in-place overwrite because cells should be erased before writing. As a result, if multiple writes are issued to the same logical address which is managed by the host, the data are written to the different memory cells (physical address) in the NAND flash memory. Therefore, the logical address should be translated to the internal physical address. Since the bit error rate (BER) of the NAND flash memory significantly increases by write/erase cycling, the write/erase cycle of each NAND block should be equalized by wear leveling.

Otherwise, intensive writes and erases will cause uncorrectable faults in a block, which results in malfunction. Wear leveling also requires logical/physical address translation. NAND flash memories are operated in parallel to enhance the performance (interleaving). Bit errors that have occurred in the NAND flash memory are corrected by error-correcting codes. In NAND flash/SCM hybrid SSDs, data allocation management is also required in the SSD controller to fully exploit the high performance of the SCMs. Hot (frequently updated) or random (small size) data are written to the SCM because the slow write of the NAND flash memory is enhanced by those data types [6].

The basics of the NAND flash memory is described in Sect. 6.2. As for SCMs, magnetic RAM (MRAM) [7], phase-change RAM (PCRAM) [8], resistive RAM (ReRAM) [9], etc. can be used which are summarized in [1] (Fig. 18.2). In an MRAM cell, magnetic tunnel junction (MTJ) is used, which has ferromagnetic–insulator–ferromagnetic layer construction. The polarity of one ferromagnetic layer is fixed, and the other layer can be switchable. When the polarity of the two layers is the same, the resistance of the MRAM cell becomes low. In PCRAM, chalcogenide materials are used, which can be changed to either amorphous (high resistance) or crystal (low resistance) by applying current. The current melts the chalcogenide material, and after that, if the current is controlled so that the layer is gradually cooled, crystal state can be realized. Metal oxides, e.g., HfO_2, are used as ReRAM cell [10]. When current is appropriately controlled, a conductive filament is formed by generating oxygen vacancy. The other current can put the oxygen back to the filament to rupture the filament.

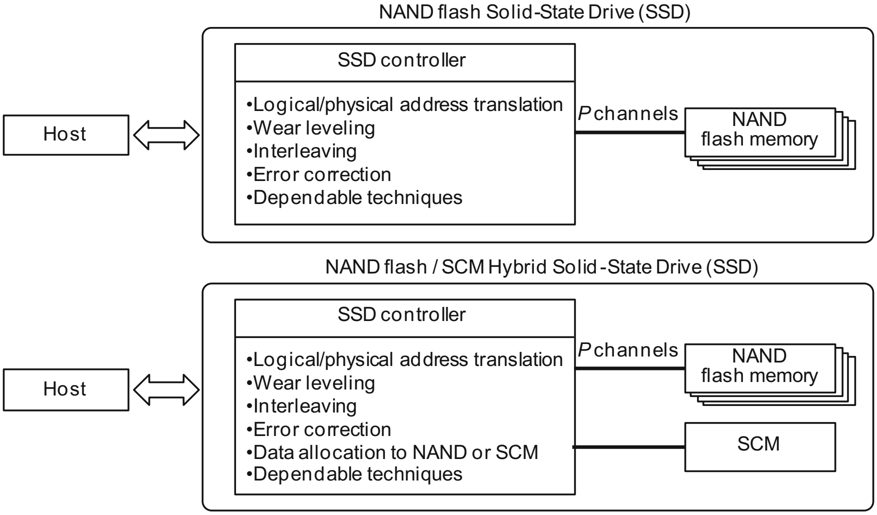


Fig. 18.1 NAND flash-only and NAND flash/SCM hybrid SSDs [5]

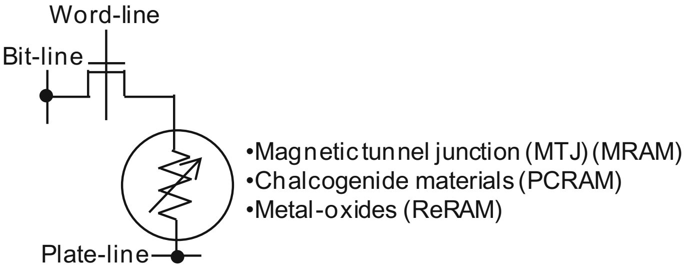

Word-line
Bit-line
•Magnetic tunnel junction (MTJ) (MRAM)
•Chalcogenide materials (PCRAM)
•Metal-oxides (ReRAM)
Plate-line

Fig. 18.2 Basic configuration of SCMs

18.3 Reliability Improvement Techniques

This chapter introduces reliability improvement techniques based on the following perspectives: error-correcting codes (ECCs), redundant arrays of independent disks (RAID), data preprocessing, and the others.

18.3.1 Techniques Related to Error-Correcting Codes (ECCs)

ECCs are the most essential dependable techniques for nonvolatile memory systems. Here, two techniques, dynamic codeword transition ECC [11] and error-prediction (EP-) low-density parity check (LDPC) [12] schemes are described, which enhance the reliability of the SSD.

In NAND flash memory, the BER significantly increases, as the number of write/erase cycles [13] is increased. The strength of the ECC is fixed and set to handle the worst-case BER, which occurs at the end of chip's life (maximum write/erase cycles) determined by the SSD manufacturer. In the early lifetime of the NAND flash memory (small write/erase cycle), the strong/fixed ECC is not only over-quality but also spoils the chance to realize smaller ECC power consumption and shorter ECC calculation latency with the weaker ECC. The dynamic codeword transition ECC scheme gradually increases the ECC strength, according to the reliability (BER) of the NAND flash memory, to realize reliability high enough with smaller ECC power consumption and shorter ECC calculation latency as possible [11]. The key point is that in the dynamic codeword transition ECC scheme, the code length of the ECC is doubled, quadrupled, and so on before the uncorrectable bit error rate after ECC exceeds the required quality (e.g., 10^{-15}), while the code rate [(user data size)/(code length)] is kept almost constant (Fig. 18.3). In the NAND flash memory, a page consists of user data and parity region. In the dynamic codeword transition ECC scheme, the parity cells in the NAND flash memory can be always mostly utilized, which is not the case if only the parity bits are increased

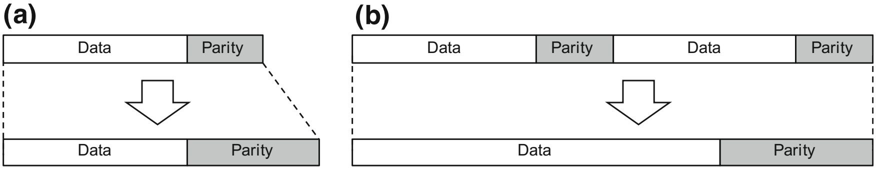


Fig. 18.3 **a** ECC strengthening by increasing only the number of parity bits [14]. **b** Dynamic codeword transition ECC scheme [11]

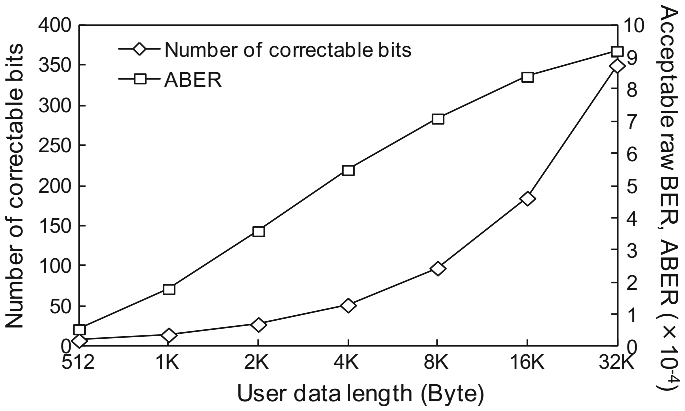


Fig. 18.4 Number of correctable bits and acceptable raw BER (ABER) versus user data length [11]

to strengthen the ECC [14]. If the BCH ECC is strengthened from “8 bit correction/1 kB codeword” to “350 bit correction/32 kB codeword”, the acceptable raw BER of the NAND flash memory can be enhanced by 17-times as shown in Fig. 18.4 [11].

As mentioned in Sect. 6.2, the BER of the scaled NAND flash memory is so high that LDPC ECC will be needed [12]. Many read cycles with slightly different reference voltages are required to obtain the precise threshold voltage information (which is called *soft information*; *hard information* is binary “1” or “0”), which causes a serious performance degradation, compared with the conventional BCH ECC scheme. Error-prediction (EP-) low-density parity-check (LDPC) scheme reduces the number of read cycles identical to the BCH ECC case when the data are sequential (stored over many pages) [12]. Instead of extracting precise threshold voltage information, EP-LDPC scheme estimates the BER of each memory cell by estimating the data retention time and considering the neighboring cells’ data. First, the overall BER is estimated from the number of “1”s in the write data and the read data (the bit errors change the number of “1”s during data retention). Then, comparing the estimated BER and the pre-recorded reliability table that stores the relation between the BER and the data retention time enables to estimate the data retention time. From the estimated data retention time, overall BER, and neighboring cell data, the BER of each cell can be estimated based on the other pre-recorded table which stores the relation among the neighboring cell data and the target cell data with various data retention times. The estimated BER is transferred to the LDPC decoder as soft information instead of the precise threshold voltage value. As a result, the acceptable data retention time increases by over 10 times, compared with the conventional BCH ECC scheme, while the sequential read performance is not degraded as the conventional soft-decision decoding LDPC scheme.

18.3.2 Techniques Related to Redundant Arrays of Independent Disks (RAID)

Page-RAID is proposed as a within-block RAID scheme for NAND flash memory and ReRAM (SCM) storage [15]. The parity is generated by XORing the bits in the bit-line direction, whereas ECC is applied in the word-line direction as shown in Fig. 18.5. When there is a page which is uncorrectable by ECC, the page can be recovered by XORing the other existing page data. Since the in-place overwriting in the NAND flash memory is prohibited, the parity is updated every time when a page is written and temporarily stored in the SCM (parity buffer). When the block is becoming full, the parity data is written to the final page of the block. The parity data is updated $N - 1$ times, where N is the number of pages in a block (e.g., 256). Therefore, the endurance of the parity buffer should be large, and thus, SCM is suitable for SCM buffer. Considering the high endurance up to 10^7 [16, 17], the capacity of the SCM can be as small as below 0.1% of the storage capacity. Moreover, since the performance of SCMs is high (e.g., 1 μs), the write access time increases by only 1%. The write access time is roughly doubled if the MLC NAND flash memory is used as the parity buffer. Note that volatile memories such as DRAMs cannot handle the sudden power outage. The acceptable BER is increased by 45% with page-RAID.

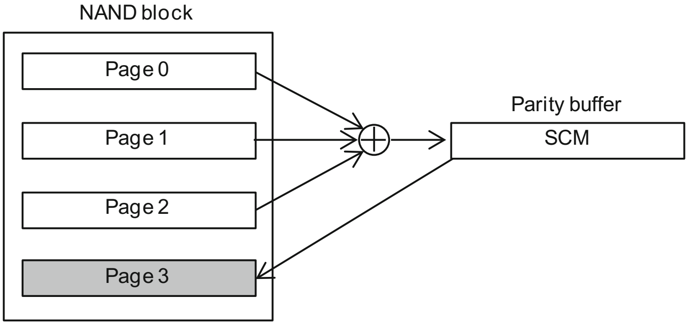


Fig. 18.5 Page-RAID [15]
]

Mirroring schemes (RAID-1) are also proposed to utilize the error characteristics of the NAND flash memories: Reverse mirroring (RM) and shift mirroring (SM) [15]. In the measurements of the 2Xnm MLC NAND flash memory, it is found that immediately after programming, the BER of the lower page is much larger than that of the upper page. (In MLC NAND flash, a physical word line is divided into two logical pages (upper/lower pages).) Moreover, the BER of the large page number cells is larger than that of the small page number cells after data retention. The concept of both the RM and SM is to pair the cells with relatively high and low reliabilities. If low-reliability cells are paired, the pair limits the overall reliability of the storage system. During read, the data from the higher reliability cell are read. RM accompanies SCM so that the data pairing can be most effective. On the other hand, SM is realized without SCM and the reliability improvement is slightly smaller than RM.

RM is explained in Fig. 18.6. RM literally reverses the order of the data in a mirrored block. For example, when a NAND block has four pages (simplified for explanation), data are written to the page number 0, 1, 2, and 3 of the primary NAND flash memory, and also written to the page number 3, 2, 1, and 0 of the mirrored NAND flash, respectively. This operation enables to pair lower/upper pages and pages with large/small page number. In NAND flash memory, the order of page writing is restricted to 0, 1, to 3 in ascending order to suppress the cell-to-cell interference [18]. Therefore, to *reverse* the data in the mirrored NAND flash memory, data should be buffered in an SCM (immune to sudden power outage), and after a full block is written in the primary NAND flash memory, the buffered data is written to the mirrored NAND flash memory in the reversed order.

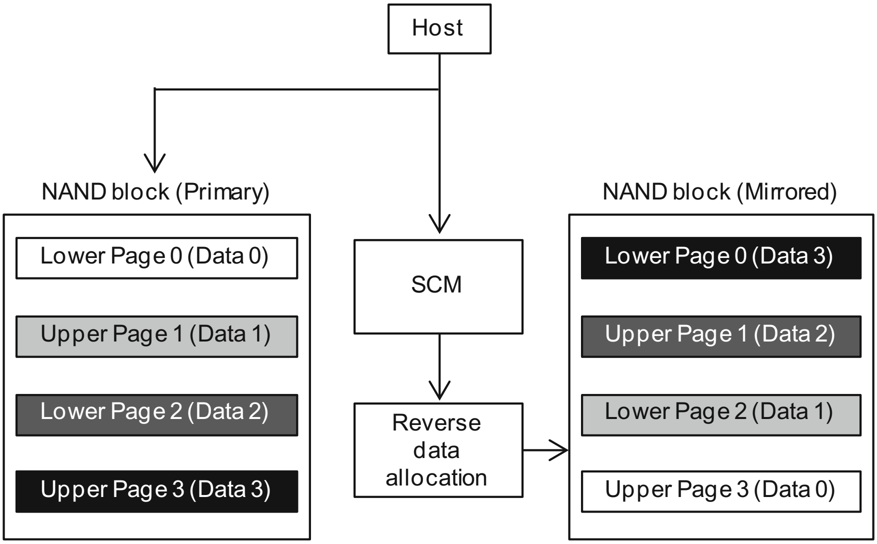


Fig. 18.6 Reverse mirroring (RM) [15]

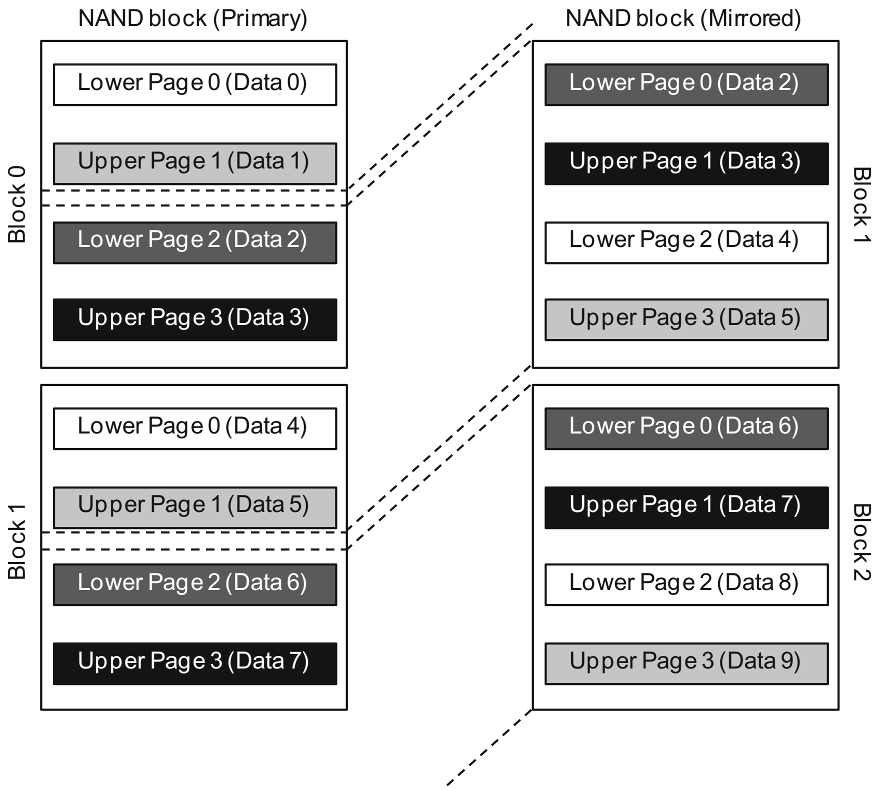


Fig. 18.7 Shift mirroring (SM) [15]

The worst BER in a block immediately after programming and after data retention is improved by 69 and 41%, respectively.

In SM which is shown in Fig. 18.7, the data written to the page number x of the primary NAND flash are written to the page number $x + i$ of the mirrored NAND flash memory. If $x + i$ exceeds the page number (N), the data are written to the page number $x + i - N$ of the next block. i is set around $N/2$. As a result, most of the cells in the upper page are paired with the cells in the lower page, and the pages in the first half of the block are paired with the latter half, which virtually realizes the same concept as RM. However, although SM has an advantage that SCM is not required, not all upper page cells are paired with lower page cells. As a result, the BER improvements right after programming and after data retention are 57 and 41%, which is smaller than and equal to RM, respectively.

Error-reduction synthesis (ERS) is an error correction technique for mirrored storage with NAND flash memories [15]. In [19], it is observed that there is a dominant error direction (“1” to “0” or “0” to “1” bit errors) in each page, which is different between the page types (upper and lower) and the dominant error condition (program disturb or data retention error dominant condition). For example, “0” to “1” error is dominant in the upper page and the lower page, when the program disturb and data retention error are dominant, respectively. If the dominant error direction is known and the data are mirrored, most of the errors can be corrected by ERS. Suppose data are written to both the primary and mirrored NAND flash memory and the error happens only from “0” to “1”. In ERS, if both bits from the primary and mirrored NAND flash memories are the same, the data are outputted as it is. If there is a conflict between the primary and mirrored NAND flash, then “0” is output because “0” bits are more reliable than “1”s when the dominant error direction is “0” to “1”. Therefore, the bit errors are corrected by ERS. The false decision may happen when both bits of the primary and mirrored NAND are failed from “0” to “1”, but the possibility is low. When ERS is combined with RM, the BER is reduced by 92%.

18.3.3 Techniques Related to Data Preprocessing

Data preprocessing can improve the reliability and the power consumption. Asymmetric coding was proposed in [19] to improve the BER of NAND flash memory. As described in the previous subsection, NAND flash memories exhibit asymmetry in error direction. Asymmetric coding increases the number of “0”s or “1”s in the programming data to compensate the error asymmetry. Suppose a page where “0” to “1” error happens much more frequently than “1” to “0” error; “1” bit is more reliable than “0” bit. For such a page, asymmetric coding increases the number of “1” for higher reliability. The processing flow of the asymmetric coding is shown in Fig. 18.8. The input data is divided into sections which contain *n* bits. To increase the population of “1”s, a section is bit-flipped if the number of “1”s in a section is not more than *n*/2. After that, “1” flag is added to show that the section is bit-flipped. Otherwise, the data are not flipped and “0” flag is added. Increasing the number of “0”s can be manipulated similarly. When *n* is 16, the population of “1”s or “0”s is increased to 60% and the memory overhead by the flag is 6.3% [19]. The

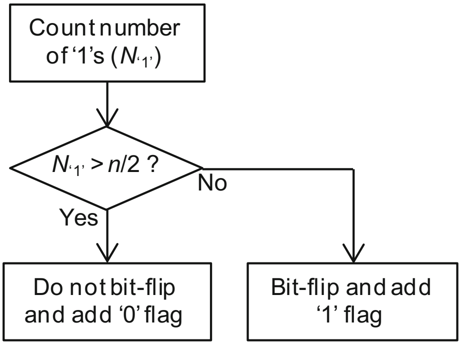

Count number of ‘1’s ($N_{‘1’}$)
$N_{‘1’} > n/2$?
No
Yes
Do not bit-flip and add ‘0’ flag
Bit-flip and add ‘1’ flag

Fig. 18.8 Asymmetric coding [19]

asymmetric coding ($n = 16$) reduces the BER of the NAND flash memory by 90%, compared with the worst case that all cells are programmed into the memory state of the highest threshold voltage.

Stripe pattern elimination algorithm (SPEA) is another data preprocessing technique which can reduce the program peak current (power) [19]. The worst program peak current should be carefully considered not to exceed the power budget, which limits the parallelism of the NAND flash memory. The performance of the storage can be enhanced if the worst-case program peak current is reduced. During programming, charging the bit-line capacitance is the main contribution to the power-supply current. Bit lines are arranged all across the NAND flash chip and the bit-line pitch is the same as the design rule. As a result, the bit-line capacitance will increase during the scaling and the program peak current will accordingly increase. Bit lines are biased to 0 V and V_{DD} when the corresponding memory cell is programmed and program inhibited [20], respectively. As a result, if the memory cells in a page are alternately programmed (stripe pattern, or "0101…" pattern), bit lines are also alternately biased to 0 V and V_{DD}, which causes the maximum peak write current because all of the inter-bit-line capacitance is charged. SPEA rearranges the data in case of a stripe pattern so that the peak write current is reduced. Figure 18.9 shows the flow of SPEA. First, the number of "1"s in the odd and even bits are separately counted ($N_{'1'odd}$ and $N_{'1'even}$). If the difference between $N_{'1'odd}$ and $N_{'1'even}$ is larger than a threshold (N_{TH}), the data are treated as a stripe pattern. If so, data in the odd bits are placed first and then, even bits, followed by "1" flag. Otherwise, data are not modified and "0" flag is added. Measured results in 4X and 3Xnm NAND flash memory show that the peak write current is reduced by 43 and 35% at maximum, respectively. Moreover, if the NAND flash cell is scaled down to 10 nm, the peak current reduction is projected to be 60%.

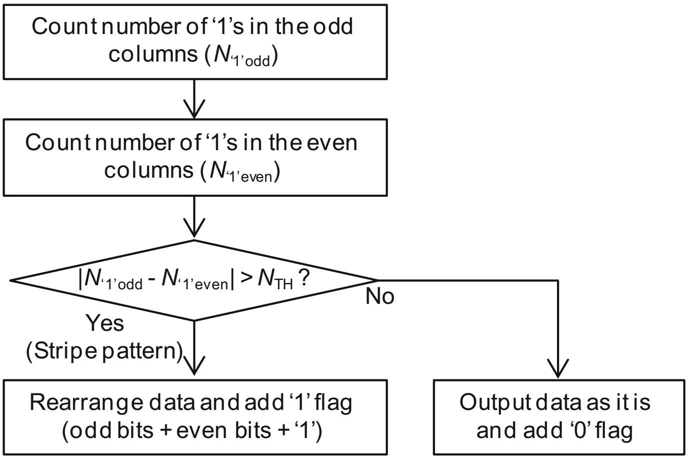

Count number of '1's in the odd columns ($N_{'1'odd}$)
Count number of '1's in the even columns ($N_{'1'even}$)
$|N_{'1'odd} - N_{'1'even}| > N_{TH}$?
Yes
(Stripe pattern)
No
Rearrange data and add '1' flag (odd bits + even bits + '1')
Output data as it is and add '0' flag

Fig. 18.9 Stripe pattern elimination algorithm (SPEA) [19]

18.3.4 Other Techniques

This subsection introduces two techniques which cannot be put into the above classifications: Error recovery (ER) [12] and error masking (EM) [15] schemes. ER scheme applies voltage pulses to the NAND flash cells to reduce the BER. Immediately after programming, the effects of program disturb and cell-to-cell coupling are dominant and the bit errors are basically caused by the increase in the threshold voltage. On the other hand, after data retention, the electrons are ejected or detrapped from the floating gate or the tunneling dielectric and therefore the decrease of the threshold voltage causes the bit errors. Concept of the ER scheme is shown in Fig. 18.10 [12]. *P*rogram *d*isturb error *r*ecovery *p*ulse (PDRP) decreases the bit errors with too high threshold voltage. By making the cell in the program inhibit condition (e.g., Control gate: 18 V and Channel: 8 V), the electrons trapped in between the control gate and the inter-poly dielectric are put out and the threshold voltage decreases. As a result, bit errors due to the program disturb is recovered. On the other hand, *d*ata *r*etention error *r*ecovery *p*ulse (DRRP) increases the threshold voltage of the memory cells to recover data retention errors. The read bias (e.g., Control gate: 3 V and Channel: 0 V) causes weak electric field across the tunneling dielectric. As a result, electrons are injected to the floating gate to compensate the decrease in the threshold voltage during data retention. PDRP reduces the BER by 76% and applying 500 DRRP decreases the BER by 56%.

Once data are written to the NAND flash memory, bit errors basically remain in the same addresses during data retention. During data retention, the threshold voltage of a memory cell continues to decrease. As a result, the bit error is irrecoverable. Error masking (EM) stores the address of the detected bit errors in the other memory such as SCMs [15]. When the NAND flash memory is read, the error recording sequence is executed. The error location which is pointed out by the ECC decoder is stored into the other memory. Each bit of the data corresponds to one bit of the error location vector. If an error is detected, the corresponding bit is changed to "1". Otherwise, the bits are "0". The error location vector is stored in the other

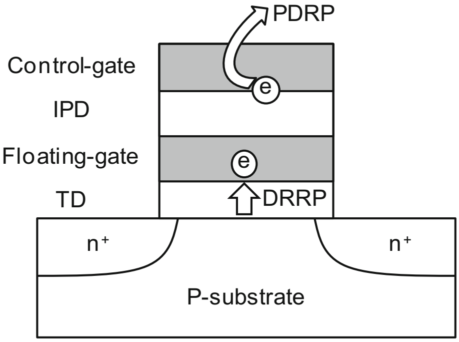


Fig. 18.10 Error recovery (ER) scheme [12]

memory with compression. Run-length encoding is effective for compression because the number of “0”s is significantly larger than that of “1”s. The EM can improve the BER by 66%.

18.4 Summary and Conclusion

Various reliability improvement techniques have been introduced in this chapter to realize dependable nonvolatile memory systems. Table 18.1 summarizes the overhead in NAND flash/SCM, performance, and the acceptable BER (ABER) improvement of the techniques in this chapter. The ABER improvement is calculated by $100/(100 - p)$ when the BER improvement is $p\%$. All of the techniques introduced in this chapter can be either combined or used separately, except that RM and SM are exclusive techniques. The techniques can be selected based on the cost, performance, and reliability, which are required for the application. For example in SD card application, the cost should be minimized and thus, mirroring techniques would not be suitable. On the other hand, in the enterprise storage which already applies mirroring, RM/SM and ERS can be implemented with minimum cost overhead.

Table 18.1 Overhead and reliability improvement by each technique

	Overhead in NAND flash	Overhead in SCM	Performance overhead	ABER improvement
Dynamic codeword Transition ECC [11]	0	0	Seq.: 0 Rand.: X17 at max.	X17
EP-LDPC [12]	0	0	Seq.: 0 Rand.: X6 (cf. Conv. BCH)	X3.7 (Code rate: 2/3)
Page-RAID [15]	0.4% (If a block has 256 pages)	0.04% of NAND flash capacity	1%	X1.45
RM [15]	0	0.04% of NAND flash capacity	1%	X3.2
SM [15]	0	0	0	X2.3
ERS [15]	0	0	0	X12
Asymmetric coding [19]	6.3% (n = 16)	0	0	X10
SPEA [19]	0.05% (2 flags per 512 Byte)	0	0	N/A
Error recovery [12]	0	0	PDRP: X2 DRRP: X500	PDRP: X4.2 DRRP: X2.3
Error masking [15]	0	16% of NAND flash capacity	2.1%	X3

References

1. R. Fackenthal et al., A 16 Gb ReRAM with 200 MB/s write and 1 GB/s read in 27 nm technology, in *IEEE International Solid-State Circuits Conference (ISSCC)* (2014), pp. 338–339
2. S. Kang et al., Performance trade-offs in using NVRAM write buffer for flash memory-based storage devices. IEEE Trans. Comput. **58**(6), 744–758 (2009)
3. J.-H. Yoon et al., Chameleon: a high performance flash/FRAM hybrid solid state disk architecture. IEEE Comput. Archit. Lett. **7**(1), 17–20 (2008)
4. H.-G. Lee, High-performance NAND and PRAM hybrid storage design for consumer electronics. IEEE Trans. Consum. Electron. **56**(1), 112–118 (2010)
5. H. Fujii et al., x11 performance increase, x6.9 endurance enhancement, 93% energy reduction of 3D TSV-integrated hybrid ReRAM/MLC NAND SSDs by data fragmentation suppression, in *IEEE Symposium on VLSI Circuits* (2012), pp. 134–135
6. K. Takeuchi, Novel co-design of NAND flash memory and NAND flash controller circuits for sub-30 nm low-power high-speed solid-state drives (SSD). IEEE J. Solid-State Circuits **44**(4), 1227–1234 (2009); JSSC 1227–1234 (2009)
7. K. Tsuchida et al., A 64 Mb MRAM with clamped-reference and adequate-reference schemes, in *IEEE International Solid-State Circuits Conference (ISSCC)* (2010), pp. 258–259
8. Y. Choi et al., A 20 nm 1.8 V PRAM with 40 MB/s program bandwidth, in *IEEE International Solid-State Circuits Conference (ISSCC)* (2012), pp. 46–47
9. H. Li and Y. Chen, *Nonvolatile Memory Design: Magnetic, Resistive, and Phase Change* (CRC Press, 2011). ISBN: 978-1-4398-0745-3
10. H.-S.P. Wong et al., Metal-oxide RRAM. IEEE Proc. (IEEE) **100**(6), 1951–1970 (2012)
11. S. Tanakamaru et al., Post-manufacturing, 17-times acceptable raw bit error rate enhancement, dynamic codeword transition ECC scheme for highly reliable solid-state drives, SSDs, in *IEEE International Memory Workshop (IMW)* (2010), pp. 88–91
12. S. Tanakamaru et al., Error-prediction LDPC and error-recovery schemes for highly reliable solid-state drives (SSDs). IEEE J. Solid-State Circuits **48**(11), 2920–2933 (2013)
13. N. Mielke et al., Bit error rate in NAND flash memories, in *IEEE International Re-liability Physics Symposium (IRPS)* (2008), pp. 9–19
14. R.-S. Liu et al., DuraCache: a durable SSD cache using MLC NAND flash, in *ACM/EDAC/IEEE Design Automation Conference* (2013)
15. S. Tanakamaru et al., NAND flash memory/ReRAM hybrid unified solid-state-storage architecture. IEEE Trans. Circuits Syst. I **61**(4), 1119–1132 (2014)
16. A. Kawahara et al., Filament scaling forming technique and level-verify-write scheme with endurance over 10^7 cycles in ReRAM, in *IEEE International Solid-State Circuits Conference (ISSCC)* (2013), pp. 220–221
17. K. Higuchi et al., Investigation of verify-programming methods to achieve 10 million cycles for 50 nm HfO_2 ReRAM, in *IEEE International Memory Workshop* (2012), pp. 119–122
18. K.-T. Park et al., A zeroing cell-to-cell interference page architecture with temporary LSB storing and parallel MSB program scheme for MLC NAND flash memories. IEEE J. Solid-State Circuits **43**(4), 919–928 (2008)
19. S. Tanakamaru et al., Highly reliable and low power SSD using asymmetric coding and stripe bitline-pattern elimination programming. IEEE J. Solid-State Circuits **47**(1), 85–96 (2012)
20. K.-D. Suh et al., A 3.3 V 32 Mb NAND flash memory with incremental step pulse programming scheme, in *IEEE International Solid-State Circuits Conference (ISSCC)* (1995), pp. 128–129

Chapter 19
Network-on-Chip Based Multiple-Core Centralized ECUs for Safety-Critical Automotive Applications

Tomohiro Yoneda, Masashi Imai, Hiroshi Saito, Akira Mochizuki, Takahiro Hanyu, Kenji Kise and Yuichi Nakamura

Abstract Current automotive electronic systems contain many ECUs (Electronic Control Units), and many of them play very important roles for safety-critical applications. However, in conventional ECU configurations, each ECU is usually tied to specific functions, and is connected to specific sensors/actuators. Thus, failure of an ECU directly leads to loss of the function related to the ECU. A centralized ECU approach has potential to resolve these issues. In this configuration, since any ECU can access any intelligent sensor/actuator and each function can be executed by any ECU, a faulty ECU no longer results in malfunction of specific functions that are assigned to it. This chapter introduces a dependable NoC (Network-on-Chip) platform that is suitable for a centralized ECU. In this platform, asynchronous design style is used to design on-/off-chip network to handle delay faults or process and other variations. Especially, for achieving the performance compatibility between

T. Yoneda (✉)
National Institute of Informatics, Tokyo, Japan
e-mail: yoneda@nii.ac.jp

M. Imai
Hirosaki University, Hirosaki, Japan
e-mail: miyabi@eit.hirosaki-u.ac.jp

H. Saito
University of Aizu, Aizu Wakamatsu, Japan
e-mail: hiroshis@u-aizu.ac.jp

A. Mochizuki
CIES, Tohoku University, Sendai, Japan
e-mail: pico@ngc.riec.tohoku.ac.jp

T. Hanyu
RICE, Tohoku University, Sendai, Japan
e-mail: hanyu@riec.tohoku.ac.jp

K. Kise
Tokyo Institute of Technology, Tokyo, Japan
e-mail: kise@cs.titech.ac.jp

Y. Nakamura
NEC, Kawasaki, Japan
e-mail: yuichi@az.jp.nec.com

S. Asai (ed.), *VLSI Design and Test for Systems Dependability*,
https://doi.org/10.1007/978-4-431-56594-9_19

on-/off-chip data transmissions, current-mode circuitry is applied. For mitigating router or link faults, a dependable routing algorithm is adopted. Finally, its dependable task execution scheme makes the platform function correctly so long as the capability of surviving processor core faults permits. The outcome of this research project has formed into an evaluation platform that includes a hardware board, a support tool for the dependable task execution scheme, and a functionality of hardware-in-the-loop simulation using a built-in plant model (please refer to Sect. 19.5 for details).

Keywords Centralized ECUs · Asynchronous on/off-chip networks
Dependable routing · Duplex/triple task execution · Evaluation kit

19.1 Introduction

Current automotive electronic systems contain many ECUs (Electronic Control Units), and their functional safety is a very important issue. In conventional ECU configurations, computational power of an ECU for specific functions is not usually utilized for other functions, even when it is possible. For example, an ECU for an antiskid brake system is almost idle in normal situations, and may have a large amount of computational power. But, such an ECU is not designed to perform other functions. Moreover, failure of an ECU directly leads to loss of the function related to the ECU, because each ECU is tied to specific functions and is connected to specific sensors/actuators.

A centralized ECU approach has potential to resolve these issues. Its idea is shown in Fig. 19.1. As shown in this figure, several or many ECUs are implemented on many-core systems, and intelligent sensors/actuators or normal sensors/actuators with small ECUs are directly connected to a network such as CAN, FlexRay, etc. In this configuration, any ECU can access any intelligent sensor/actuator. Thus, each function for specific sensors/actuators can be executed in any ECU, and one ECU can execute multiple functions depending on its load. More importantly, a faulty ECU no longer results in malfunction of specific functions that are assigned to it. This is because those functions can now be executed by another ECU, if the detection and recovery mechanism is implemented properly.

Important issues related to success of this approach are as follows:

1. The requirement of computational power differs among small family-type cars and large luxury cars, and reliability requirement may also be different among them. This requires many different sizes of many-core systems, but their implementation cost should not be high.
2. Automotive companies sometimes have acute demands for the dependability against a chip fault. This means that implementing many cores in a single large chip is not sufficient, but a multiple chip configuration is required.

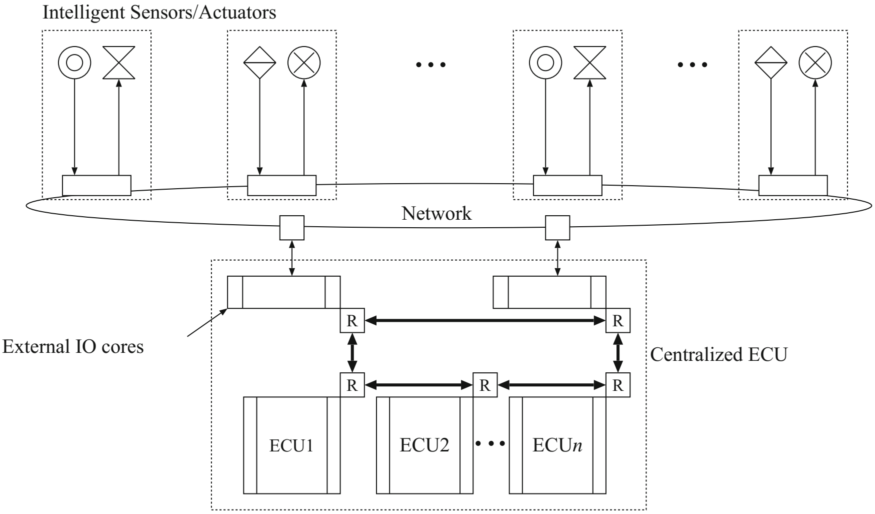


Fig. 19.1 Centralized ECU approach (modified from Fig. 1b in [1])

From these points of view, large MPSoCs (Multiprocessor System-on-Chips) do not seem very appropriate for the centralized ECUs. Some European projects [2, 3] assume NoC (Network-on-Chip) platforms for the centralized ECUs. NoC platforms are nice, because they are scalable and flexible. However, it is not clear if the above issues are being addressed in these projects.

Our solution for this problem is a multi-chip NoC approach [1], where multiple NoCs are connected via off-chip links, and on-chip networks are seamlessly extended to a multi-chip network, such that the node address is uniform within a multi-chip NoC, and there is no difference between on-chip communications and inter-chip communications. Thus, it is easy to obtain suitable configurations for different requirements simply connecting small and inexpensive NoC-based chips.

We have developed a multi-chip NoC-based many-core platform that is suitable for a centralized ECU for the above reasons. In order to satisfy high dependability requirement for safety-critical automotive applications, our platform addresses this dependability issue in the following three different levels:

- Circuit level: The on-chip and inter-chip networks including routers in our platform are implemented fully asynchronously. Since such asynchronous implementation needs no global clocks, it has tolerance against process, temperature, and other variations, and makes it easy to connect many synchronous cores with different clock domains and to form a multi-chip configuration by extending the on-chip network to an inter-chip network. Especially, since the networks use the encoded links, they are also very robust to delay faults.
- Routing level: Each router uses a dependable routing algorithm. Thus, even if single link, router, or chip fault occurs, packets are routed detouring around the

affected network component. Moreover, an online-dependable routing algorithm is used. Thus, the packet re-routing can be done very quickly after the fault detection.
- Task execution level: Each application task is loaded in several processor cores redundantly, and usually two processor cores execute the same task simultaneously using the same inputs. The results of the task are then sent to an external IO core and are compared there. If a mismatch is found, the task is executed again, but using three processor cores, to find the correct results and detect a faulty core. If a faulty core is successfully detected, it is excluded from the system, and tasks are continuously executed on a reconfigured system.

Our platform also provides a support tool for the above task execution scheme such that users only have to prepare a simplex version of application programs in Simulink. Furthermore, a functionality of hardware-in-the-loop simulation using a built-in plant model that is executed by a soft processor core on an FPGA is developed. Currently, a simplified vehicle dynamics plant model is available and can be used freely on our platform.

This chapter introduces some details of our platform and shows some preliminary evaluation results when it is applied to an integrated attitude control system of a four-wheel drive electric vehicle.

19.2 Asynchronous On-chip and Inter-chip Network

It is recommended that readers also refer to Chap. 9, Sect. 9.3 for understanding basic ideas of asynchronous NoCs.

19.2.1 Routers

In our platform, an on-chip and inter-chip networks use a 2D (two-dimensional) mesh topology. This topology is shown in Fig. 19.2. As shown in this figure, each router has five ports, four for communicating with neighboring routers and one for its computational core. The terms *north*, *south*, *east*, and *west* are used to indicate the directions on this topology, that is, the north (south) means the direction where the y value in (x, y) increases (decreases), and the east (west) means the direction where x value in (x, y) increases (decreases).

On this topology, packets are transferred using the *wormhole switching*. A packet consists of several flits, and a flit consists of 32-bit data payload and 2-bit flit header. The flit header indicates the type of flits, i.e., *a head flit*, *a data flit*, and *a tail flit*. The head flit uses a part of the data payload to contain the destination router location. Our router architecture is shown in Fig. 19.3. The encoded links are used in our routers (see Fig. 9.9 of Chap. 9, Sect. 9.3). Thus, the block arrow to an input channel or from an output channel has 68 wires for 32-bit data with 2-bit flit header. The thin arrow

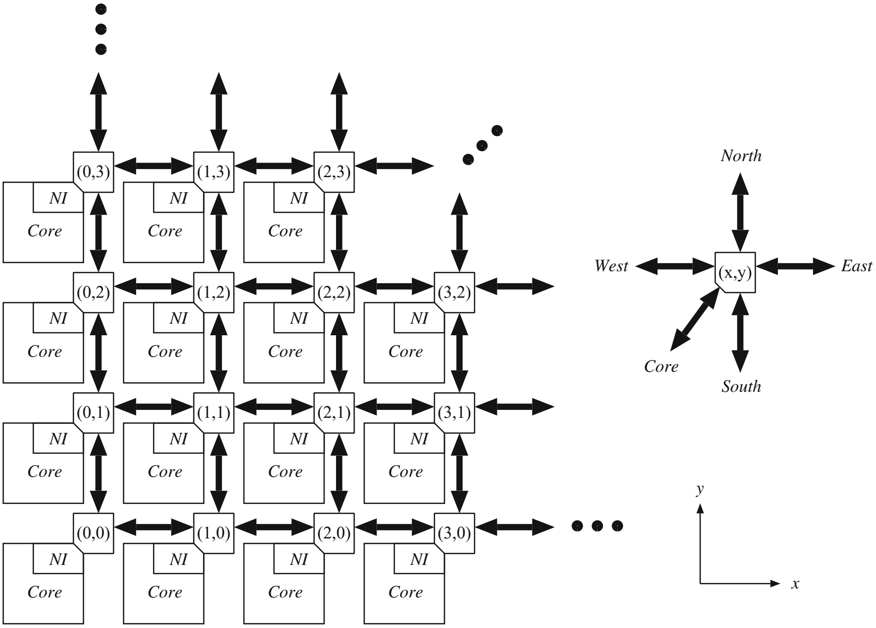


Fig. 19.2 Network topology

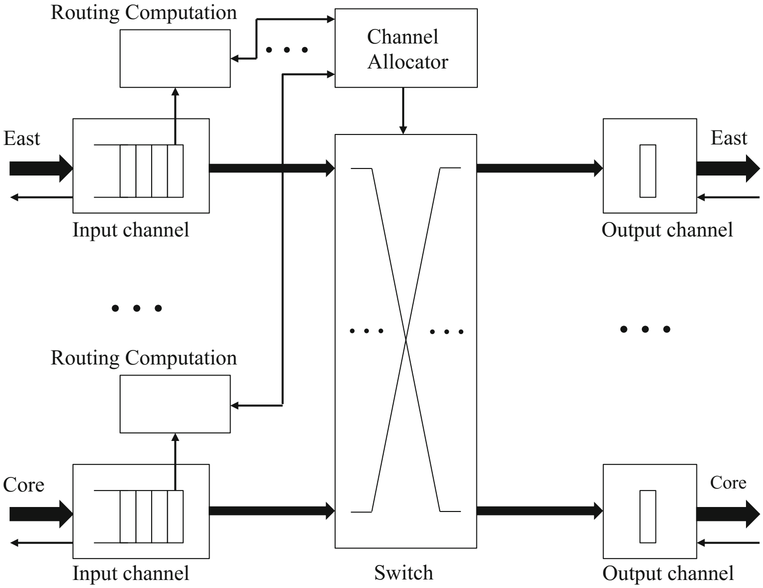


Fig. 19.3 Router architecture

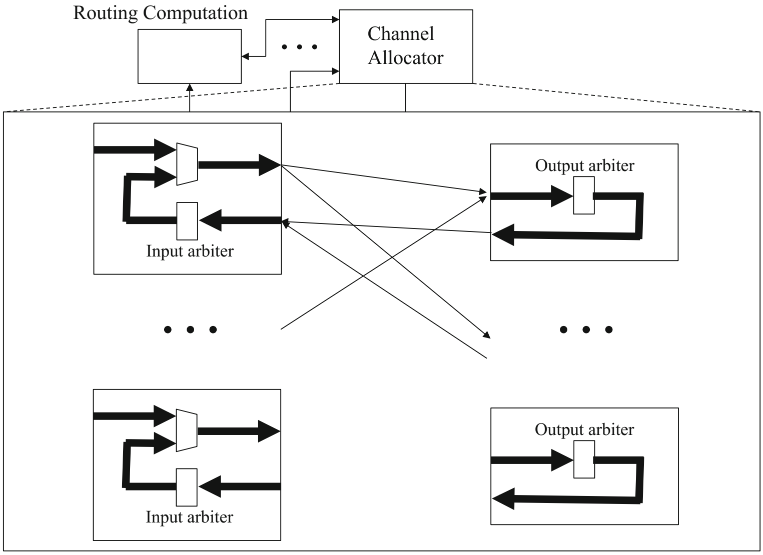


Fig. 19.4 Arbitrations in Channel Allocator

from an input channel or to an output channel represents a 1-bit acknowledgment signal. A code detector is placed at the front of each input channel, and an encoding circuit with a DFF is used at the end of each output channel. The queues or input buffers in the input channels are implemented using *MOUSETRAP* pipelines with 34-bit data path. No encoding is used inside a router, and thus, its data path is 34 bits, which is represented by thinner block arrows in Fig. 19.3.

The routing computation unit performs the dependable routing algorithm shown later in Sect. 19.3. The channel allocator establishes paths on the crossbar switch from input channels to output channels and controls the flow of flits. For example, Fig. 19.4 shows how arbitrations are done for obtaining an output channel. Since our dependable routing algorithm is based on *an adaptive routing*, each packet tries to find one or more routes at each router in order to avoid congested routes. For implementing this idea, the channel allocator has an output arbiter for each output channel and an input arbiter for each input channel. When a head flit arrives at an input channel, the channel allocator sends requests to several output arbiters according to the result of the routing computation. The similar actions are taken for other head flits in different input channels. Thus, each output arbiter may receive several requests from different input channels. One of such requests is chosen by an output arbiter, and the corresponding grant is sent to the input channel side. In the input channel side, since several grants may be obtained, one of them is chosen by an input arbiter, and the requests for other output channels are withdrawn. Then, a route from this input channel to the corresponding output channel is established, and the flits are actually transferred through the data path.

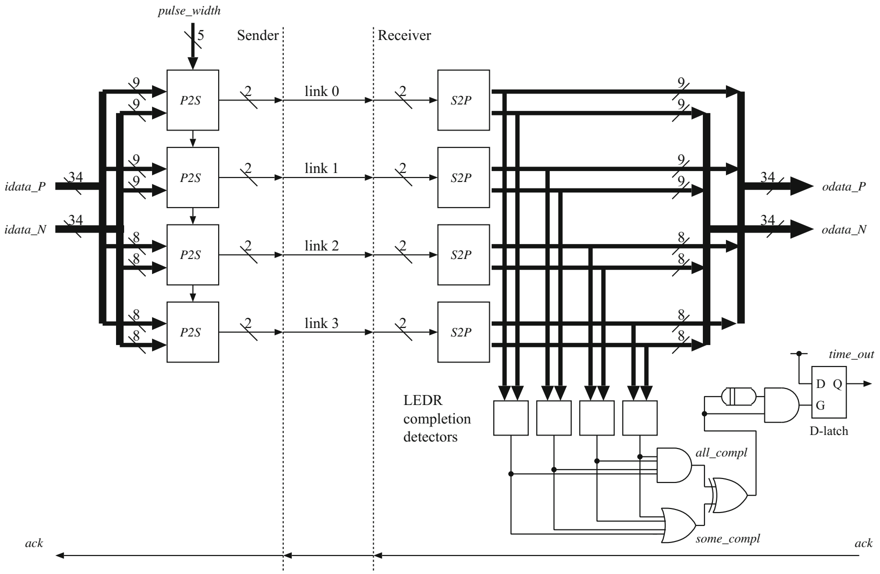


Fig. 19.5 Off-chip communication mechanism (from Fig. 6 in [1])

19.2.2 *Off-chip Connections*

Since the bit width of the off-chip links is too small for on-chip links due to the limited number of pins of IC packages, some parallel-to-serial (*P2S*) and serial-to-parallel (*S2P*) conversion mechanisms are used.

Figure 19.5 shows the architecture of our off-chip communication mechanism. The current implementation uses four serial *LEDR (Level Encoded Dual-Rail)* [4] communication links, considering the trade-off between the performance and the pin-number limitation, but the number of the serial links can be easily adjusted. The *P2S* module generates nine consecutive codewords of 1-bit LEDR encoding for a given 9-bit LEDR codeword. The lower two *P2S* modules have only 8-bit LEDR inputs, but dummy signals are inserted in order to use the same design of the *P2S* module. The pulse width for this serialization should be carefully selected such that the pulses are wide enough to be propagated to the receiver side against the PCB wire capacitance. Thus, our implementation uses programmable delay elements and the *pulse_width* bits to the *P2S* module decide their delay values. The *S2P* module gathers the serialized data and reconstructs the original 9-bit LEDR codeword. The *ack* signal of the receiver side is directly forwarded to the sender side. This means that the serialized LEDR codewords are not acknowledged one by one. Instead, the acknowledgment is done for each whole original 34-bit LEDR codeword. This choice is made in order to reduce the overhead of the acknowledgment for each serialized codeword. The waveforms of relevant signals are shown in Fig. 19.6.

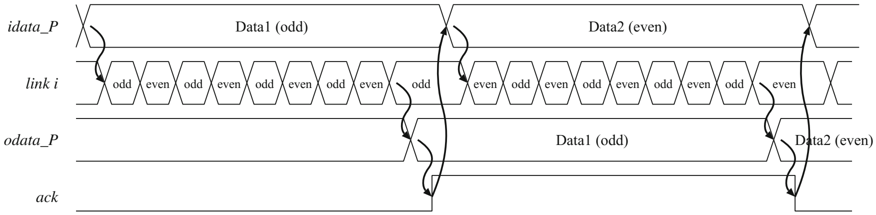


Fig. 19.6 Waveforms of relevant signals in the off-chip communication mechanism (from Fig. 7 in [1])

In order to detect permanent link failures, a link time-out detection mechanism, which is shown in the lower part of Fig. 19.5, is implemented. This link time-out detection mechanism watches the completion detection timings of four LEDR encoded serial links. Their time differences are usually very small. Thus, *some_compl* and *all_compl* are asserted almost at the same time. However, if a failure occurs in a link, and one of the completion detectors does not indicate the completion, *some_compl* goes high, but *all_compl* does not in odd cycles, and in even cycles, *all_compl* goes low, but *some_compl* does not. Thus, the EXOR gate produces a pulse long enough to set the time-out FF. Note that this method uses the time differences of the completion of each serial link, and thus, it does not depend on the flit transmission time over the links. Hence, small time-out value can be used, which makes it possible to detect link failures very quickly.

19.2.3 Design of a Current-Mode Interface

In this subsection, we describe an energy-efficient off-chip data transmission interface based on current-mode circuitry. In the partially serialized data transmission provided in the previous subsection, it is necessary to utilize parallel-to-serial (P2S) converters at a sender and serial-to-parallel (S2P) converters at a receiver, because the number of I/O pins for the off-chip data transmission is limited. In order to perform high-speed and energy-efficient data transmission, a current-mode circuit style with dynamic current feedback mechanism is used in the I/O interface between P2S and S2P [5]. On the off-chip link wire, both high current drivability during data transition and a small voltage-signal swing of basic switching gates are obtained in our current-mode circuit, because of monitoring the voltage level on the link wire and of supplying an adequate feedback into current signals. In fact, high-speed switching with relatively small steady current flow is achieved in comparison with that of conventional current-mode interfaces such as current-mode logic (CML) and low-voltage differential signaling (LVDS) styles. Moreover, the use of a power-gating method to cut off the steady current flow makes it possible to greatly reduce the power dissipation of our I/O interface, since the off-chip data transmission is

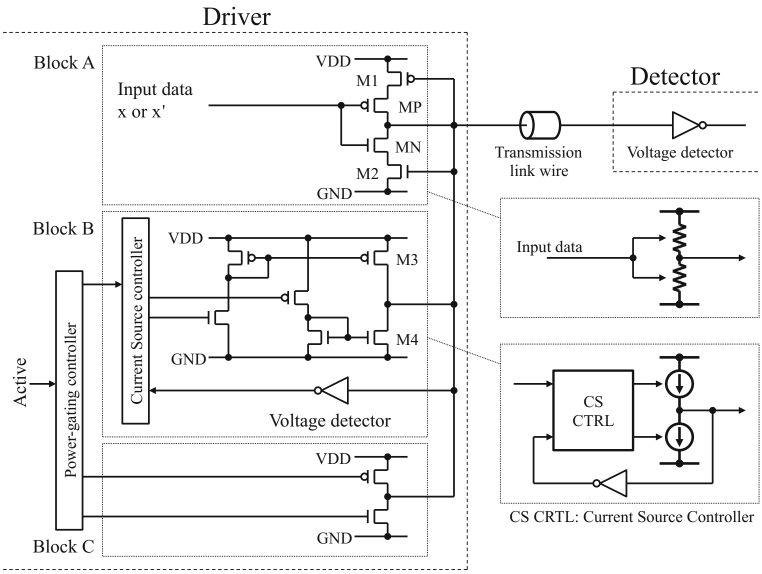


Fig. 19.7 Circuit diagram of the proposed I/O interface

supposed to be activated, for example, at every 10 ms intervals on average in our typical automotive applications.

The circuit diagram of the off-chip current-mode I/O interface is depicted in Fig. 19.7. At the sender, the driver is located between the P2S converter and the output I/O pad. At the receiver, the detector is located between the input I/O pad and the S2P converter. The driver contains Blocks A, B, and C. Block A is designed by complementary variable resistors. Block B is designed by switched current sources. Block C is implemented by a three-state buffer to set VDD or GND when the mode is inactive. The input data comes from the P2S converter. The power-gating control signal "Active" is generated in the router.

Block A acts as an accelerator for beginning of a signal transition part and variable resistances to determine the stable voltage level. Block B acts as switched current sources to determine the stable voltage level and their current levels are to be small. Block C reduces the release time from the standby mode. The detector at the receiver is designed by a voltage detector which is an inverter. It amplifies a small voltage swing signal on the link wire into a full swing signal.

Figure 19.8 shows the behavior of Blocks A and B using an equivalent circuit diagram. The fall and rise transitions are indicated as shown in Fig. 19.8a, b, respectively. Blocks B and A are expressed by two switched current sources and two variable resistors. Before the transition, the high (low) voltage level on the link wire is determined by the weak charge (discharge) current at the resistor M1 (M2) and the medium discharge (charge) current at the current source M4 (M3) as shown in Fig. 19.8a. The initial voltage level is 0.8 V (0.4 V) under the supply voltage "VDD"

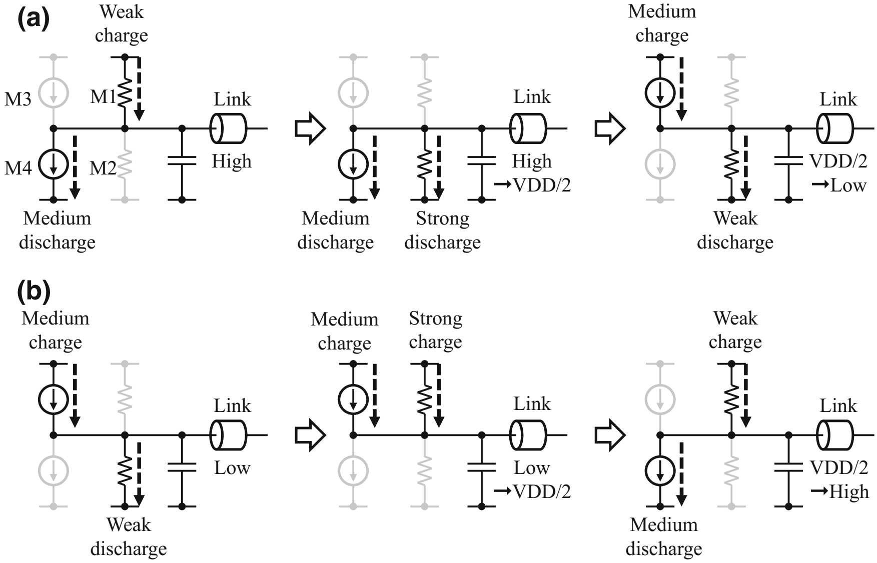


Fig. 19.8 Behavior of the I/O interface: **a** transition from high to low, and **b** transition from low to high

of 1.2 V. The ground "GND" level is 0 V. When input signal turns from VDD to GND (from GND to VDD), the activated resistor is switched from M1 to M2 (from M2 to M1) by the MP/MN inverter and the strong discharge (charge) current flows due to the variable resistance to set by the voltage level at the link wire. Hence, large current through M2 and M4 (M1 and M3) accelerates the transition at the link wire. After the voltage level on the link wire is reached to VDD/2, M4 (M3) is turned OFF and M3 (M4) is turned ON by the feedback signal of the voltage detector in Block B. The discharge (charge) speed is getting down and the transition power can be saved. Even though the transition speed is slow, the voltage level on the link wire is already smaller (larger) than VDD/2 and the logical value change is also already noticed at the receiver. As a result, high-speed switching and power saving are obtained simultaneously, because the fast transition time part and power-saving time part are separated using this dynamic current feedback mechanism. In the standby mode with no data transmission, there is no steady current flow by turning off the current sources in Block B. When standby mode is released, Block B restores the voltage level of the link wire and Block C accelerates the restoration by supplying charging and discharging currents which drive VDD/2.

Figure 19.9 shows simulated waveforms of the off-chip I/O interface and on a 10 mm link wire under the best-case process condition at a supply voltage of 1.2 V and a temperature of 25 °C using a 130 nm CMOS bulk process. This result includes the P2S converters at the sender and the S2P converters at the receiver where the bit width of data is 35, the number of I/O pins is 16. The dual-rail signals, (idata,

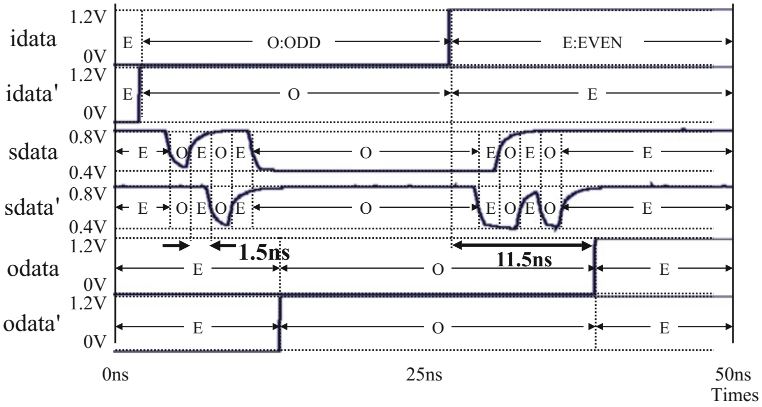


Fig. 19.9 Simulated waveforms of the I/O interface and on the link wires

idata′) and (odata, odata′), indicate the LSB input signal pair of the P2S converter at the sender and the LSB output signal pair of the S2P converters in the receiver. The serialized dual-rail signals (sdata, sdata′) indicate the LSB-side five-bit data on the link wire where the voltage swing is 0.4 V. The average cycle time of the five-bit serial data transmission is 1.5 ns and the average total time of the 35-bit data transmission is 11.5 ns.

Using multiple-valued current-mode circuitry, quaternary data of the LEDR dual-rail lines and ternary data of the 4-phase dual-rail lines can be superimposed into a link wire [6, 7].

19.3 Dependable Routing Algorithm

The asynchronous NoC platform mentioned in the previous section is suitable for a many-core system on which a centralized ECU is implemented, because it is scalable and flexible. However, if a fault occurs in a network component, such as a router or a link, many computational cores that are working correctly may be affected severely, depending on routing algorithm used. For example, consider a case where router (1, 1) goes faulty on a 4 × 4 2D mesh network. If a *dimension-order routing* algorithm [8], one of very popular routing algorithms for a 2D topology, is used, packets are sent first in the x-dimension and then in the y-dimension to reach the destination router. Thus, every packet sent to router (x, y) with $1 \leq x \leq 3, 0 \leq y \leq 3$, $(x, y) \neq (1, 1)$ from a computational core connected to router (0, 1) is affected as shown in Fig. 19.10, because such a packet always goes through a faulty router (1, 1). In this case, totally 17% of working computational pairs are affected. This is, of course, not a desirable situation. This section mentions a dependable routing

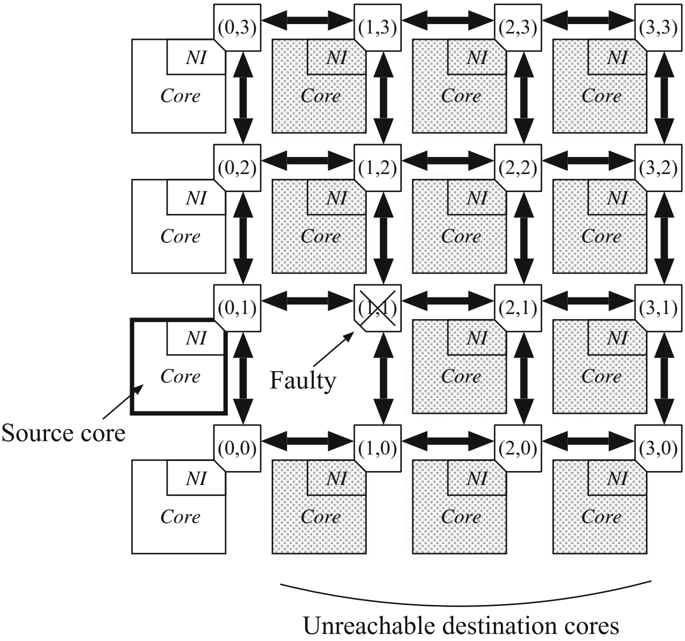


Fig. 19.10 Influence by faulty router (1, 1)

algorithm that reduces this number to 0% and is very important to construct our dependable NoC platform.

The following are assumed or required in the network of our platform.

1. Either one router or one link goes faulty. Furthermore, such a faulty component is certainly identified by every router that is connected to it.
2. If a fault occurs at a time when a packet is just going through the network component, it is acceptable that the exact packet is lost. This packet loss is handled in a higher layer of protocol. However, the number of the affected packets should be small. Thus, the detour path selection should be done as soon as possible.
3. The routing algorithm should be implemented with a simple hardware in order to reduce the performance overhead of routers.
4. Deadlock due to detouring around faulty components should be avoided.

The above requirements 2 and 3 are needed for maintaining the real-time properties of automotive applications.

19.3.1 Basic Idea

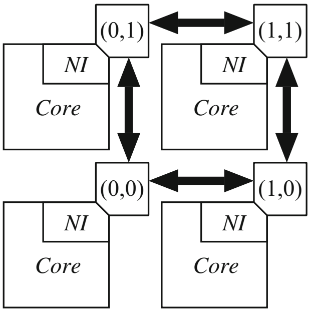
From the above requirements, off-line dependable routing algorithms such as [9] are not so suitable for our platform, mainly because they use complicated off-line processes to gather fault information. Thus, online dependable routing algorithms are preferred, although they can tolerate less faults than the off-line algorithms. As for deadlock avoidance, many methods (e.g., [10, 11]) are based on virtual channels. Generally, they have better performance than the algorithms without virtual channels, but their implementation is more complicated. Again from the above requirement 3, we have chosen an algorithm that uses no virtual channels for deadlock avoidance.

The algorithm proposed in [12] satisfies these two properties, that is, it is an online algorithm and needs no virtual channels. Our routing algorithm is obtained by modifying it. Its main idea to avoid deadlocks is *turn model*. A deadlock happens when packets try to occupy output channels in a circular manner. The following is one example (see also Fig. 19.11):

- Packet *A* occupies the north output channel of router (0, 0) and waits for the east output channel of router (0, 1).
- Packet *B* occupies the east output channel of router (0, 1) and waits for the south output channel of router (1, 1).
- Packet *C* occupies the south output channel of router (1, 1) and waits for the west output channel of router (1, 0).
- Packet *D* occupies the west output channel of router (1, 0) and waits for the north output channel of router (0, 0).

In this case, if one of the above four turns is disallowed, then this deadlock situation never happens. Since the reverse case should also be considered, [12] disallows two turns, east–south turn, and northwest turn. This means that packets cannot go to the negative directions (i.e., the direction where x-coordinate or y-coordinate decreases, which is west or south) after going to the positive directions (i.e., east or north). Thus, this method is also called *negative-first* routing algorithm.

Fig. 19.11 Routers considered for a deadlock example



Under this constraint, it is possible to design an adaptive routing algorithm. Actually, the routing computation algorithm shown below chooses two or less directions (i.e., a set *can* below). Then, an output channel connected to a faulty component is dropped from this set, and the requests are sent to the output arbiters of the remaining output channels, as shown in Fig. 19.4. This is a basic idea for detouring around the faulty component.

When a packet with a destination router *des* arrives at a router *cur*, a candidate output channel set $can \subset \{north, south, east, west, core\}$ is computed as follows.

1. If ($des = cur$), $can \leftarrow \{core\}$.
2. If *des* is a neighbor of *cur*, $can \leftarrow \{out\}$, where $out \in \{north, south, east, west, core\}$ is the output channel direction that is connected to *des*.
3. If *des* is located to the south, east, or southeast of *cur*,

   a. $can \leftarrow \{south\}$, if the south channel is connected to a non-faulty component, and
   b. $can \leftarrow \{west\}$, otherwise.

   Since the negative moves cannot be taken after the positive moves, the negative moves should be taken sufficiently enough until *des* comes to the northeast and can be reached only by positive moves. In a case where *des* is to the east, once a packet is sent to the east, which are positive moves, it cannot come back from the detour route using negative moves. Thus, another negative move is needed. Note that this is not a minimal route. If a faulty element is encountered when going to the south, the detour route to the west is possible, because it is also a negative move. Note that a special case that *cur* is on the negative edge, where no west routers exist, is not considered here. See below.
4. If *des* is located to the west, north, or northwest of *cur*,

   a. $can \leftarrow \{west\}$, if the west channel is connected to a non-faulty component, and
   b. $can \leftarrow \{south\}$, otherwise.

   This can be explained similarly to the above.
5. If *des* is located to the southwest of *cur*, $can \leftarrow \{south, west\}$. Since this destination can be reached only by negative moves, no restrictions are needed.
6. Let des' denote a location, where (x_d, y_d) and (x'_d, y'_d) are the coordinates of *des* and des' with $(y'_d = y_d - 1)$ and $(x'_d = x_d - 1)$. If $des' = cur$, $can \leftarrow \{north, east\}$. This seems reasonable, because the destination is located to the northeast. However, this should be implemented carefully. For example, after going th the north, if the east link is faulty, there is no detour route. Thus, such link fault information should be forwarded to the current router. The details are shown in Sect. 19.3.2.
7. If des' is located to the east of *cur*,

   a. $can \leftarrow \{east\}$, if the east channel is connected to a non-faulty component, and
   b. $can \leftarrow \{north\}$, otherwise.

When a faulty element is encountered during east moves, the detour route to the north is possible. This is because that moves as well as the remaining moves up to the destinations are all positive moves. The reason that *des*′ is headed instead of *des* is that in a case that a packet is reached to the y-coordinate of *des*, any detour route needs the negative moves, which is not allowed. If *des*′ is headed, the detour route to the north is possible at the location where a faulty component is encountered, and after the location, there should be no more faulty components from our single-fault assumption (see the assumption 1 on p. 12).

8. If *des*′ is located to the north of *cur*,

   a. *can* ← {*north*}, if the north channel is connected to a non-faulty component, and
   b. *can* ← {*east*}, otherwise.

   This can be explained similarly to the above.
9. If *des*′ is located to the northeast of *cur*, *can* ← {*north, east*}. Since this destination can be reached only by positive moves, no restrictions are needed.

There are four remaining special cases as follows.

10. If the x-coordinates of *des* and *cur* are 0, and *des* is located to the south of *cur*,

    a. *can* ← {*south*}, if the south channel is connected to a non-faulty component,
    b. *can* ← {*east*}, otherwise. After this detour move, *can* ← {*south*}.

    This corresponds to the above 3, but the detour route is obtained by the move to the east, instead of west, because there exists no router in the west side. The two moves for the detour route are special, and the normal algorithm above is used after them. Although this actually includes a disallowed turn, this is acceptable from the consideration that the circular form for the occupied output channels cannot be established due to the edge.
11. If the y-coordinates of *des* and *cur* are 0, and *des* is located to the west of *cur*,

    a. *can* ← {*west*}, if the west channel is connected to a non-faulty component,
    b. *can* ← {*north*}, otherwise. After this detour move, *can* ← {*west*}.

    This can be explained similarly to the above.
12. If the x-coordinates of *des* and *cur* are 0, and *des* is located to the north of *cur*,

    a. *can* ← {*north*}, if the north channel is connected to a non-faulty component, and
    b. *can* ← {*east*}, otherwise. After this detour move, *can* ← {*north*} twice.

    This corresponds to the above four, but the detour route is obtained by the move to the east, instead of west, because there exists no router in the west side. In this case, these detour moves are not disallowed. However, after these detour moves, the above four is applied, and this move causes a disallowed turn. Again, this is acceptable due to the edge.

13. If the x-coordinates of *des* and *cur* are 0, and *des* is located to the east of *cur*,

    a. *can* ← {*east*}, if the east channel is connected to a non-faulty component, and
    b. *can* ← {*north*}, otherwise. After this detour move, *can* ← {*east*} twice.

    This can be explained similarly to the above.

19.3.2 Fault Information Propagation

The above dependable routing algorithm assumes fault indications from the neighboring routers or links. It has the following inefficiency.

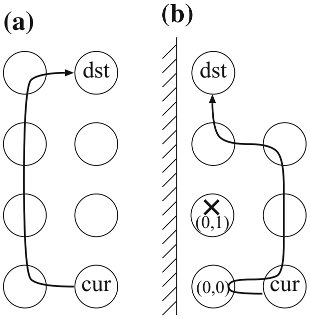
- Even when no faulty elements exist, several redundant routes are chosen for positive moves. One example is shown in Fig. 19.12a, where going directly to the north is disallowed from above item 4.
- When a faulty element exists, more redundant routes are chosen according to the special handling at negative edges. One example is shown in Fig. 19.12b. In this example, the current router does not know the fault to its northwest, and thus, sends packets to (0, 0). However, (0, 0) has to send them back to (1, 0) in order to detour around the faulty router (0, 1) according to above item 12.
- In order to handle the case mentioned in above item 6, the fault indications only from the neighbors are insufficient.

For addressing these issues, our method [13] extends the propagation of the fault information and modifies the routing algorithm accordingly.

Figure 19.13 shows this new fault propagation mechanism. LFD (Link Fault Detector) is a fault detector of the corresponding input link, which is assumed in the original idea. For example, WF (West Failure) is connected to the LFD output (oWF) of the west neighbor router, and works as the fault indication signal from it.

The first extension is to forward the fault information from north to south in order to avoid the redundant paths as shown in Fig. 19.12a. This is implemented by a signal

Fig. 19.12 Drawbacks in a simple implementation (modified from Fig. 3 in [13])



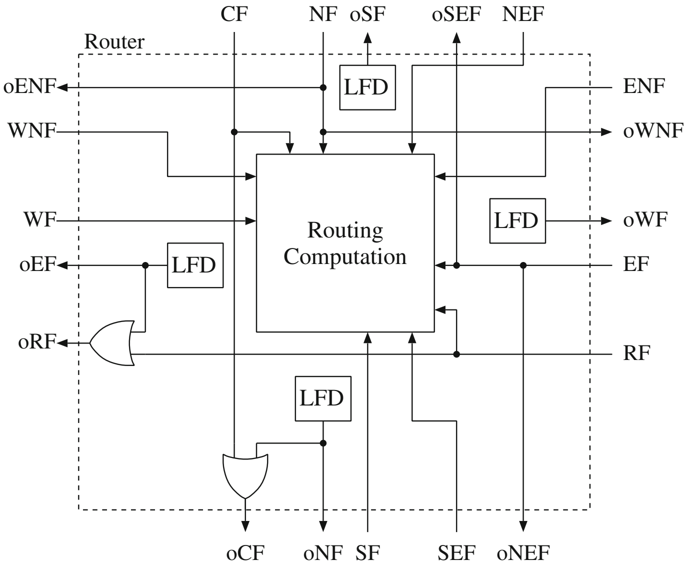


Fig. 19.13 Fault propagation mechanism (from Fig. 4 in [13])

CF (Column Failure), which is connected to oCF of the north neighbor router, where oCF is produced by taking OR of an incoming CF and its LFD. The routing algorithm can be modified such that packets are routed directly to the north in the case of Fig. 19.12a, once it is confirmed using the CF that there are no faulty elements in the north of the line. Note that this algorithm is conservative, because faulty elements under the destination and over the destination cannot be distinguished. But, it is always safe.

The similar forwarding is used in the row direction, which is RF (Row Failure). Note that the forwarding signals from south to north or west to east are not needed, because the redundant paths as shown in Fig. 19.12a are not taken for such directions.

The second extension is a forward signal from northwest neighbor to enable the current router to detect faulty elements in the case of Fig. 19.12b. This is implemented by a signal WNF (West side NF), which is obtained by just forwarding the NF signal of the west neighbor. The routing algorithm is modified such that packets are routed to the north direction in the special situation where the current router is at $(1, y)$, and the destination router is located to the north at the west edge (i.e., $(0, y')$ with $y' > y$) with WNF = 1. Note that such a positive move is allowed only when a faulty router exists at the position shown in the figure. Thus, the detection by the WNF signal is indispensable. SEF (South side EF) is also used for handling the similar situation with respect to the south negative edge.

Finally, in order to detect a fault in the west input link or the south input link of the destination router, forward signals similar to the above are used. ENF (East side NF) and NEF (North side EF) are those signals. By observing those signals, the southwest neighbor of the destination router can correctly route the packets.

19.3.3 Fault Handling Mechanism

The link time-out detection mechanism shown in Fig. 19.5 is used to indicate to the sender router that the corresponding outgoing link is faulty. Although not implemented in the current base chip, a router or on-chip link fault can also be detected using various standard fault detection mechanisms such as error detecting codes, self-checking techniques, and packet-level time-out detection. The sender router uses this information to try to detour around this faulty element using the dependable routing algorithm. One important issue here is how to handle the affected packets. In the wormhole routing, a head flit occupies the channels when it is routed, and the corresponding tail flit releases those channels when it goes through. If a router or link failure happens just after a head flit goes through it, the head flit will reach the destination router eventually as usual, but the following flits stop before the faulty element. As a result, a series of channels on the path that the head flit occupied have been blocked forever. Hence, such a blocked path should be released when the faulty element is detected.

In order to manage this issue, the following modifications have been made on the original design. When a fault occurrence is recognized at the receiver side by *LFD*, *gen_tail* signal is generated as shown in Fig. 19.14a, if a packet is really going through this router. This condition can be checked by *packet_flying*, which is set when a head flit is detected, and reset when a tail flit is detected. When *gen_tail* is asserted, a pseudo tail flit and its request signal are sent to the first stage of the MOUSETRAP FIFO. Figure 19.14b shows how the first stage of the MOUSETRAP FIFO is modified. As a result, a pseudo tail flit is generated at this router and sent to the destination router releasing the occupied channels along the path. If some specific data pattern is defined for this pseudo tail flit, the computational core at the destination router can recognize that this packet is affected by a failure. Anyway, it is unavoidable that some packets flying on the failure element may be lost. Some retransmission procedure should be performed in a higher layer of the communication protocol (i.e., software level).

Figure 19.15 shows how the router output unit is modified in order to handle the remaining flits blocked before the faulty element. When this output unit is notified of a fault occurrence by *LFD* signal, it causes the transparent latch to be kept open, regardless of *ack*. As a result, *internal_ack* is instantly generated when *internal_req*

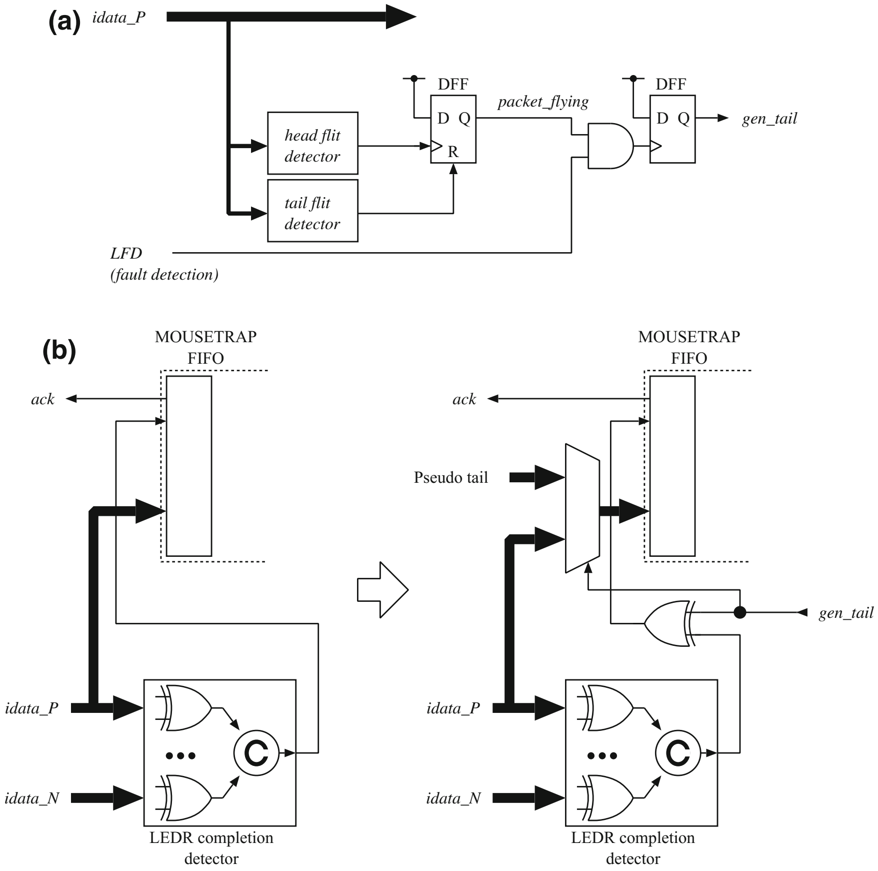


Fig. 19.14 Fault handling mechanism at a receiver side (from Fig. 8 in [1])

is given, and thus, incoming flits are immediately accepted and acknowledged. This means that those flits are thrown away, and the channels occupied by those flits are eventually released. Note that the following incoming packets are detoured around the faulty element by the dependable routing, and thus, this output unit connected to the faulty element is never used for those packets.

The above mechanism is very important to maintain the real-time properties of automotive applications. Note that this kind of timely error handling is not easy in off-line dependable routing algorithms.

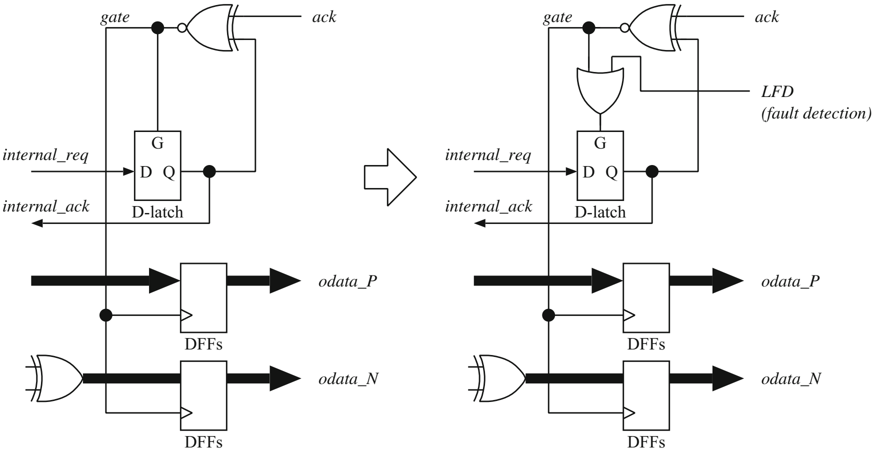


Fig. 19.15 Fault handling mechanism at a sender side (from Fig. 9 in [1])

19.4 Dependable Task Execution

19.4.1 Scheme

Since there are many processor (or computational) cores available in our platform, we utilize them for both the performance and dependability improvement. It is assumed that the application programs are described in Simulink without considering anything about redundant task execution. One consideration required in writing Simulink programs is that the granularity of tasks should be defined properly. As shown later, a task is a basic unit that is executed redundantly and the correctness of the results is guaranteed. Thus, if small and many tasks are defined, the overhead for the dependability becomes large. On the other hand, a task is executed sequentially in one processor. Thus, it is desired that concurrent codes are stored in different tasks. This process may be (semi) automated, but currently, we rely on the programmers. Defining tasks is actually done by defining the corresponding Simulink subsystems as *atomic*.

Then, our support tool automatically extracts the data flow relation from the Simulink programs, and allocate those tasks to the available processor cores redundantly, based on the idea shown in [14]. That is, if the redundancy is given as r, r copies of each task are statically loaded to the processor cores. Our dependable task execution scheme based on [15] (see also Chap. 12, Sect. 12.5) uses these redundantly allocated tasks in order to perform duplex task execution, triple task execution, and dynamic task-pair reconfiguration. Its goal is to keep the application functioning correctly, even if several processor cores go down one by one.

In the dependable task execution scheme, the copies of each task are classified as *active*, *standby*, or *inactive*. For each task, there should exist at least two active copies

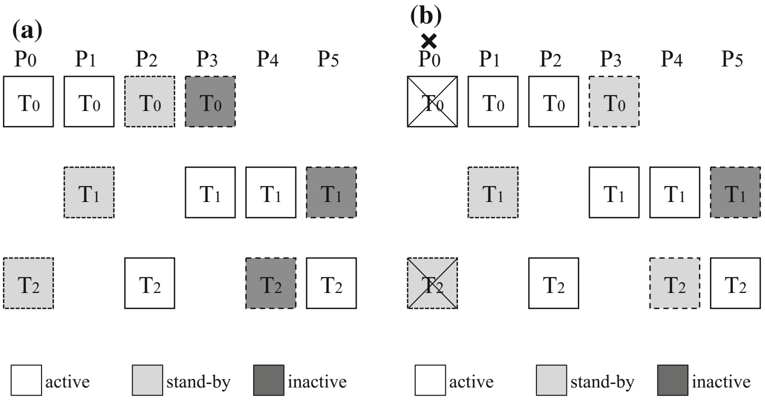


Fig. 19.16 Task allocation and reconfiguration (from Fig. 5 in [16])

and one standby copy. The remaining ones, if they exist, should be inactive. These copies are stored in different processor cores. Usually, only active copies are actually executed by processor cores. Standby copies are executed only when mismatch is found in the results of the active copies. Inactive copies are never executed, but they are candidates for standby copies. One example of this task allocation is shown in Fig. 19.16a. In this example, there are six available processor cores $P_0 \dots P_5$, and three tasks $T_0 \dots T_2$ are used with redundancy $r = 4$. The active copies of T_0 are stored in P_0 and P_1, and its standby and inactive copies are stored in P_2 and P_3, respectively. Each processor core has two copies of different tasks, for example, P_0 has T_0's active copy and T_2's standby copy.

Our scheme uses one or two *external IO core(s)*. The external IO core sends data needed for the task execution to the processor cores that store the corresponding copies of tasks. When a processor core receives data for task execution, they are stored in the appropriate input variables of the task copy. A processor core executes an active copy of a task, if all of its input variables are ready. If there are several such executable active copies, they are executed sequentially. The task execution updates its state variables and output variables. Then, both the state and output variables, i.e., results, are sent to the external IO core, where the results of two active copies are compared. If they match, the data in the output variables are used to prepare the input data for other tasks. Otherwise, in order to obtain the correct data and identify the faulty processor cores, the task is executed again by its standby copy as well as the active copies. This time, the external IO core receives three results, which are used for the majority voting. If a faulty processor core is identified, the system is reconfigured to exclude it. In this process, if an active (standby) copy is stored in the faulty processor core, the corresponding standby (inactive) copy becomes active (standby). Furthermore, if a standby copy becomes active, the corresponding inactive copy becomes standby. One example where P_0 becomes faulty is shown in Fig. 19.16b.

A key issue in this scheme is that the state variables in standby copies should be always updated in order that they can join the triple execution mode whenever required. For this purpose, the external IO core sends the data in the state variables to the corresponding standby copies, when the comparison succeeds. In the processor cores that contain standby copies, they just store the received data into the appropriate state variables of the standby copies. When the triple execution mode is actually performed, the standby copies can perform the re-execution correctly using these state variables. On the other hand, another care is needed with respect to the state variables in the active copies. They are always updated by executing the task codes, and thus, when the active copies are required to be re-executed, those state variables have already been updated, and they may be no longer the same as the ones used for the first execution. Therefore, in our scheme, the usual active copy execution begins with copying the current state variables to some backup area. When the triple execution is required, the state variables are first rolled back from the backup area, and then task copies are actually executed using the same input variables. One miner issue is that the standby copy also needs the input data. It is possible for the external IO core to send it to the standby copy with the triple execution request. In order to simply implement the external IO core, however, the external IO core currently sends the input data to both the active copies and the standby copy together.

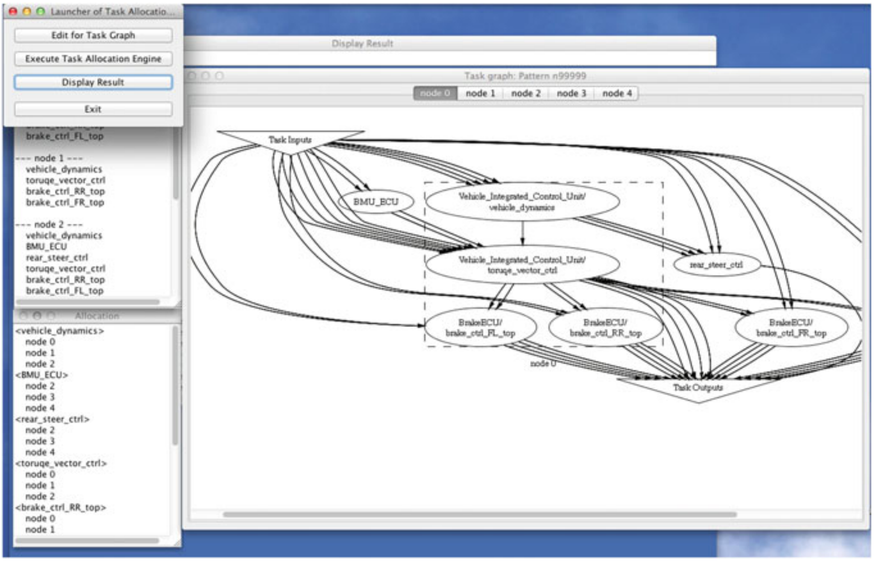
The reason that the triple execution mode is not ordinarily used is to save power dissipation and utilize available processor performance efficiently.

In order to efficiently detect a faulty processor that produces no outputs, “I’m alive” (IA) message is used. That is, each processor core sends the IA message to the external IO cores periodically, and the external IO core marks a processor core as faulty, if the IA message is not sent from the processor core within some time period. This prevents the external IO core from waiting unnecessarily for the data from the stopped processor core in the result comparison process.

Considering the reliability of the external IO core, it is actually duplicated.

19.4.2 Support Tools

Our support tools consist of a front-end GUI, a redundant task allocation engine, and back-end scripts. The front-end GUI shows a task graph that is obtained from a given Simulink program. As mentioned in the previous subsection, a Simulink subsystem that is defined as *atomic* is assumed to be a task, and the data flow relation between tasks is shown. A user can adjust the granularity of tasks observing such a task graph. The information needed for the redundant task allocation, such as estimated task execution times, task sizes, and so on as well as the NoC size and task redundancy r, can also be given through the GUI. Then, a user can launch the redundant task allocation engine. The allocation results are also shown using the front-end GUI (Fig. 19.17). The C codes for the corresponding tasks are generated with Simulink embedded coder. The back-end scripts add a wrapper to each task code, where the wrapper handles the packet communication and manages the various processes for



```
  brake_ctrl_FL_top

--- node 1 ---
  vehicle_dynamics
  toruqe_vector_ctrl
  brake_ctrl_RR_top
  brake_ctrl_FR_top

--- node 2 ---
  vehicle_dynamics
  BMU_ECU
  rear_steer_ctrl
  toruqe_vector_ctrl
  brake_ctrl_RR_top
  brake_ctrl_FL_top
```

```
<vehicle_dynamics>
  node 0
  node 1
  node 2
<BMU_ECU>
  node 2
  node 3
  node 4
<rear_steer_ctrl>
  node 2
  node 3
  node 4
<toruqe_vector_ctrl>
  node 0
  node 1
  node 2
<brake_ctrl_RR_top>
  node 0
  node 1
```

Fig. 19.17 Front-end GUI of our support tool

the dependable task execution. Finally, according to a configuration file prepared by a user, the back-end scripts generate the compiled codes for each processor core, and the codes for the external IO cores.

19.5 Evaluation Kit

On our platform, two types of NoC systems are available, one is a multi-chip ASIC version of an NoC that has a fully-asynchronous on-chip network, and the other is an FPGA version of a synchronous NoC. The fully-asynchronous design style in the former has tolerance against process, temperature, and other variations, and makes it easy to connect many synchronous cores with different clock domains and to form a multi-chip configuration by extending the on-chip network to an off-chip network. On the other hand, users can try various configurations and debug/evaluate their designs easily using the FPGA version (e.g., with FPGA tools like a ChipScope). Both the NoC systems adopt the dependable routing algorithm mentioned in Sect. 19.3 so that a single faulty link or router can immediately be detoured around. As shown in Fig. 19.18, these NoC systems can be selected by "NoC SW" controlled from a PC through the USB3.0 interface.

The ASIC-NoC board can contain up to four base chips, each of which includes 2 × 2 2D mesh on-chip network and four V850E processor cores. Those base chips are connected via off-chip links, and 4 × 4 2D mesh can be configured, when four

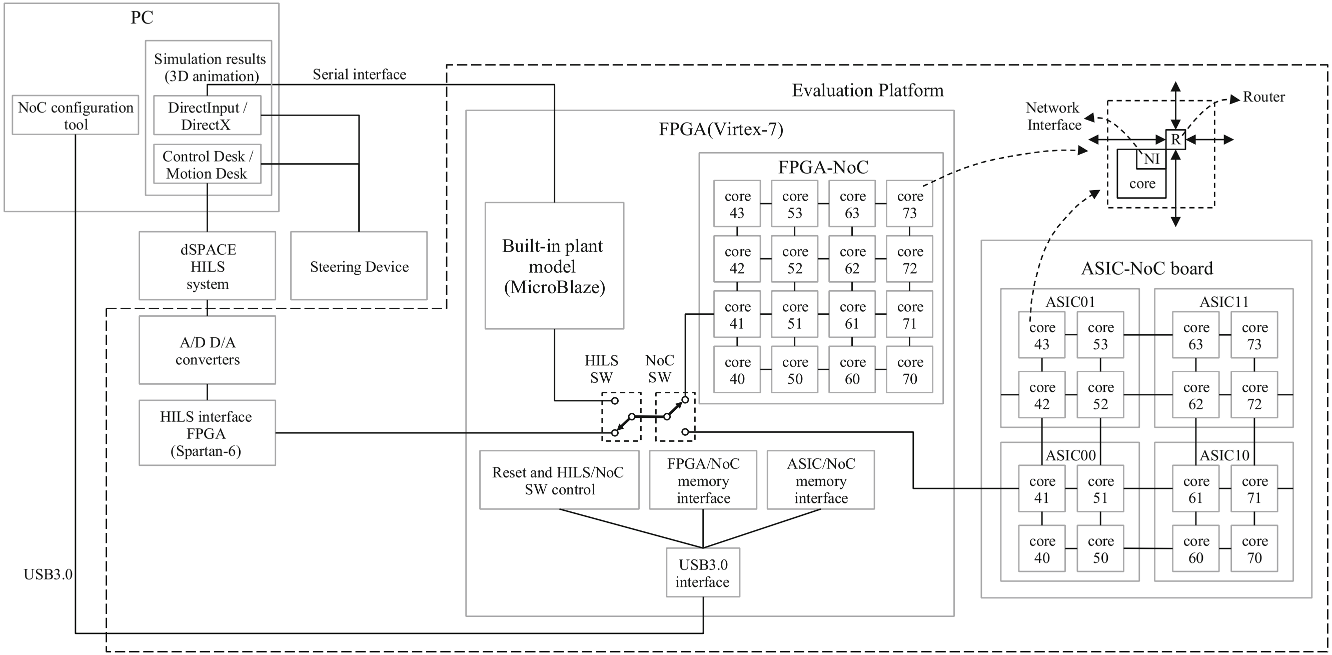


Fig. 19.18 Our hardware platform (from Fig. 1 in [16])

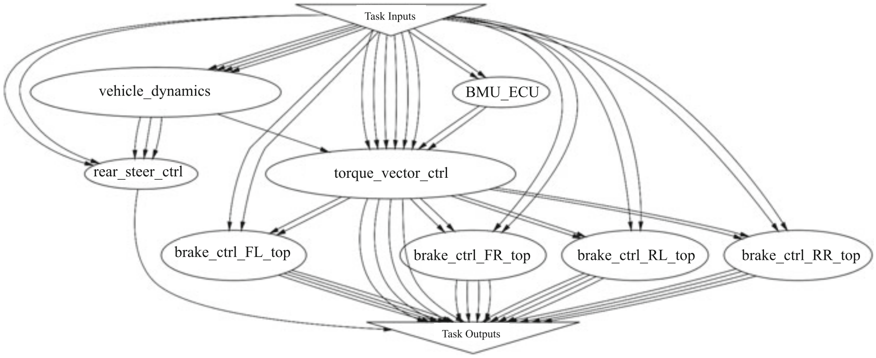


Fig. 19.19 Task graph for our preliminary evaluation (from Fig. 6 in [16])

base chips are used. Considering the extendability and the performance, we are using 5-link base chips. For example, the base chip "ASIC00" shown in Fig. 19.18 has a link to "NoC SW", two links to the base chip "ASIC01", and two links to another base chip "ASIC10". In order to fit the signal pins to our 256-pin LSI package, the off-chip links are partially serialized, as mentioned in Sect. 19.2.

The FPGA-NoC currently contains 4 × 4 2D mesh and sixteen V850E processor cores, but the NoC size can be adjusted depending on the applications.

It is assumed that one of these NoC systems is connected to either a real HILS (Hardware-in-the-loop simulation) system or a built-in plant model, in order to visualize the results obtained by the ECU application tasks. Currently, our platform has a HILS interface for a dSPACE HILS system. As for the built-in plant model, a simplified vehicle dynamics plant model is available, and is executed on a Xilinx soft processor MicroBlaze. Thus, even users who do not have a real HILS system can evaluate their ECU applications easily, although the precision of the simulation is a little degraded.

As a preliminary evaluation, we have applied our platform to an integrated attitude control system of a four-wheel drive electric vehicle. For this application program, eight tasks are defined, and six copies of each task ($r = 6$) are allocated to eight processor cores. Figure 19.19 shows the task graph of this application program. In this experiment, the FPGA version is used, where each processor core has 64 kB local memory, and runs at 50 MHz. For the external IO cores, the same processor cores (i.e., V850E) are used, but much smaller processors or even sequential machines can serve as well. The time for task execution is around 400 μs for small six tasks, and around 2000 μs for remaining large tasks. The time for comparison at the external IO cores is around 20 μs. In order to simulate a faulty processor core, several processor cores are reset one by one. Then, the system has been successfully reconfigured, and performed the application program normally until 5th processor core goes down. Those who are interested may contact Tomohiro Yoneda for the current availability of the tools and evaluation kits.

19.6 Conclusion

This chapter describes our dependable NoC platform suitable for a safety-critical automotive applications. In this platform, in order to handle delay faults or process and other variations, asynchronous design style is used to design on-chip and inter-chip networks. In ASIC base chip, current-mode circuitry is applied for achieving the performance compatibility between on-/off-chip data transmissions. For mitigating router or link faults, a dependable routing algorithm is adopted. Finally, our dependable task execution makes the platform function correctly so long as the capability of surviving processor core faults permits. This chapter also shows some preliminary evaluation results, when it is applied to an integrated attitude control system of a four-wheel drive electric vehicle.

Acknowledgements This work is supported partially by VLSI Design and Education Center (VDEC), the University of Tokyo in collaboration with Synopsys, Inc and Cadence Design Systems, Inc.

References

1. T. Yoneda, M. Imai, N. Onizawa, A. Matsumoto, T. Hanyu, Multi-chip NoCs for automotive applications, in *Proceedings of PRDC2012* (2012), pp. 105–110
2. Recomp, *Reduced Certification Costs for Trusted Multi-Core Platforms*, http://atc.ugr.es/recomp/
3. Race, *Robust and Reliant Automotive Computing Environment for Future Ecars*, http://projekt-race.de/
4. M. Dean, T. Williams, D. Dill, Efficient self-timing with level-encoded 2-phase dual-rail (LEDR), in *Advanced Research in VLSI*, ed. by C.H. Séquin (MIT Press, 1991), pp. 55–70
5. H. Shirahama, A. Mochizuki, Y. Watanabe, T. Hanyu, Energy-aware current-mode inter-chip link for a dependable gals noc platform, in *Proceedings of IEEE International Symposium on Circuits and Systems (ISCAS2014)* (2014), pp. 1865–1868
6. A. Mochizuki, H. Shirahama, T. Hanyu, Design of a quaternary single-ended current-mode circuit for an energy-efficient inter-chip asynchronous communication link, in *Proceedings of 44th IEEE International Symposium on Multiple-Valued Logic (ISMVL2014)* (2014), pp. 67–72
7. A. Mochizuki, H. Shirahama, Y. Watanabe, T. Hanyu, Design of an energy-efficient ternary current-mode intra-chip communication link for an asynchronous network-on-chip. IEICE Trans. Inf. Syst. **E97-D**(9), (2014)
8. W. Dally, B. Towles, *Principles and Practices of Interconnection Networks*, (Morgan Kaufmann Publishers, 2003)
9. D. Fick, A. DeOrio, G. Chen, V. Bertacco, D. Sylvester, D. Blaauw, Highly resilient routing algorithm for fault-tolerant NoCs, in *Proceedings of DATE09* (2009), pp. 21–26
10. P.-H. Sui, S.-D. Wang, Fault-tolerant wormhole routing algorithm for mesh networks. IEE Proc. Comput. Digit. Tech. **147**(1), 9–14 (2000)
11. J. Zhou, F. Lau, Adaptive fault-tolerant wormhole routing in 2D meshes, in *Proceedings of IPDPS01* (2001)
12. C.J. Glass, L.M. Ni, Fault-tolerant wormhole routing in meshes. *Proceedings of FTCS23* (1993), pp. 240–249

13. M. Imai, T. Yoneda, Improving dependability and performance of fully asynchronous on-chip networks, in *Proceedings of ASYNC2011* (2011), pp. 65–76
14. H. Saito, T. Yoneda, Y. Nakamura, An ILP-based multiple task allocation method for fault tolerance networks-on-chip, in *Proceedings of MCSoC2012* (2012), pp. 100–106
15. M. Imai, T. Yoneda, Fault diagnosis and reconfiguration method for network-on-chip based multiple processor systems with restricted private memories. IEICE Trans. Inf. Syst. **E96-D**(9), 1914–1925 (2013)
16. T. Yoneda, M. Imai, H. Saito, T. Hanyu, K. Kise, Y. Nakamura, An NOC-based evaluation platform for safety-critical automotive applications, in *Proceedings of APCCAS2014* (2014)

Chapter 20
An On-chip Router Architecture for Dependable Multicore Processor

Kenji Kise

Abstract The multicore and manycore architectures exploiting thread-level parallelism have become promising because of their high-performance and low-power consumption. However, the dependability degradation of multicore and manycore chips caused by soft errors is becoming a serious problem. In order to mitigate this problem, this chapter describes SmartCore system (smart manycore system with redundant cores and multifunction routers) to improve the dependability of a manycore chip with flexible DMR (dual modular redundancy) using redundant cores and the original NoC router named the multifunction router. We discuss the multifunction router architecture where the unique functions of the packet modification, the packet comparison to detect errors occurred on cores, and the packet duplication for DMR are realized efficiently. The benefit of the SmartCore architecture consists in its simplicity that the NoC router is capable of detecting errors as well as directing and copying the packets sent between the processor cores. This enables building manycore processor system with ease and very little overhead.

Keywords Network-on-chip · Multicore processor · Manycore processor
Dependable multicore · Dual modular redundancy

20.1 Introduction

To enhance the power and performance efficiency of processor chips, multicore and manycore architectures exploiting thread-level parallelism have become promising. In the near future, more than a few thousand cores will be integrated on a manycore chip due to the continuous technology scaling of the semiconductor industry.

In addition to the power and performance issues for these chips, the dependability issue will be a serious problem because it is estimated that the rate of the soft error mainly caused by the cosmic ray could increase from one error per year to one error per month and more in a decade.

K. Kise (✉)
Tokyo Institute of Technology, Tokyo, Japan
e-mail: kise@c.titech.ac.jp

S. Asai (ed.), *VLSI Design and Test for Systems Dependability*,
https://doi.org/10.1007/978-4-431-56594-9_20

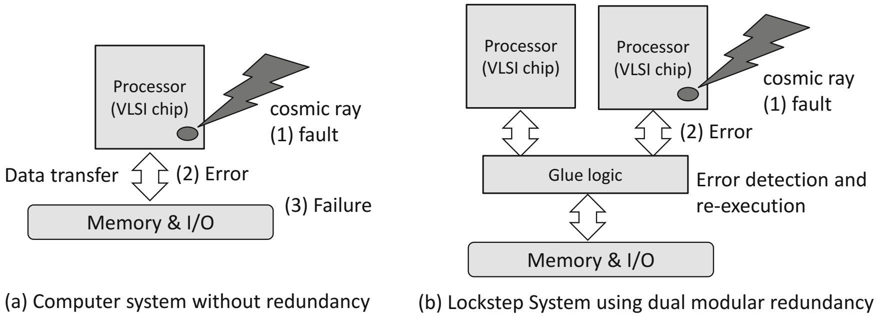


Fig. 20.1 A computer system without redundancy and a lockstep system with dual modular redundancy

Lockstep [1] system has been used to design some dependable computer systems. Figure 20.1 shows two systems: (a) a computer system without redundancy where injected fault may cause errors and finally may lead to failure, and (b) a lockstep system with dual modular redundancy (DMR). In lockstep system, two identical processor chips execute the same program redundantly, and the glue logic detects an error occurred on a processor chip by comparing two chips' outcomes. The pair of processors should be synchronized and their outputs are compared at every cycle. The drawbacks of lockstep system are the large additional hardware cost and power consumption.

This chapter describes SmartCore system [2] (smart manycore system with redundant cores and multifunction routers) toward a manycore processor which consists of more than a few thousand cores. SmartCore system is a mechanism to improve the dependability of a manycore chip with flexible DMR using redundant cores and multifunction routers.

20.2 SmartCore System

SmartCore system improves the dependability of a manycore processor adopting network-on-chip (NoC). It detects errors occurred on cores in the packet level. A node on a manycore processor transfers data to other nodes in the packet unit. Therefore, the error is detected by comparing a packet with the correct packet. SmartCore system does not detect the errors occurred on NoC routers and transmission links between routers. It is another challenge to be solved.

First, we show the normal communication flow on a 2D mesh topology multicore with dimension-order routing. Figure 20.2a shows a physical layout of a 16-node multicore processor with the 4 × 4 mesh topology. Each dash-lined rectangle represents a node consisting of a processing element (or core) indicated by a triangle and an NoC router indicated by a circle. Each node has an identifier which is

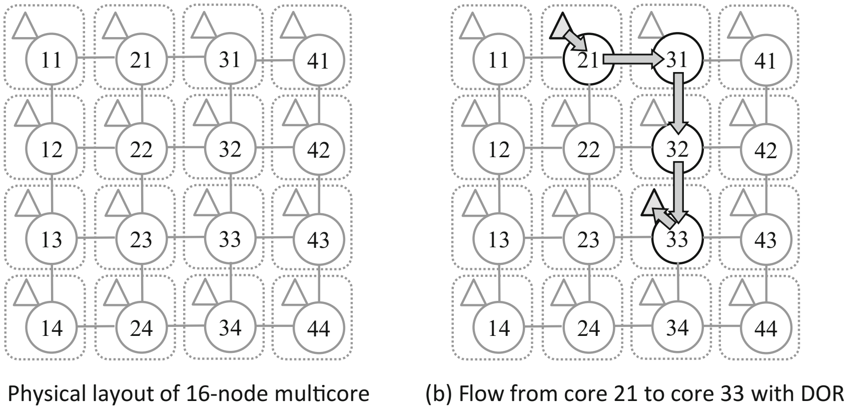

11
21
31
41
12
22
32
42
13
23
33
43
14
24
34
44
(a) Physical layout of 16-node multicore
(b) Flow from core 21 to core 33 with DOR

Fig. 20.2 The normal communication flow from core 21 to core 33 on a 2D mesh topology multicore processor with dimension-order routing

constructed by concatenating the x-coordinate and y-coordinate. In this figure, the top-right node's identifier is 41 (x = 4, y = 1).

Figure 20.2b shows a normal communication flow from core 21 to core 33. We use the XY dimension-order routing where a packet first proceeds in the horizontal direction (x-dimension) and then in the vertical direction (y-dimension). In this example, a packet is transferred from core 21 to core 33 via four routers in the following sequence: 21, 31, 32, and 33.

Second, we show the logical communication flow of SmartCore system. In Fig. 20.3, the comparison of flows between a normal system and SmartCore system is shown. Figure 20.3a shows a flow of the normal system where core A sends a packet to core B. The narrow arrow represents the data transfer between core and router in a node. The gray wide arrow between nodes indicates the communication between the source node and the destination node. This communication may involve multiple router traversals.

Figure 20.3b shows the corresponding logical communication flow in SmartCore system. For the dual modular redundancy, a pair of nodes, a master and a slave, is used for node A, and the same for node B. Therefore, a total of four nodes (master node A, slave node A, master node B, and slave node B) are used for the normal system's node A and B.

Both master/slave nodes A have the same logical node identifier of A and execute the same thread. Similarly, master/slave nodes B have identifier of B and execute the same thread. The packet injection from core A in the normal system corresponds to two identical packet injections from master/slave core A in SmartCore system. One packet from slave core A is injected to slave router A, and slave router A modifies the packet's destination to master core A; therefore, the packets from slave core always arrive at the pairing master router. The other packet from master core A is injected to master router A. Therefore, both packets from master/slave cores A arrive

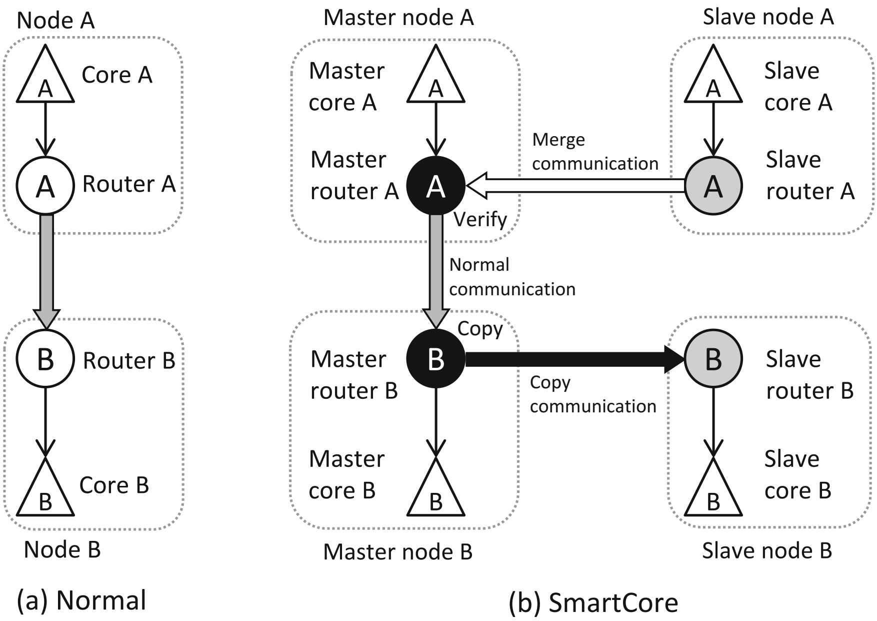


Fig. 20.3 The comparison of logical communication flows between a normal system and SmartCore system

at master router A where two packets are compared to detect the error occurred on either master/slave core A. The white wide arrow represents a unique communication of SmartCore from the slave router to the master router, and it is called "merge communication."

While waiting for the arrivals of two packets and comparing the packets, master router A sends the packet, whose destination is master core B, toward master router B, which is represented by the gray wide arrow in Fig. 20.3b. This communication is called "normal communication."

When the packet arrives at master router B, the router duplicates the packet. One packet is forwarded to master core B. The other is sent to slave core B by modifying the packet's destination to slave core B. This unique communication, which is represented by the black wide arrow in Fig. 20.3b, is called "copy communication." Thus, master/slave cores B receive the same packets and continue to execute the same program.

Third, we show an example of physical communication flow on SmartCore system. Figure 20.4a shows a normal communication flow from core A to core B where node A is assigned to node 21 and node B is assigned to node 14. As we see in Fig. 20.2, a packet proceeds in the horizontal direction to node 11 and then goes in the vertical direction to node 14.

Figure 20.4b shows the corresponding communication flow on SmartCore system where master/slave nodes A and master/slave nodes B are assigned to node 21, 42, 14,

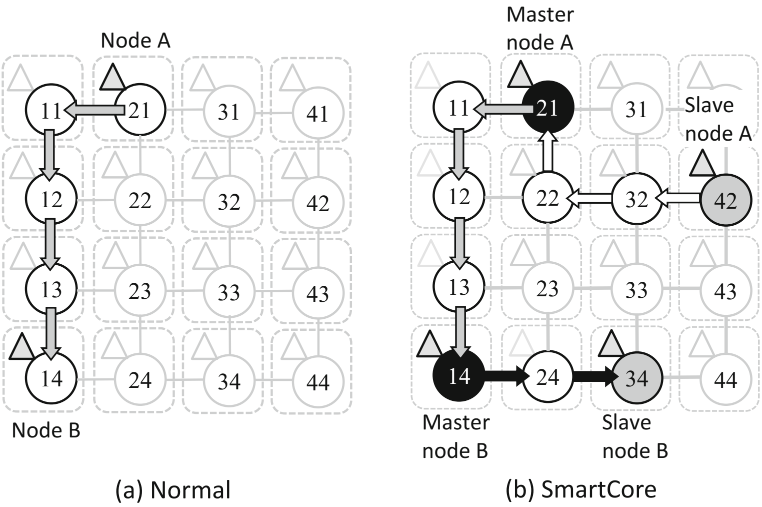


Fig. 20.4 The comparison of the physical communication flows between a normal system and SmartCore system

and 34, respectively. The flow from router 42 to router 21 is a merge communication. The flow from router 21 to router 14 is normal communication. And the flow from router 14 to router 34 is copy communication. The packets from core 21 and 42 are compared at router 21. Router 14 duplicates the packet and sends them to core 14 and 34.

In contrast to the fixed DMR of lockstep, the flexible DMR is supported by SmartCore system. After the chip fabrication enabling SmartCore system, the option of whether to use DMR or not for each thread, which depends on the criticality of the thread, can be selected by the operating system, system software, and system users. Moreover, for every thread with DMR, any node can be assigned as its master/slave nodes.

Some node mapping strategies for SmartCore system processing eight threads are shown in Fig. 20.5. Figure 20.5a shows a normal node mapping strategy without DMR. In this case, the eight nodes are assigned to eight threads. The identifier with a letter "L" indicates that the logical thread is allocated to the node. In this example, logical thread 11 (L11) is allocated to the top-left node.

Figure 20.5b, c shows two mapping strategies with DMR of SmartCore system. We assume that the four threads L11, L12, L21, and L22 are critical, and each should be executed on two cores. Figure 20.5b shows an interleave node mapping strategy where two continuous nodes in the x-direction are allocated for a logical thread. The identifier with a letter "M"/"S" indicates that the node is allocated as the master/slave node. The gray-colored two nodes are allocated to L11, and they make a pair for DMR. In this example, the left node with M11 is the master and the right node with S11 is the slave. This is a straightforward mapping strategy for high

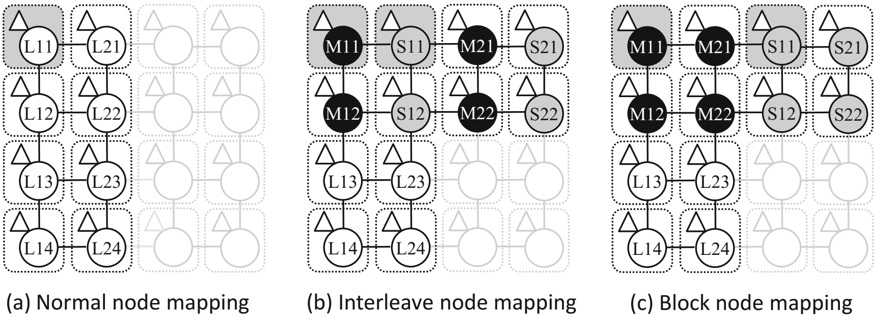


Fig. 20.5 Some node mapping strategies for SmartCore system running eight threads. Four threads for L11, L12, L21, and L22 nodes are critical

performance because the number of routers between the master and the slave in a pair is the smallest.

Figure 20.5c shows a block node mapping strategy where the blocked master nodes (M11, M12, M21, and M22) are adjacent nodes. This is a mapping for higher dependability, where the master node and the slave node of each pair are far away from each other in order to alleviate the effect of the common cause failure.

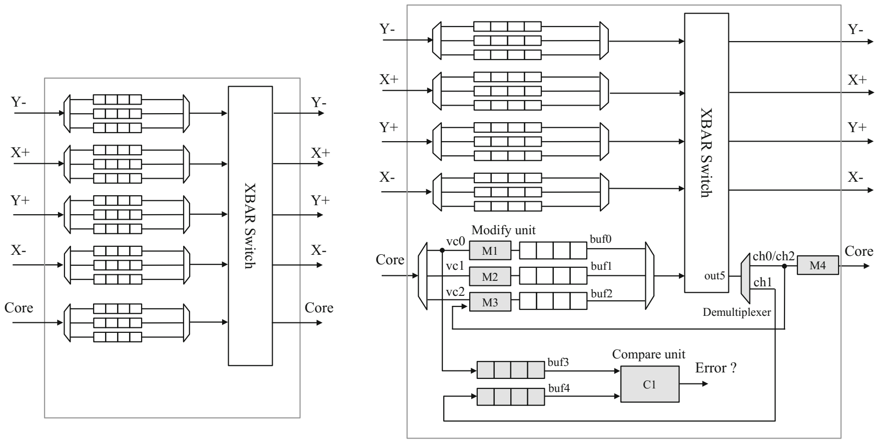
20.3 NoC Multifunction Router for SmartCore System

We describe the multifunction router architecture for SmartCore system. Figure 20.6 shows the main data paths of an input-buffered router and a multifunction router for SmartCore system. The multifunction router is based on the standard input-buffered router [3] with three virtual channels as shown in Fig. 20.6a.

The additional hardware units from an input-buffered router are gray colored in Fig. 20.6b. They are two buffers named buf3 and buf4, a compare unit C1, four packet modify units named from M1 to M4, and a demultiplexer before M4.

The multifunction router could behave as the input-buffered router. This is obvious because two data paths in Fig. 20.6 become identical when setting the demultiplexer output to ch0, and connecting the input and output wires of each packet modify unit (M1, M2, M3, and M4) directly. In Fig. 20.5, the white color routers are the multifunction router configured as the standard input-buffered routers.

We discuss the deadlock issue and the usage of virtual channels. From the communication flow in Fig. 20.4b, we see some forbidden turns to the horizontal direction after the vertical direction at router 21 and router 14. Note that these forbidden turns occur only at master routers. These turns are not allowed in XY dimension-order routing and may cause the deadlock. To avoid this deadlock, the multifunction routers use three virtual channels (vc0, vc1, and vc2). Specifically, vc0, vc1, and vc2 are used for the normal, merge, and copy communication, respectively.



(a) Data path of an input-buffered router

(b) Data path of a multifunction router

Fig. 20.6 The main data paths of an input-buffered router and a multifunction router for SmartCore system

We explain the router behavior in a slave node. Please remember that the slave router A in Fig. 20.3 modifies the packet's destination to master core A, and vc1 is used for the merge communication. Therefore, a packet from a slave core is injected to the slave router with vc1 link and then entered into M2. The modify unit M2 changes the packet's destination to the pairing master core. After that, the packet is stored in buf1 to be routed to the pairing master core. In the slave node of a packet receiving side (slave router B in Fig. 20.3), a packet arrives through the copy communication via vc2. The packet is routed through the switch to out5. The demultiplexer emits the packet to ch2. The modify unit M4 sets the virtual channel number for the packet to vc0 in order to use the normal communication. Then, the packet is transferred to the slave core.

Next, we explain the router behavior in a master node. First, let us see the packet comparison mechanism done in master router A in Fig. 20.3. A packet from the master core is injected into the master router via vc0 link. Then, the packet is duplicated. One packet is entered into M1 where its virtual channel number is set to vc1 in order to use the normal communication. The other is stored in buf3 for the comparison. A packet from the slave router is injected to the master router via vc1 with the destination modified to the master core. Therefore, as shown in Fig. 20.6, the packet is routed through the switch to port out5. The demultiplexer emits the packet to ch1. After that, the packet is stored in buf4. Note that each flit of the packet is stored in an entry of buf3 and buf4. In particular, buf3 and buf4 are used as FIFO buffers like other input buffers. When the valid flits are in both buf3 and buf4, C1 dequeues two flits from these two buffers and compare them in order to detect errors occurred on cores.

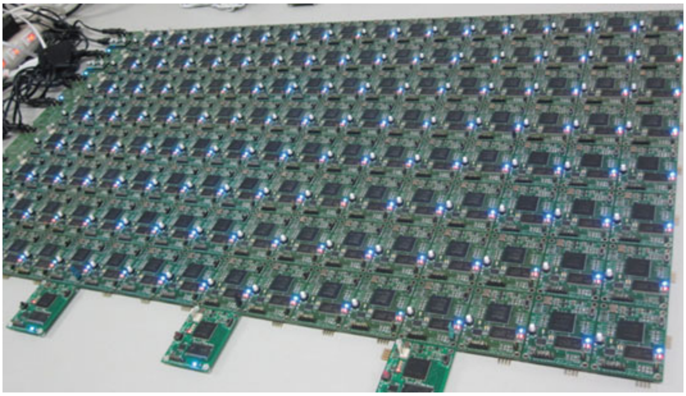


Fig. 20.7 The multi-FPGA-based processor simulation platform

Second, we discuss the packet duplication mechanism done in master router B in Fig. 20.3. A packet is injected to the master router via vc0 link. The destination of the packet is the master core. The packet is routed through the switch to port out5. The demultiplexer emits the packet to ch0. After that, the packet is duplicated. One packet is ejected to the core in the same node, and the other is entered into M3 where the packet's destination is modified to the pairing slave node and the virtual channel number is modified to vc2. Then, the packet is stored in buf2. This packet will arrive at the slave core through the copy communication.

The verifications of SmartCore system with some benchmark programs are done using not only software simulations but also the original designed multi-FPGA prototyping system [4] shown in Fig. 20.7. Although this FPGA prototyping system has been commercialized in 2012, currently it is not for sale from the licensing issue.

20.4 Conclusion

This chapter describes SmartCore system to improve the dependability of a manycore chip with flexible DMR using redundant cores and the multifunction NoC routers. The key to realize SmartCore system is the multifunction router architecture. We discuss the multifunction router architecture where the unique functions of the packet modification, the packet comparison to detect errors occurred on cores, and the packet duplication for dual modular redundancy are realized efficiently.

The benefit of the SmartCore architecture consists in its simplicity that the router is capable of detecting errors as well as directing and copying the packets sent between the processor cores. This enables building manycore processor system with ease and very little overhead.

References

1. PowerPC 750GX Lockstep Facility. IBM Application Note (2008)
2. T. Shinya, S. Shimpei, M. Takefumi, K. Kenji, Smart core system for dependable many-core processor with multifunction routers. *International Conference on Networking and Computing (ICNC'10)*, pp. 133–139, November 2010
3. D. William, T. Brian, *Principles and Practices of Interconnection Networks* (Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 2003)
4. S. Takamaeda, S. Sano, Y. Sakaguchi, N. Fujieda, K. Kise, Scalable core system: a scalable many-core simulator by employing over 100 FPGA. *The 8th International Symposium on Applied Reconfigurable Computing (ARC2011)*, March 2012

Chapter 21
Wireless Interconnect in Electronic Systems

Tadahiro Kuroda and Atsutake Kosuge

Abstract Since conventional mechanical connectors have metal contacts that are susceptible to contamination, fatigue, and wear, they are unreliable and failure-prone components of systems. Signal integrity is also degraded due to an impedance discontinuity at the electrodes. To overcome such problems, various kinds of noncontact type wireless interconnection methods have been studied. Noncontact communications that use near-field coupling provide immunity to mechanical damages caused by vibration/friction and isolation from water/chemicals while reducing fabrication costs. A problem for conventional near-field communications such as inductive and capacitive couplings is poor signal integrity due to the impedance mismatch. This chapter introduces the basic concept and features of transmission line coupler (TLC), an impedance-matched and terminated wide-bandwidth coupler enabling signal branching without signal reflections. Two transmission lines are coupled to form TLC, same as microstrip filters. The broadband characteristics enable baseband communication. A 12 Gb/s data link was confirmed by experiments at a distance of 1 mm. A 12.5 Gb/s 8-drop multidrop bus system was also confirmed by experiments by using TLC at each signal branching point. Strong misalignment tolerance of TLC realizes high vibration tolerance too. Under the same vibration as satellite launching and vehicles, no change in the characteristics and no bit errors were confirmed. Analysis and design of coupler and transceiver are presented. Examples of applications are shown. Issues and countermeasures in each application are discussed.

Keywords Near-field communication · Near-field coupling · Electromagnetic coupling · Transmission line coupler (TLC) · Wireless connector
Wireless packaging

T. Kuroda (✉)
Keio University, Yokohama, Japan
e-mail: kuroda@elec.keio.ac.jp

A. Kosuge
Hitachi, Ltd., Hitachi, Japan
e-mail: Atsutake.Kosuge@ieee.org

S. Asai (ed.), *VLSI Design and Test for Systems Dependability*,
https://doi.org/10.1007/978-4-431-56594-9_21

21.1 Introduction

Although connectors are widely used for connecting modules, reliability problems arise as system speed increases and system size decreases. The reliability problem, as explained in Sect. 8.1, is caused by the mechanism for physically crimping the exposed electrode with a spring. Because the electrode is exposed, there is wear on the electrode with each insertion. Also, if there is vibration, power flicker occurs as electrodes are disconnected that can result in communication errors and loss of data. Signal quality can also be degraded by loss of continuity in the impedance at the electrodes. Another problem is that miniaturization is difficult because a spring structure is required to ensure physical contact between the electrodes.

To solve such problems, research is being done on noncontact type connections, which use electronic means rather than mechanical means. Contactless connections eliminate mechanical problems such as friction and power flicker. Such connections are also suitable for miniaturization and circuit profile reduction because they can be formed simply by drawing an antenna pattern in the wiring on the circuit board. This chapter describes various methods that have been proposed for wireless interconnection. The transmission line coupler (TLC), in particular, is described in detail as a transmission scheme that uses near-field electromagnetic coupling.

21.2 Wireless Interconnection

The three types of wireless interconnection that are being used are those that use millimeter waves, lumped constant type coupling that uses coils and capacitors, and distributed constant type coupling that uses both the electric field and the magnetic field. The features of each of the three types are described below.

21.2.1 Millimeter Waves

Connection methods that use millimeter waves transmit a radio signal to a remote location via an antenna in the same way as in conventional wireless communication between terminals. Millimeter waves are often used for connections between modules within equipment in particular because high data rates on the order of 10 Gb/s are possible [1, 2]. However, modulation at the high frequency of 60 GHz requires complex transceiver circuits and the power consumption is also high. Compared to the energy consumption of ordinarily wired transceivers, which is 10 pJ/b or less, transceivers that use RF or millimeter waves consume about 100 pJ/b, which is higher by a factor of 10.

21.2.2 Near-Field Electromagnetic Coupling

Communication via near-field electromagnetic coupling is possible. Magnetic field coupling using coils [3, 4] and electric field coupling using capacitors [5] are being studied. Near-field electromagnetic coupling offers two advantages. One is that the transceiver circuit can be built in about the same way as a digital circuit with a low power consumption (See Sect. 21.3.). The other advantage is that there is little signal leakage. A coupler that uses near-field electromagnetism operates in theory as a first-order differential filter. Accordingly, its characteristic does not have a sharp peak at a particular frequency as does an antenna. By transmitting the digital signal without modification, a first-derivative waveform appears on the receiving side. The signal can then be easily restored by a receiver that has an integrating function. Modulation and demodulation are not necessary, so the first stage amplifier of the receiver can be eliminated and the transceiver can be constructed almost entirely of digital circuits. Thus, low power operation is possible. The power consumption of 4.68 mW has been reported for communication at 1.2 Gb/s over a distance of 1 mm by magnetic field coupling using a coil [4]. With near-field communication, the signal attenuates in proportion to the third power of the distance, so the signal is not radiated far and there is little signal leakage.

A problem for near-field communication is speed. The two factors that affect speed in near-field communication are the parasitic component and signal reflection. For an inductor, the diameter of the coil must be roughly three times as large as the communication distance between ordinary coils. On the other hand, parasitic capacitance increases with the coil size. Thus, the resonant frequency determined by the parasitic capacitance and the coil inductance is lower and the communication band is restricted. For example, if the communication distance is 1 mm, the designed coil diameter is about 3 mm. In that case, the resonant frequency is about 2.0 GHz and the maximum data rate is limited to about 1 Gb/s. Actually, a data rate of 1.2 Gb/s has been obtained using a coil that has a diameter of 2.4 mm for a communication distance of 1 mm [4].

The other factor that affects speed is that impedance matching is not possible. For transmission lines that are longer than 1/20 of the wavelength, the phase of the signal is different at each point on the transmission line, so it acts as a distributed constant circuit. For a 1 GHz signal, a transmission line that is roughly 7 mm or longer will behave as a distributed constant circuit, with the wavelength shortening effect included. On the other hand, coils and capacitors behave in a lumped constant manner, so the characteristic impedance cannot be determined. Without matched terminals, signal reflection occurs, the signal waveform is greatly disturbed, and the data rate is restricted. In addition, the transceiver must be located nearby.

The problems described above can be solved by using a transmission line coupler (TLC) [6–11]. By arranging transmission lines facing each other, signals can be transmitted between the lines via near-field electromagnetism. A transmission line coupler is a distributed type system that uses both magnetic field coupling

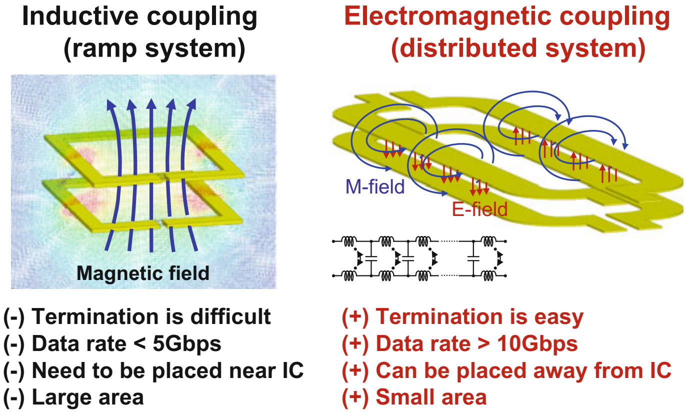


Fig. 21.1 Comparison between inductive coupling and electromagnetic coupling

and electric field coupling, so terminal matching is possible that enables a data rate of 12 Gb/s at a distance of 1 mm [6]. The features of this type of coupling are shown in Fig. 21.1. The details are described in the next section.

21.3 Transmission Line Couplers

A transmission line coupler (TLC) is a transmission line that has distributed electric field coupling and magnetic field coupling. Because this type of coupler allows impedance matching, it provides a broad bandwidth. There is no signal reflection at the line connection, so the coupler can be placed at a distance from the IC. In addition, the communication band depends only on the length of the coupler line; there is no dependence on the line width or communication distance. This section summarizes the TLC design methodology and presents application examples.

21.3.1 TLC Design

Because a transmission line coupling allows terminal matching, it provides a broad communication bandwidth (Fig. 21.2). The characteristic impedance can be adjusted by changing the transmission line width or the distance between lines. It is normally designed to be 50 Ω. There is no signal reflection in a 50 Ω transmission line, even when the connection is at a distance from the IC. Accordingly, communication at over 10 Gb/s is possible.

The four parameters of the TLC are communication distance, *d*, line width, *W*, distance between lines, *S*, and the length of the coupler line, *L*. The communication

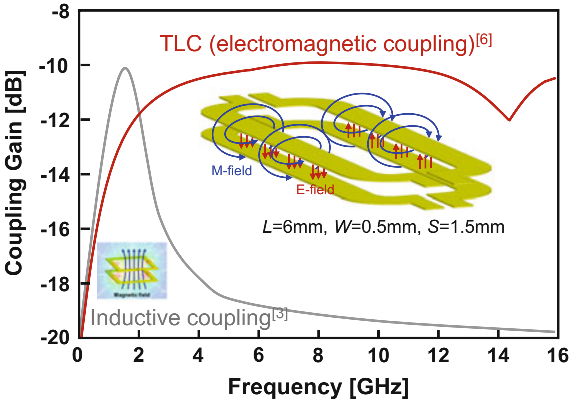


Fig. 21.2 Frequency characteristics of TLC

band depends only on the length of the coupler line, so it is determined independently of the communication distance, the line width, or the distance between lines. The central frequency of the communication band, f_c, is inversely proportional to the line length as shown in the following equation. The central frequency, therefore, shifts toward higher frequencies as the line length decreases (Fig. 21.3).

$$f_c = \frac{c}{4L\sqrt{\varepsilon_r}}$$

In the above equation, c is the speed of light in vacuum and ε_r is the relative permittivity of the substrate material. As the length of the coupler line decreases, the frequency increases and faster communication is possible. In practice, however, there is line loss on the transmission line that connects the TLC and the IC, so the maximum transfer rate that is obtained is limited by line loss. Also, if the line length is reduced and the central frequency shifts in the higher direction, the lower cutoff frequency also shifts upwards. In that case, the total signal power transmitted to the

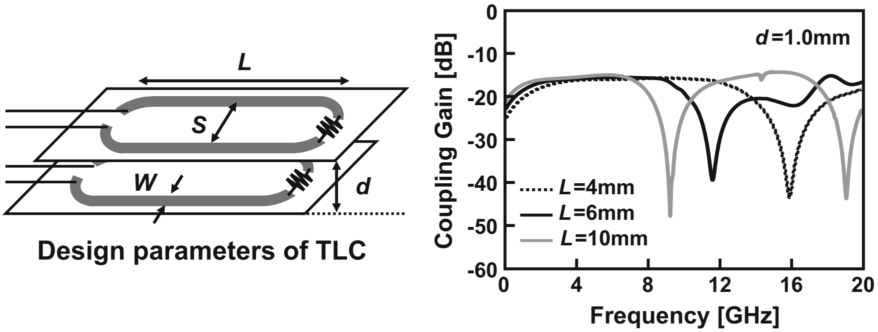


Fig. 21.3 Design parameters of TLC

receiver decreases, the received signal amplitude decreases, and signal becomes more susceptible to noise. Conversely, if the signal line length is excessively long, the upper cutoff frequency is reduced, which may give rise to intersymbol interference (ISI). Therefore, the coupler line length is limited to a certain range, which is typically from 3 to 5 mm. The coupling gain and characteristic impedance of the TLC depend on the line width and the communication distance. To maintain a constant coupling gain and characteristic impedance, the line width must be large relative to the communication distance. The distance between lines is set to about three times the line width to prevent coupling between differential lines. In the example presented in reference [9], the line width, *W*, is 0.5 mm and the distance between lines, *S*, is 1.25 mm for a communication distance, *d*, of 0.1 mm.

The TLC has high tolerance to misalignment, both vertically and horizontally (Fig. 21.4). The coupling gain for a communication distance of 1 mm is 14 dB, but decreases to only 4.4 dB when the distance is increased by a factor of 1.5. Because sufficient received signal amplitude can be maintained, there is no degradation of reliability and communication is possible. To secure an even higher amplitude tolerance, an amplifier can be added to the receiver. Similarly, there is high tolerance of misalignment in the horizontal direction. Even if there is misalignment on the order of the line width (*W*) in the line-width direction and half of the line length (*L*) in the line-length direction, the decrease in coupling gain is only 1.7 dB. A mechanism for fine alignment is not needed, so the implementation cost can be reduced.

The TLC uses baseband communication, so the transceiver can be constructed as a digital circuit in the same way as for conventional wired communication (Fig. 21.5). Accordingly, a complex modulator–demodulator mechanism is not required, so fast communication is possible with low power consumption. The TLC is driven by a line driver in the same way as for conventional wired communication. The output impedance of the driver stage is adjusted to the characteristic impedance of the TLC. Because the TLC is typically designed for a characteristic impedance of 50 Ω, the output impedance of the driver is adjusted to 50 Ω. Because the TLC is a contactless connection that is electrically isolated, the DC component is not

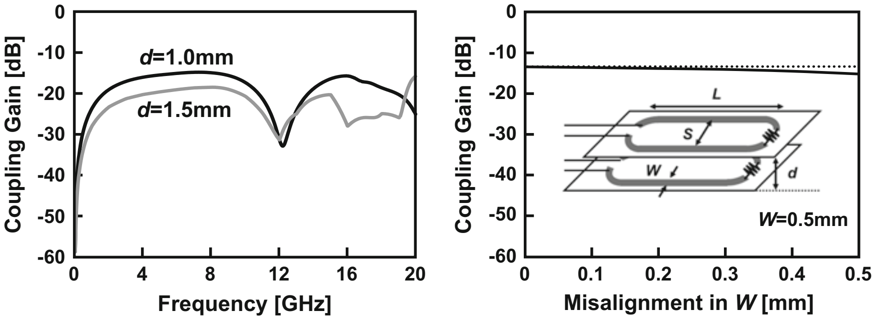


Fig. 21.4 Misalignment tolerance

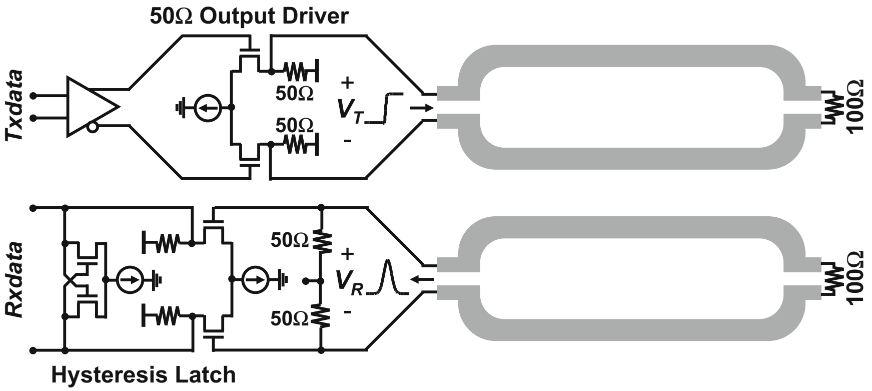


Fig. 21.5 Transceiver circuit schematics

transmitted. The transmitted waveform, therefore, appears on the receiver side as a first-derivative pulse waveform. To recover the DC component, a hysteresis latch is used in the receiver. When a signal that is higher than a certain threshold arrives, the hysteresis latch inverts the output. Accordingly, the effect of noise can be suppressed by setting a high threshold value if the signal-to-noise ratio (SNR) is sufficiently high. The threshold value can be adjusted according to the ratio of two tail current sources. The power required by the hysteresis latch is about the same as for a typical current mode logic (CML) latch circuit, which is 1 mW or less for a 65 nm CMOS circuit. The power required to restore the original digital waveform from the received pulse waveform is therefore slight.

Using TLC, enables data transfer at 12 Gb/s at a distance of 1 mm (Fig. 21.6). The bit error rate (BER) is 10^{-13} or less, which indicates transmission reliability that is comparable to conventional wired communication. On the other hand, the

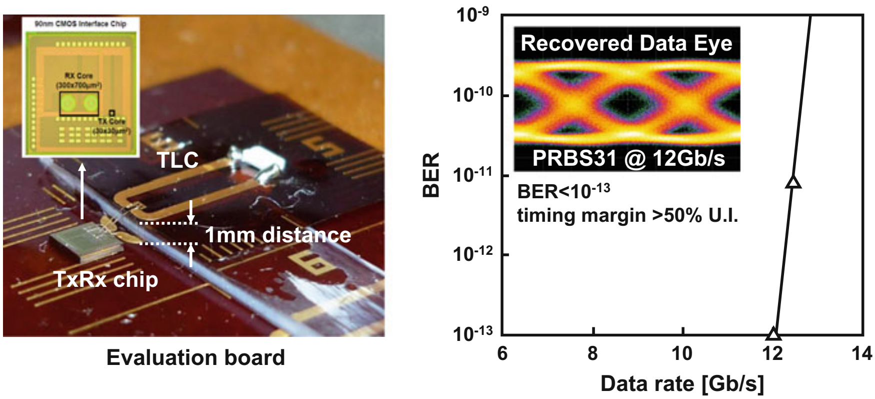


Fig. 21.6 12 Gb/s data transmission at a 1 mm communication distance

BER depends on the SNR, and if a WiFi or LTE transmitting antenna that is generating a 30-dBm interference signal is near the coupler, communication errors occur [11]. In that case, measures such as described in [11] are needed. The power consumption of a circuit fabricated with 90-nm CMOS technology is 7.4 pJ/b. This connection technology can, therefore, provide the same high energy efficiency as wired communication [6].

21.3.2 TLC Application Examples and Their Design

One application area for TLC's is in wireless packaging of modules in high-performance IT equipment such as servers, which can take advantage of the high speed and high quality offered by TLC connections. TLC's can be configured as multidrop buses (Fig. 21.7). A multidrop bus can connect multiple modules on a single bus, thus greatly reducing the number of wires and the surface area used. With conventional wire connectors, on the other hand, wires at branch points become stubs that give rise to multiple signal reflections, thus limiting communication speed to 3.2 Gb/s. That problem does not arise with TLC connections because uniform impedance is maintained in signal branching. That feature makes it possible to maintain point-to-point signal quality in a multidrop bus configuration. However, there is a problem concerning the adjustment of the coupling gain of the

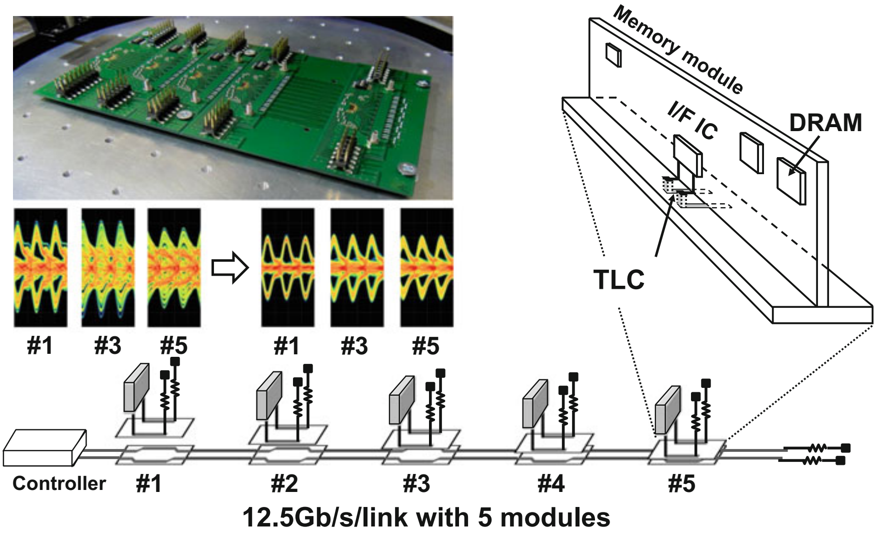


Fig. 21.7 Noncontact multidrop bus system for server application

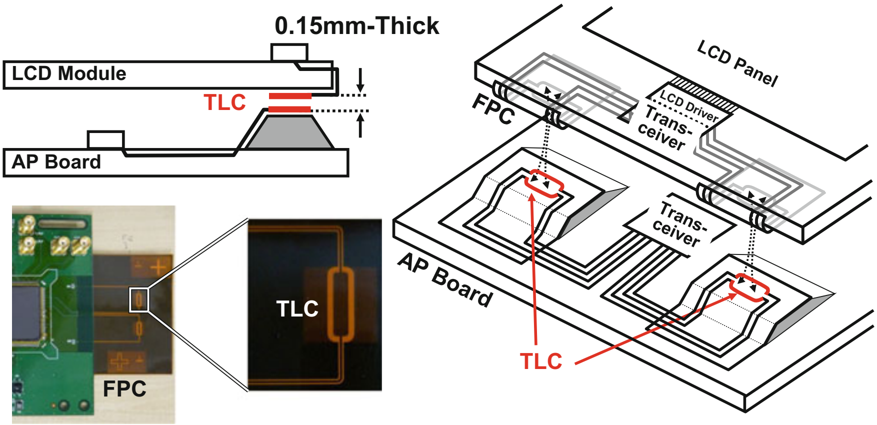


Fig. 21.8 0.15-mm thick noncontact connector for mobile devices

TLC's. If all of the TLC's have the same coupling gain, high signal power can be obtained with the first TLC, but there is attenuation as the signal passes each subsequent TLC, resulting in a low signal amplitude. Therefore, the coupling gain of each coupler is adjusted so as to evenly distribute the signal power over all the modules. The coupling gain can be adjusted by varying the communication distance. By further optimizing the line width on the bus side, a uniform impedance can be maintained. In this way, a data transfer rate of 12.5 Gb/s can be achieved, that is five times as fast as the current maximum [7, 8].

Another application area for TLC's is handheld devices such as smartphones, which can benefit from the compactness and low implementation cost offered by TLC interconnection. A thinner product design can be achieved by using TLC wireless connectors between the LCD display and the main circuit board (Fig. 21.8) [9]. The coupler patterns can be formed directly using wiring patterns on the circuit boards, so a connector housing is not necessary and ultimately thin connectors can be achieved. Because the TLC enables matched termination, the TLC connection can be made on the transmission line at a distance from the IC. By forming the TLC and transmission line on a flexible substrate, the TLC can be placed anywhere within the device, as shown in Fig. 21.8.

One of the features of the TLC is that a single coupler can transmit two different signals (Fig. 21.9). By sandwiching the TLC between the substrate and a resin that has about the same relative permittivity with impedance matching, it is possible to restrict the signal propagation to a single direction (e.g., Port 3 → Port 1). The distant signal (Port 4 → Port 1) is received at only one-tenth the strength of the signal received from the near terminal (Port 3 → Port 1). Because the receiver accepts only a signal above a threshold, only the signal received from the nearby

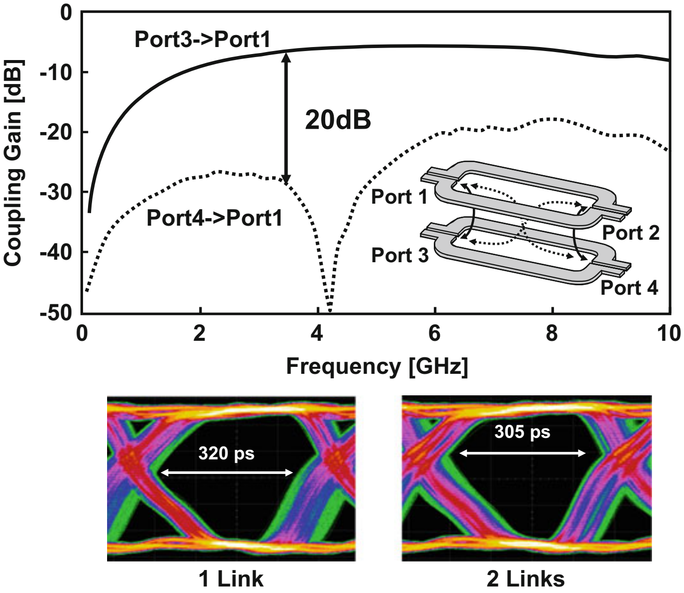


Fig. 21.9 Simultaneous two-links in one coupler

terminal is recovered. Therefore, a single coupler can transmit two different signals. Measurement data shows that the timing margin for two-channel simultaneous transmission is only slightly less than single channel transmission at 2 Gb/s (Fig. 21.9). Transmitting different signals over two channels can double the efficiency of using circuit board area.

Because the TLC is a noncontact connection, it is robust against vibration. Even if the vibration changes the communication distance, communication is not affected. It is, therefore, suitable for automotive applications, which require a high tolerance of vibration. Application to automotive LAN can reduce the total weight of LAN wiring by 30% [10]. High coupling gain can be achieved even through the wiring insulation by enveloping the wires of a twisted-pair cable. It is thus possible to form a clip type connection at any place on the wiring harness without stripping the wires (Fig. 21.10). This new type of connector enabled by the concept of TLC is called electromagnetic clip connector and is very well suited to automotive LAN applications. For conventional connectors, strength against vibration is maintained by collecting all the wiring harness connectors in a junction box that increases overall cable length because all the wiring must extend to the junction box. Electromagnetic clip connectors, on the other hand, can be used in any location on the wiring

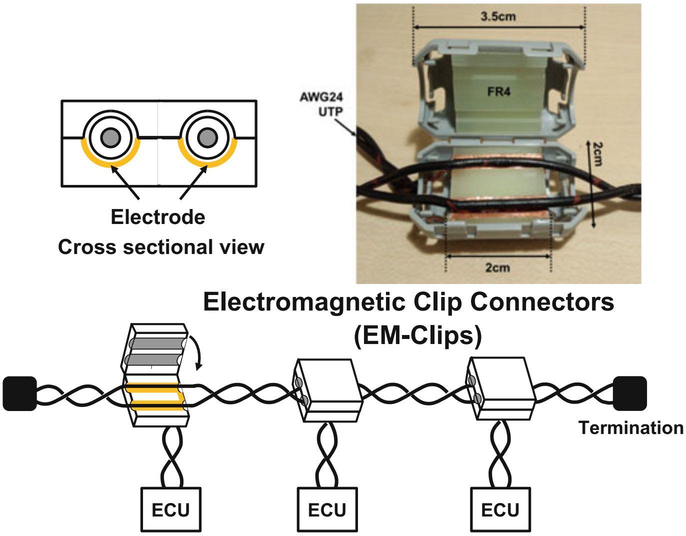


Fig. 21.10 In-vehicle LAN with electromagnetic clip connectors

harness without concern for vibration, so the electronic control units (ECU) can be connected with the minimum amount of wiring. The harness weight can thus be reduced by 30%, including the weight of wires.

21.4 Conclusion

Using wireless interconnection can improve performance, reduce size, and lower costs to an extent not possible with conventional mechanical wire connectors. The TLC wireless connector features impedance matching for high-bandwidth signal transmission, making it suitable for servers and other high-performance IT equipment that can take advantage of the high-speed and high-quality communication that TLC connectors offer. For smartphones and other such handheld devices, this technology also offers speed, compactness, and lower cost. For automobiles and other high-vibration environments, TLC's eliminate power flicker and reduce cost by making the conventional countermeasures unnecessary. Wireless interconnection can also reduce electrical harness weight. The benefits of using TLC connections are summarized in Fig. 21.11.

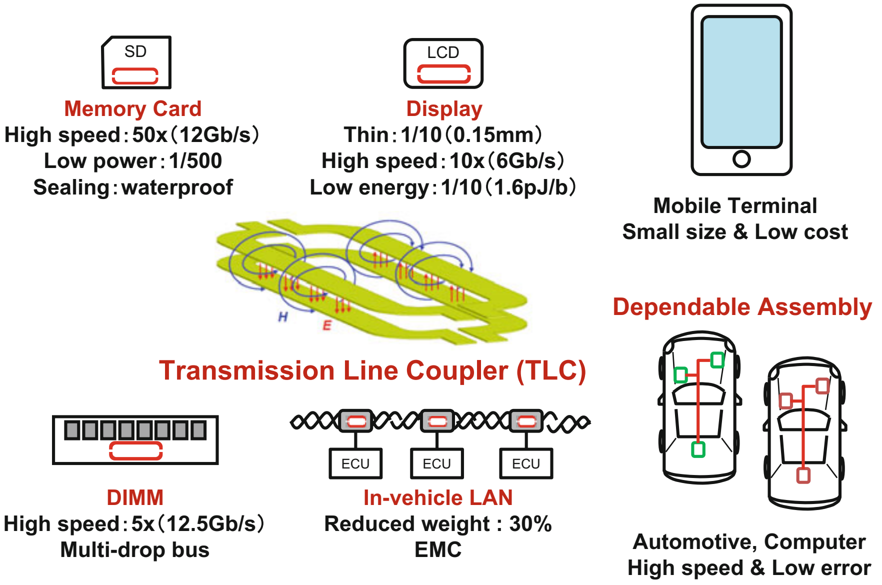


Fig. 21.11 Various applications of TLC

References

1. J. Lee et al., A low-power fully integrated 60 GHz transceiver system with OOK modulation and on-board antenna assembly, in *IEEE International Solid-State Circuits Conference (ISSCC'09). Digest of Technical Papers*, February 2009, pp. 316–317
2. Y. Tanaka et al., A versatile multi-modality serial link, in *IEEE International Solid-State Circuits Conference (ISSCC'12). Digest of Technical Papers*, February 2012, pp. 332–333
3. S. Kawai et al., A 2.5 Gb/s/ch inductive-coupling transceiver for non-contact memory card, in *IEEE International Solid-State Circuits Conference (ISSCC'10). Digest of Technical Papers*, February 2010, pp. 264–265
4. H. Cho et al., A 1.2 Gb/s 3.9 pJ/b, mono-phase pulse-modulation inductive-coupling transceiver for mm-range board-to-board communication, in *IEEE International Solid-State Circuits Conference (ISSCC'13). Digest of Technical Papers*, February 2013, pp. 202–203
5. K. Ikeuchi et al., 500 Mbps, 670 μW/pin capacitively coupled receiver with self reset scheme for wireless connectors, in *IEEE Asian Solid-State Circuits Conference (A-SSCC'08). Digest of Technical Papers*, November 2008, pp. 93–96
6. T. Takeya et al. A 12 Gb/s non-contact interface with coupled transmission lines, in *IEEE International Solid-State Circuits Conference (ISSCC'11). Digest of Technical Papers*, February 2011, pp. 492–493
7. W.-J. Yun et al., A 7 Gb/s/Link non-contact memory module for multi-drop bus system using energy-equipartitioned coupled transmission line, in *IEEE International Solid-State Circuits Conference (ISSCC'12). Digest of Technical Papers*, February 2012, pp. 52–53
8. A. Kosuge et al., A 12.5 Gb/s/Link non-contact multi drop bus system with impedance-matched transmission line couplers and dicode partial-response transceivers, in *Proceedings of the IEEE Custom Integrated Circuits Conference (CICC'12)*, September 2012, pp. 7.9.1–7.9.4

9. W. Mizuhara et al., A 0.15 mm-thick non-contact connector for MIPI using vertical directional coupler, in *IEEE International Solid-State Circuits Conference (ISSCC'13). Digest of Technical Papers*, February 2013, pp. 200–201
10. A. Kosuge et al., An electromagnetic clip connector for in-vehicle LAN to reduce wire harness weight by 30%, in *IEEE International Solid-State Circuits Conference (ISSCC'14). Digest of Technical Papers*, February 2014, pp. 496–497
11. A. Kosuge et al., A 6 Gb/s 6pJ/b 5 mm-distance non-contact interface for modular smartphones using two-fold transmission line coupler and EMC-qualified pulse transceiver, in *IEEE International Solid-State Circuits Conference (ISSCC'15). Digest of Technical Papers*, February 2015, pp. 176–177

Chapter 22
Wireless Power Delivery Resilient Against Loading Variations

Hiroki Ishikuro

Abstract This chapter introduces wireless power delivery systems for battery-less small-size applications. Various kind of new applications such as large volume contactless memory cards or wearable devices will be realized by using wireless power delivery. However, dependability issues should be considered in the wireless power delivery systems for battery-less systems. Small-size low-cost implementation, fast load tracking ability, and reduction of electromagnetic interference (EMI) are typical dependability issues which should be solved. Wireless power delivery technique by inductive coupling is explained at first and several techniques to solve the issues are introduced. For the efficiency improvement, simultaneous power transfer and voltage boosting are tried to eliminate a DC-to-DC converter or charge-pump circuit for data write operation into the flash memory chip. For the fast power control, vector summing of magnetic field and ΔΣ modulated sub-harmonic switching techniques are explained. For the application of large volume SD card size wireless solid-state drive (SSD), these techniques were implemented into the wireless power delivery system using 0.18 μm-CMOS technology and inductor printed on the PCB board. Experiments with vector summing technique demonstrated a voltage boosting up to 16.3 V at 1 W power transfer with 50% power efficiency. The response time against the load change is 35 μs, which is faster than the conventional system by two orders of magnitude. In the experiments with ΔΣ modulated sub-harmonic switching technique, power efficiency was improved at low power transmission and spurious emission was suppressed by 8 dB.

Keywords Wireless power delivery · Inductive coupling · SSD
Fast-tracking · EMI

H. Ishikuro (✉)
Keio University, Yokohama, Japan
e-mail: ishikuro@elec.keio.ac.jp

S. Asai (ed.), *VLSI Design and Test for Systems Dependability*,
https://doi.org/10.1007/978-4-431-56594-9_22

22.1 Applications and Issues of Wireless Power Delivery Systems

Wireless power transfer technology has long history and is put into practical use from 1990s. Battery charging for cordless phone or electrical toothbrush is one of such application and RF-ID tag is another successful application of wireless power delivery. These applications use inductive coupling. In the case of battery charging, strongly coupled inductors are used for watt-class power transfer. For the RF-ID tag, loosely coupled inductors are used and power efficiency is very low. However, the required power is very small and the low efficiency does not become problem. To improve the power efficiency in the weakly coupled system, wireless power transfer which uses magnetic resonance has been proposed [1, 2] and attract much attention for the application of battery charging for electric car. Wireless power transfer using microwave and directional antenna [3] is the other technique, which makes it possible to deliver electric power over a long distance.

Recently large volume nonvolatile memory devices such as solid-state drive (SSD) play more and more important roles in computer system or information appliance. Such devices are connected with the host by wire to transfer the data and power. If the power and data can be transferred by wireless, the connector and cable can be eliminated (Fig. 22.1a). This brings dependability to the system because it can become waterproof and free from contact failure. It also brings flexibility to the system design.

According to the roadmap of SD Association [4], 2T byte volume with bus speed of 312 Mbps is standardized for the specification of future SD card. As described previously, many researches on the wireless power transfer which used inductive coupling [5] or magnetic resonance [1, 2] have been reported. Wireless power transfer standard such as “Qi” [6] has been established and several products have already been in commercial use. In such application, secondary side (receiver side) contains battery and it acts as a buffer which hides rapid secondary side load variation from primary side, hence, fast power control is not required.

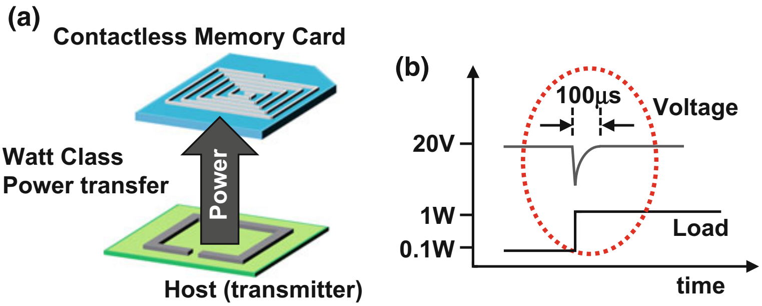


Fig. 22.1 Wireless power delivery for large volume memory card

However, for the application of the wireless memory card, it is not practical to contain a battery in the card. Therefore, the rapid load change in the card may disturb the voltage (Fig. 22.1b) and degrade the circuit operation or device reliability. As used in the RF-ID cards [7], shunt regulator (voltage limiter) can suppress the voltage variation in the card by consuming overloaded power. In the case of RF-ID, because circuits consume only milli-watt order power, the power efficiency is not important. Thus, it is enough to use shunt regulator at secondary side. However, the peak power of the future terra-byte class memory devices becomes watt class and the heat generated in the regulator degrades system reliability. To avoid such problem, high-speed power control is inevitable. Commonly used watt-class wireless power delivery systems, for example, Qi standard contains the battery at secondary side, and rapid load change does not occur. Therefore, these systems usually chose several hundred kHz for switching frequency, which is not sufficient for quick response to load variation. To achieve high-speed power control, MHz band frequency is suited. However, if the wireless power transfer uses MHz band frequency, the allowed frequency band (ISM band Industrial, Scientific and Medical (ISM) band) is narrow (Fig. 22.2) [7], and frequency modulation cannot be used for power control. For example, the available frequency range for the 6.78 MHz band is ±15 kHz and for the 13.56 MHz band is ±7 kHz.

Another requirement in the contactless memory card is a voltage boosting for data write operation. In the flash memory chip, charge-pump circuit is embedded to generate a high voltage. However, charge pump consumes about 60% of power during write operation in NAND flash memory chip [8]. To improve the efficiency, DC-to-DC converter can be used. However, the additional components are required which increases the size and cost of the card.

From the next section, wireless power transfer techniques with voltage boosting which is developed [9, 10] for compact size battery-less applications are introduced. Although the motive application is SD card size wireless memory card, these techniques can be utilized for wide variety of applications such as wearable devices or medical implantable devices.

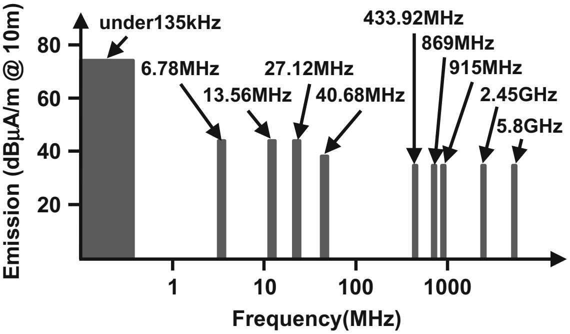


Fig. 22.2 Frequency chart of ISM band

22.2 Wireless Power Delivery by Inductive Coupling

In general, wireless power delivery system by inductive coupling consists of a transmitter, strongly coupled inductors, and a rectifier (Fig. 22.3). The transmitter converts input DC voltage to AC signal by switching transistors. The AC signal drives the transmitting inductor and magnetic field is induced by the AC current in the inductor. In the receiver side, AC voltage is induced in the receiving inductor and the AC voltage is rectified to generate DC output voltage. Since the coupling coefficient between the transmitting and receiving inductor is lower than one (typically 0.5 at most), leakage inductances impede the AC current flow through the inductors. To cancel these leakage inductances, capacitors are usually placed in parallel or in series with the inductors and the resonant frequency is tuned at switching frequency.

For battery charging applications, such as electric toothbrush or recent Qi standard, the switching frequency of several hundred kHz is usually used. Since there is a battery in the receiver side, the load variation is gradual and fast power control is not required for these applications. The transmitting power is controlled by frequency modulation. Since the LC tuned inductors are used, the transmitting power becomes maximum when the switching frequency is set at resonant frequency. If the switching frequency is de-tuned from resonant frequency, the transmitting power is reduced.

As mentioned in the previous section, fast power control is required for watt-class battery-less application. If the MHz band is used for switching frequency, allowed frequency band is very narrow and usual frequency modulation cannot be used for power control. Furthermore, EMI should be suppressed even when the transmitting power is rapidly controlled.

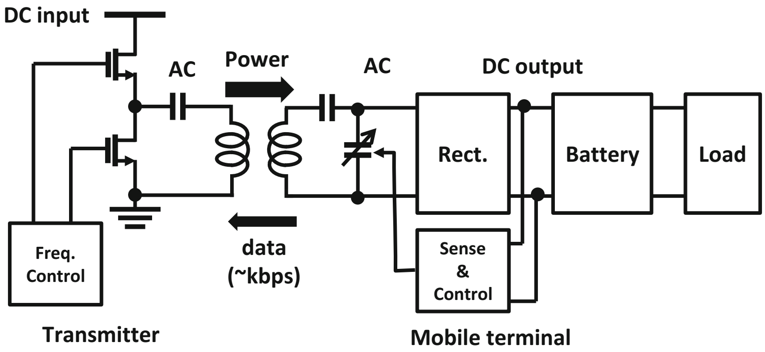


Fig. 22.3 Wireless power delivery system by inductive coupling

22.3 Approach for Power Efficiency Improvement and Size Reduction

In the application of large volume memory card, NAND flash memory requires high voltage during data write operation. Figure 22.4a shows one example to boost the secondary side voltage for this kind of application. As described previously, frequency modulation cannot be used for transmitting power control in the wireless power delivery system which uses MHz band. Therefore, in the primary side, DC-to-DC converter which adjusts input DC voltage should be placed to control the transmitting power. The driver circuit (*TX*) converts the DC to AC current. At secondary side, rectifier converts AC to DC voltage again, and DC-to-DC converter or charge-pump circuit boosts the voltage to required level for data write operation. Total efficiency can be written as,

$$\eta_{Total} = \eta_{DC-DC\ Converter} \times \eta_{TX} \times \eta_{Coil} \times \eta_{Rectifier} \times \eta_{Boost\ Circuit} \tag{22.1}$$

Since every component has a power loss, the total efficiency becomes low. For example, it has been reported that the power efficiency of DC-to-DC converter for controlling input-voltage is about 93% [11]. And, power efficiency of the charge pump for nonvolatile memory decreases with increased ratio of voltage boosting. If voltage boosting ratio is larger than 5, the reported power efficiency of the charge-pump circuit is 53% [12]. Furthermore, if the rectification in the receiver is carried out before voltage boosting, the power loss in the rectifier becomes large because the voltage drop by the diode is relatively large. The rectifier loss can become approximately 25% if the rectifier output voltage is 3.3 V. As a result, Eq. (22.1) becomes

$$\eta_{Total} = 0.93 \times \eta_{TX} \times \eta_{Coil} \times 0.75 \times 0.53 = 0.37 \times \eta_{TX} \times \eta_{Coil}.$$

Furthermore, the DC-to-DC converter or charge pump increases the number of discrete components, cost, and module size.

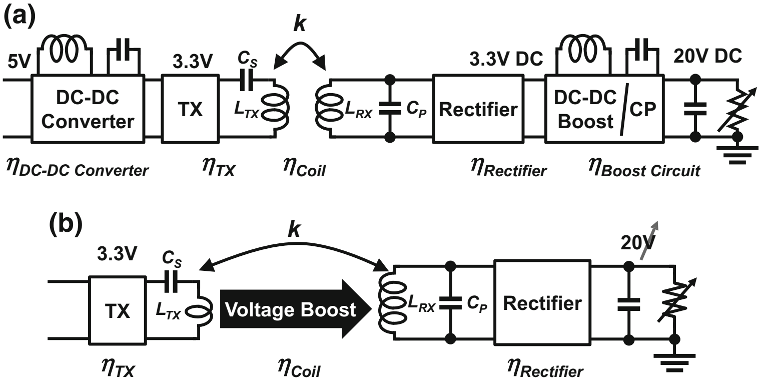


Fig. 22.4 Wireless power delivery system for improved power efficiency and reduced module size

Figure 22.4b shows an architecture to improve the power efficiency and reduce the module size. Instead of voltage boosting by DC-to-DC converter or charge-pump circuit, the secondary side voltage is boosted by using inductors with large winding number ratio between the primary and secondary inductors. The advantage of this approach is the reduced number of components which brings an improved efficiency and therefore, reduced size and cost. The total power efficiency can be given as,

$$\eta_{Total} = \eta_{TX} \times \eta_{Coil} \times \eta_{Rectifier}. \tag{22.2}$$

In this approach, the winding number ratio between the transmitter and receiver inductors becomes large for voltage boosting. Thus, it is thought that transmission efficiency falls about several percent. However, since the DC-to-DC converter and charge pump can be removed, overall efficiency improves. Moreover, in rectifier circuit, the relative voltage drop by the diode is small because the voltage is boosted prior to the rectification. The loss by the rectifier can be reduced to 7.3%. Therefore, the Eq. (22.2) can be rewritten as

$$\eta_{Total} = \eta_{TX} \times \eta_{Coil} \times \eta_{Rectifier} = \eta_{TX} \times \eta_{Coil} \times 0.93.$$

The issue of this approach is that some techniques to rapidly control the transmitting power is required without using DC-to-DC converter or frequency modulation. Several kinds of techniques can be used to solve this issue and two techniques are introduced in the next section.

22.4 Fast Load Tracking and EMI Reduction Technique

22.4.1 Vector Summation of Magnetic Fields

Figure 22.5 shows a transmitting power control by vector summing of magnetic fields [9]. The transmitter consists of two drivers and coils which forms two half-bridge configurations in this figure. The phase difference between the switching clocks in each driver introduces the phase difference between the current in each inductor. The induced magnetic fields are summed in the secondary inductor. The power contribution from each primary coils (L_{TX1} and L_{TX2}) is P_O and $P_O\, e^{j\theta}$, respectively and secondary power can be expressed as,

$$Power = P_O \times (1 + \cos\theta). \tag{22.3}$$

Same kind of power control technique which uses a full-bridge structure with phase shift PWM has been proposed [13]. By shifting the phase of the switching clocks, the duty ratio when the current flow through the transmitting inductor can be changed and the transmitting power can be controlled. However, the current flows

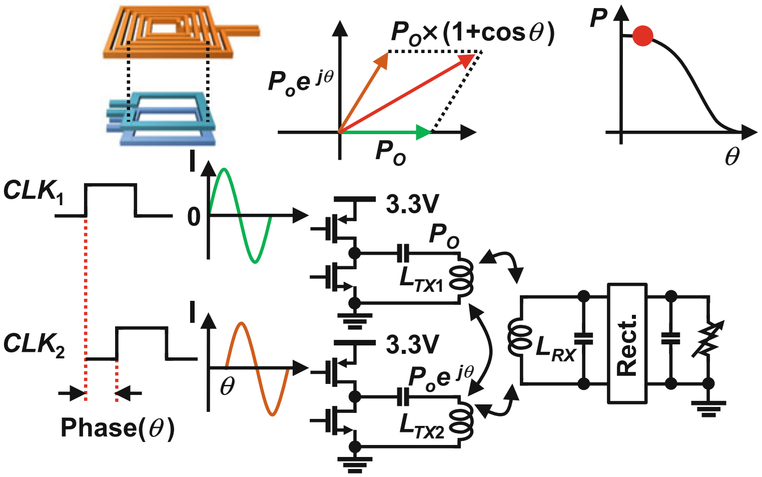


Fig. 22.5 Power control by vector summing of magnetic fields

through both PMOS and NMOS at the same time. Since the voltage is boosted by using large winding number ratio, the primary inductor for the application of wireless memory card has only one turn. Therefore, parasitic resistances of MOSFETs bring severe power loss. In the half-bridge configuration, current flows through only PMOS or NMOS at the same time, thus, reduces power loss. Furthermore, using two half-bridge configurations reduces the required current in one transistor to half. In standard CMOS technology, it is difficult to transfer high power because large current becomes stress for MOSFET and degrades its characteristics. Therefore current reduction in one transistor becomes advantage.

22.4.2 Sub-harmonic Switching Technique

The other technique for the fast transmitting power control is switching frequency control between fundamental and sub-harmonic of resonant frequency [10].

Figure 22.6 shows the operation principle of the power control by sub-harmonic switching. Both the transmitter and receiver use LC resonant circuits to improve the power efficiency. To transmit maximum power, the output driver is driven by a clock signal at f_{res} (resonant switching mode) (Fig. 22.6a). When the high-side switch is on (ϕ_1), the current begins to flow into the inductor and converted to the magnetic field energy. Since the LC resonance is used, the inductor current begins to decrease at quarter cycle and becomes zero at half cycle of f_{res}. At this moment (ϕ_2), the high-side switch is off and low-side switch is on. The current flows through the loop formed by an inductor, capacitor, and low-side switch. In this sequence, rectangular voltage waveform whose fundamental frequency is same as

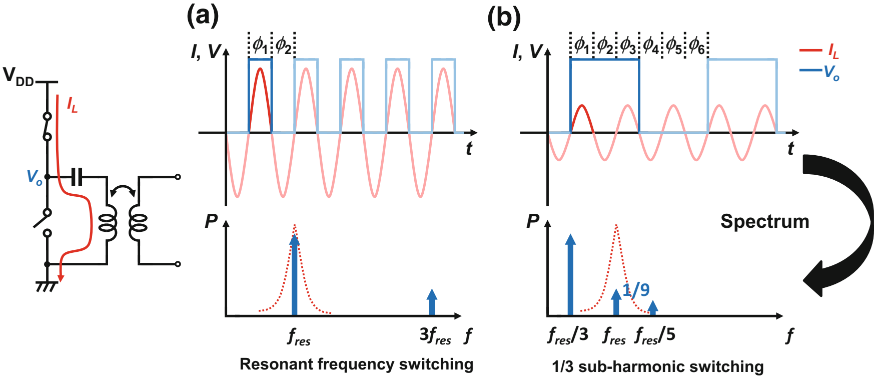


Fig. 22.6 Transmitting power control by resonant/sub-harmonic switching

f_{res} is applied to LC resonant circuit. Since the conductance of the LC circuit is maximum at resonant frequency and becomes small at the other frequency, the current flow through the LC circuit is in proportion to the fundamental component of the rectangular voltage form. The harmonic components of the rectangular waveform are suppressed.

If the switching frequency is set at $f_{res}/3$ (sub-harmonic switching mode) (Fig. 22.6b), the power is transferred in the following way. From phase ϕ_1 to ϕ_3, the high-side switch is on and low-side switch is off. During the phase ϕ_1, the current flows from power supply to the inductor. Then, at phase ϕ_2, the current flows back to the power supply, and at ϕ_3, the current flows again from the power supply. From phase ϕ_4 to ϕ_6, the high-side switch is off and low-side switch is on. The current flows back and forth in the loop formed by the inductor, capacitor, and low-side switch. The energy dissipated by the receiver is refilled at every three cycles of f_{res} and transmitting power can be reduced. This can be explained in the frequency domain in the following way. The fundamental component of the rectangular voltage waveform cannot excite the current in the LC circuit because the conductance of the LC circuit at this frequency is small. On the other hand, the third harmonics of the rectangular waveform coincides with the resonant frequency of the LC circuit and excite the current in the LC circuit. Since the voltage amplitude of the third harmonics is one-third of the fundamental components, the transmitted power is one-ninth of that of the resonant switching.

By changing the ratio between the switching by f_{res} and $f_{res}/3$, the transmitted power can be continuously controlled. Different from FM or PWM, the frequency of the current flowing through the inductor is close to f_{res} and zero current switching is achieved in both the switching mode. This dramatically reduces the unwanted spurious emission.

To further reduce the spurious emission, a ΔΣ modulator is adopted to generate the control signal to change between the resonant switching and sub-harmonic switching mode as shown in Figs. 22.7 and 22.8.

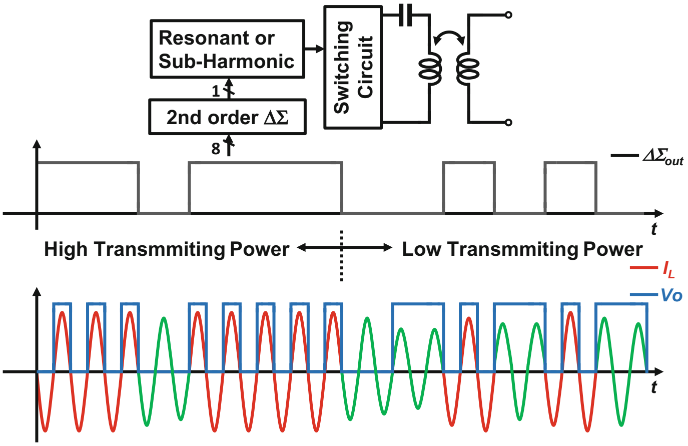


Fig. 22.7 EMI reduction by ΔΣ modulation of resonant and sub-harmonic switching

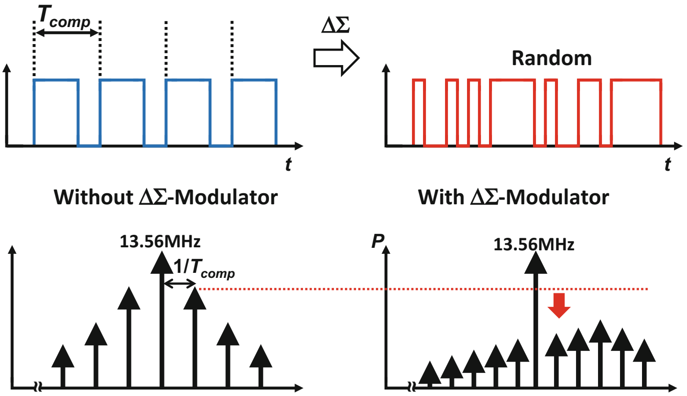


Fig. 22.8 Spur spreading by ΔΣ modulation of resonant and sub-harmonic switching

22.5 Wireless Power Delivery System Implementation

A. System Overview

Figure 22.9 shows block diagram of the developed power transfer system for large volume memory card. The metal layers in the PCB are used for transmitting and receiving inductor. Phase difference between the switching clocks for primary coils L_{TX1} and L_{TX2} is controlled by Delay Locked Loop (DLL). Then, dead time generator inserts the non-overlap phase between the switching clocks for PMOS and NMOS to prevent V_{DD} and GND from being shorted. The resonant frequency of the primary inductors is tuned by series LC connection.

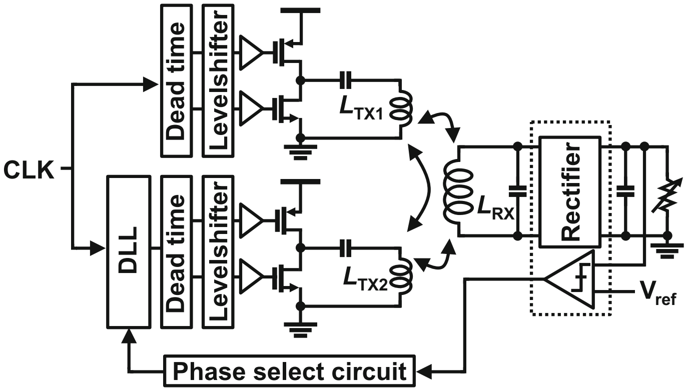


Fig. 22.9 System block diagram of the wireless power delivery for large volume memory card

Considering the SD card size, diameters of the transmitting and receiving inductors are about 20 mm. The turn number of primary and secondary inductors are one and eight, respectively. The self-inductance of primary (L_{TX}) and secondary inductor (L_{RX}) are 41 nH and 2.58 μH, respectively. The distance between the primary and secondary inductors are several millimeter.

In the secondary side, parallel LC connection is adopted to tune the resonant frequency. Since the parallel connected LC circuit acts as current source at resonant frequency, high voltage can be obtained, making it suitable for voltage boosting. The gate cross-coupled rectifier is used to convert from AC to DC voltage. The generated DC voltage is compared with the reference voltage and fed back to the DLL for power control.

B. Series-Parallel Resonance Link Design

At primary side, transmitting inductors L_{TX1} and L_{TX2} are the same size. On the other hand, the distances between the primary and secondary inductors are much longer than the distance between each primary inductors. To improve the power transfer efficiency, reactance component of each leakage inductance should be canceled by capacitors at switching frequency.

As explained in Fig. 22.2, several frequencies can be used for wireless power delivery as ISM band. Considering that the tradeoff between the response speed, components size, and power transfer efficiency, the switching frequency of 6.78 MHz or 13.56 MHz becomes a candidate for this application. If the higher switching frequency is chosen, the response speed for power control can be improved and component size can be decreased. However, the power transfer efficiency degrades by the charge and discharge through parasitic capacitance and resistance of MOSFETs. If lower frequency is chosen, the power efficiency can be increased. In this work, placing the emphasis on the efficiency, the resonant frequency of primary and secondary inductors are tuned at 6.78 MHz. The capacitances for resonance in the primary side are determined as 14 and 13 nF, and secondary side is determined as 220 pF.

Using Electromagnetic field solver simulator, each parasitic resistor is obtained. The primary side's parasitic resistance (R_{main1}, R_{main2}) is 70 mΩ, while the secondary side (R_{main3}) is 3 Ω.

C. Rectifier

Gate cross-coupled rectifier [14] is adopted. Figure 22.10 shows rectifier circuit. Thick oxide lateral-diffused MOS (LDMOS) with maximum rated voltage of 32 V are used. At secondary side, induced voltage between the coil terminals is high because of voltage boosting, V_{GS} of gate cross-coupled NMOS becomes large and on-resistance of NMOS is low. As a result, V_{DS} of NMOS is also low and parasitic diode in NMOS does not turn on. Therefore, no additional dynamic bulk regulation transistors are necessary for switch NMOS, which improves rectifier efficiency. Reducing the dropout voltage by PMOS of the rectifier improves power efficiency in the rectifier circuit and increases the rectified dc voltage V_{rect_out}.

To minimize the dropout voltage and improve power efficiency, the W/L ratio is increased as large as the chip area permitted.

E. Feedback Control

In this system, bang-bang control is adopted. At initial state, to prevent break down of the MOSFETs and device connected to this wireless power delivery system, phase difference between the switching clocks for primary coils is start from 180° (minimum transmitting power). Then, the rectified output voltage is compared with the reference voltage and fed back to the phase select circuit of the DLL.

During the system start-up, the output voltage of the rectifier is lower than the target voltage. At first, the counter is set at its maximum count level. To increase the transmitting power, the phase select circuit decrements the counter and reduce the phase difference. The counter and phase difference is reduced every cycle until

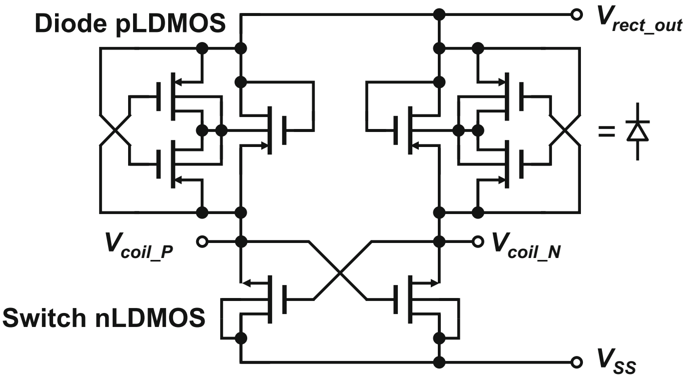


Fig. 22.10 Rectifier circuit in the secondary side

the output voltage reaches the target voltage. Once the output voltage exceeds the target voltage, the phase select circuit increments the counter and increase the phase difference. As a result, the transmitted power and output voltage of the rectifier is decreased. Since the phase control signal is updated at every cycle of clock, the transmitter can reach its maximum power setting within 32 clock cycles from start-up.

When load variation occurs, the output voltage of the rectified changes. When the power consumption of the load decreases, the required power reduces. The phase control circuit increases the phase difference to reduce the transmitting power. On the other hand, if the power consumption of the load increases, the phase control circuit reduces the phase difference to increase the transmitting power. As a result, the output voltage becomes constant value against the load variation.

22.6 Experimental Results

Figure 22.11a, b are power transceiver modules and Fig. 22.12a, b are test chip microphotographs. An 0.18 μm-CMOS process with high-voltage LDMOS option was used. Low voltage (1.8 V) MOSFETs are used for DLL and other control circuit. Medium voltage (5 V) MOSFETs are used as switching driver circuit and high-voltage (32 V) LDMOSFETs are used in secondary circuit. The inductor size in the PCB board is 20 mm × 20 mm. The chip size of both the transmitter and rectifier are 2.5 mm × 2.5 mm.

In the experiment, distance between the primary and secondary inductors is set at 1 mm. Switching frequency is 6.78 MHz.

Figure 22.13 shows the relation between the receiver power and clock phase of the DLL. 50% efficiency and 1 W power delivery at 266 Ω load is achieved. Power can be controlled while keeping the efficiency about 40% across the range of max-to-half power. Figure 22.14 shows the output voltage with and without power

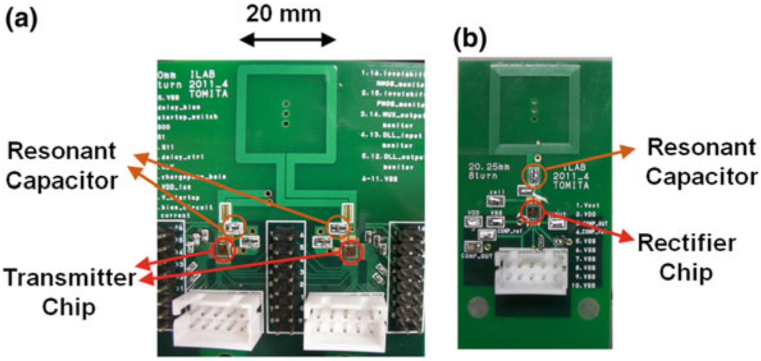


Fig. 22.11 Power transmitter and receiver module

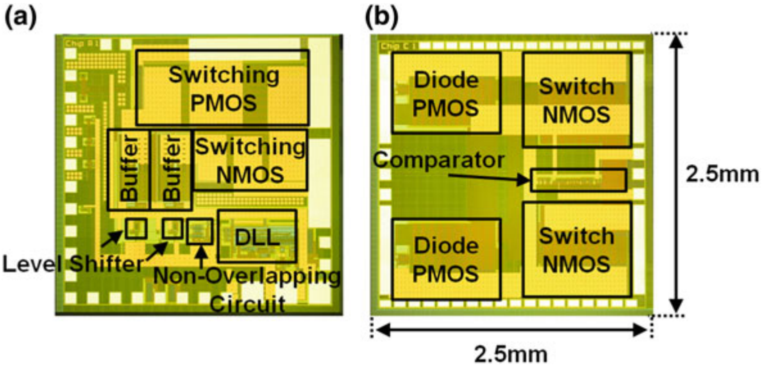


Fig. 22.12 Fabricated test chip in 0.18 μm-CMOS with high-voltage LDMOS option, **a** transmitter chip, **b** rectifier chip

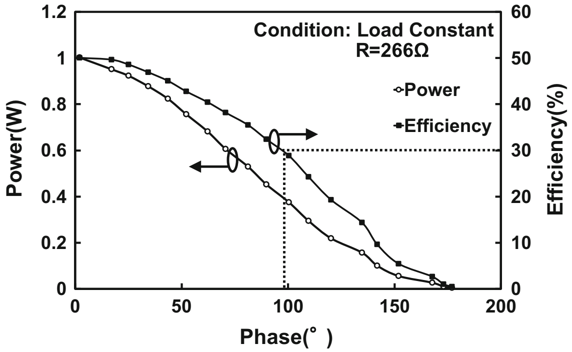


Fig. 22.13 Relation between receiver power and phase difference of switching clocks of two transmitters

control when the secondary side load is changed. By controlling the transmitting power, the secondary side voltage can be stabilized.

Figure 22.15 shows the measured transient response of the power control loop. Even when the secondary side load is changed from 71 mW to 1 W, the voltage drop is only 2.7% and it takes only 35 μs to recover the output voltage. This response time about 100 times faster than that in the wireless power transceiver for "Qi" standard.

In the previous experiments which used vector summing of two transmitters, the power efficiency becomes low when the transmitted power is small. Most of the time in the operation, memory card consumes power much lower than the peak power. Therefore, power efficiency at lower transmitting power is also important.

The other experiments which used power control by ΔΣ modulated switching between fundamental and sub-harmonic resonant frequency was carried out. In this

Fig. 22.14 Voltage regulation by vector summing of two transmitters

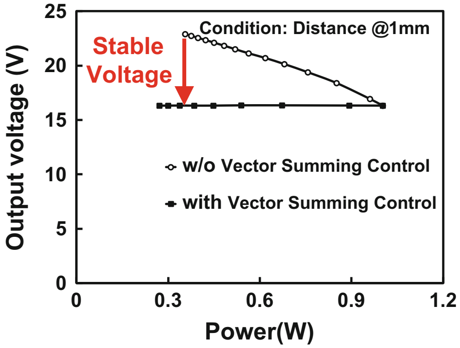
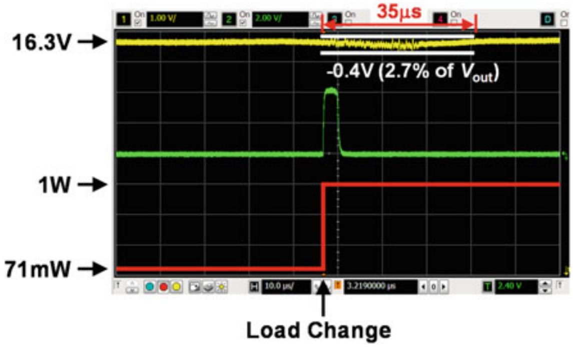


Fig. 22.15 Transient response when the load is changed from 71 mW to 1 W



experiment, only one transmitter was used. The power supply voltage is 1.8 V for controller and 3.3 V for class-D amplifier. The middle voltage (5 V) MOSFETs are used for level shifter and class-D amplifier. LC resonant circuit was tuned at 13.56 MHz. The clock frequency is switched between 13.56 MHz (fundamental) and 4.52 MHz (sub-harmonic) for resonant switching and sub-harmonic switching, respectively. At the output of the rectifier, a comparator is placed to detect the rectified voltage. All the circuits in receiver side are designed using high-voltage LDMOS with rated voltage of 32 V. The off-chip capacitor to remove the ripple has capacitance of 33 nF. The comparator output signal is fed back to the loop filter and ΔΣ modulator in the transmitter side.

Figure 22.16 shows the measured relation between the transmitted power and total power transmission efficiency as a function of power setting code. In this experiment, the distance between the transmitter coil and receiver coil is set at 5 mm. Maximum power of 0.52 W can be delivered with an efficiency of 50%. The transmitted power range is wider than one order of magnitude. Compared with the previously mentioned experimental results (Fig. 22.13) the relation between the transmitted power and setting code has good linearity which enables the simple design of feedback loop. Furthermore, reasonable efficiencies are maintained over the power setting.

Fig. 22.16 Power setting code versus transferred power and total power efficiency

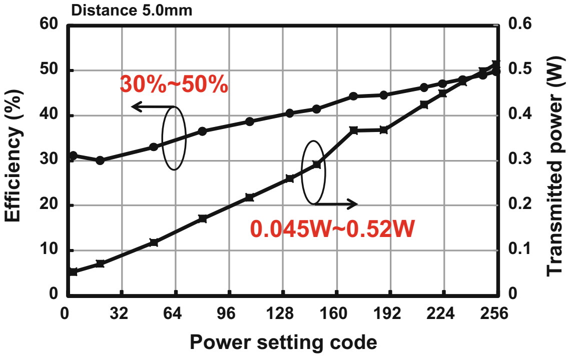


Fig. 22.17 Spurious emission level as a function of power setting code

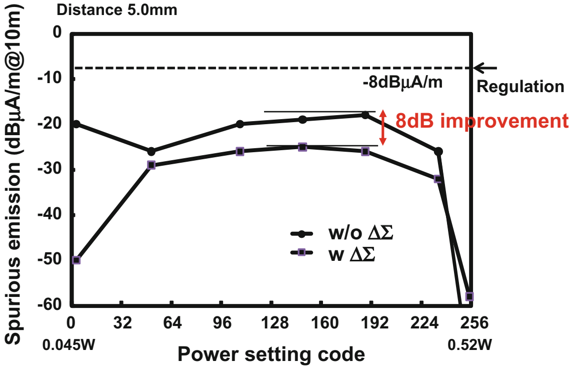


Figure 22.17 shows the spurious emission level from the developed wireless power delivery system. For the comparison, the spurious emission levels with and without ΔΣ modulator are plotted. In each case, the worst level spurious tone is chosen. The ΔΣ modulator suppresses the spurious tone by 8 dB and spurious tone meets the regulation with enough margin.

22.7 Summary

Wireless power delivery system for battery-less application was introduced. As dependability issues for this kind of power delivery system, the requirement of fast load tracking ability and EMI suppression were discussed. To realize the fast load tracking and EMI suppression, rapid power control techniques with vector summing of magnetic field and ΔΣ modulated sub-harmonic resonant frequency switching were introduced.

Aiming the application of large volume SD card size wireless memory card (SSD), voltage boosting wireless power transfer system with the above-mentioned techniques were developed using 0.18 μm-CMOS and printed inductors in PCB board. The size of the inductors are 20 mm × 20 mm and test transceiver chip is 2.5 mm × 2.5 mm. Experiments with vector summing technique demonstrated a voltage boosting up to 16.3 V at 1 W power transfer with 50% power efficiency. The response time against the load change is 35 μs which is faster than the conventional system by two orders of magnitude. In the experiments with ΔΣ modulated sub-harmonic switching technique, power efficiency was improved at low power transmission and spurious emission was suppressed by 8 dB.

References

1. A. Kurs, A. Karalis, R. Moffatt, J.D. Joannopoulos, P. Fisher, M. Soljačić, Wireless power transfer via strongly coupled magnetic resonances. Science **317**, 83 (2007)
2. T.C. Beh, T. Imura, M. Kato, Y. Hori, Basic study of improving efficiency of wireless power transfer via magnetic resonance coupling based on impedance matching, in *IEEE International Symposium on Industrial Electronics Dig* July, 2010, pp. 2011–2016
3. R.M. Dickinson, Power in the sky: requirements for microwave wireless power beamers for powering high-altitude platforms. IEEE Microwave Mag. **14**(2), 36–47 (2013)
4. SD Association, https://www.sdcard.org/home/
5. A. Radecki, H. Chung, Y. Yoshida, N. Miura, T. Shidei, H. Ishikuro, T. Kuroda, 6W/25mm^2 inductive power transfer for non-contact wafer-level testing, in *IEEE ISSCC Dig,* Feb, 2011, pp. 230–232
6. Wireless Power Consortium, *Qi System Description Wireless Power Transfer Volume I: Low Power Part 1: Interface Definition Version 1.0.2,* April, 2011, pp. 1–50
7. K. Finkenzeller, *RFID HANDBOOK*, 2nd edn. (Translated by R. Waddington), Munich/FRG, original German language published by Carl Hanser Verlag, The Atrium/Southern Gate/Chichester/West Sussex PO19 8SQ/England (Wiley, 2003), pp. 161–181
8. K. Ishida, T. Yasufuku, S. Miyamoto, H. Nakai, M. Takamiya, T. Sakurai, K. Takeuchi, 1.8V Low-transient-energy adaptive program-voltage generator based on boost converter for 3D-integrated NAND flash SSD. IEEE J. Solid-State Circuits **46**(6), 1478–1487 (2011)
9. K. Tomita, R. Shinoda, T. Kuroda, H. Ishikuro, 1W 3.3V-to-16.3V Boosting wireless power transfer circuits with vector summing power controller. IEEE J. Solid-State Circuits **47**(11), 2576–2585 (2012)
10. R. Shinoda, K. Tomita, Y. Hasegawa, H. Ishikuro, Voltage-boosting wireless power delivery system with fast load tracker by ΔΣ-modulated sub-harmonic resonant switching, in *IEEE International Solid-State Circuits Conference (ISSCC)* Feb, 2012, pp. 288–290
11. C. Zheng, D. Ma, A 10-MHz green-mode automatic reconfigurable switching converter for DVS-enabled VLSI systems. IEEE J. Solid-State Circuits **46**(6), 1464–1477 (2011)
12. A. Richelli, L. Mensi, L. Colalongo, P.L. Rolandi, Z.M. Kovacs-Vajna, A 1.2-to-8V Charge-pump with improved power efficiency for non-volatile memories, in *IEEE ISSCC Dig*, Feb, 2007, pp. 522–619
13. T. Ishii, H. Kakehashi, H. Ogasawara, T. Ninomiya, Piezoelectric-transformer inverter with full-bridge phase-shift control scheme, in *Institute of Electronics Information and Communication Engineers Dig*, Nov, 1999, pp. 45–51
14. M. Ghovanloo, K. Najafi, Fully integrated wideband high-current rectifiers for inductively powered devices. IEEE J. Solid-State Circuits **39**(11), 1976–1984 (2004)

Chapter 23
Extended Dependable Air: Use of Satellites in Boosting Dependability of Public Wireless Communications

Kazuo Tsubouchi, Suguru Kameda, Hiroshi Oguma, Akinori Taira, Noriharu Suematsu and Tadashi Takagi

Abstract We propose "Extended Dependable Air" as a highly reliable wireless network. Extended Dependable Air can be used in the "3S" areas: space, surface, and sea. For the implementation of the Extended Dependable Air, two key technologies using satellite systems such as the Quasi-Zenith Satellite System (QZSS) and the Global Positioning System (GPS) are proposed; One is a QZSS Spread Spectrum Code Division Multiple Access (SS-CDMA) short-message communication system, and the other is a heterogeneous wireless system with a network selection scheme using positioning information. The former, the QZSS SS-CDMA short-message communication system, is proposed for large-scale disaster relief. The target capacity of the proposed system is the transmission of at least three million message data per hour. Because this method provides high-density user multiplexing using long spread codes in the uplink, highly accurate timing and frequency synchronization among all terminals is the most important issue. SS-CDMA ensures the use of QZSS positioning signals and maintains the orthogonality in the time and frequency domains among all the codes transmitted from terminals. The latter, the heterogeneous wireless systems, are candidates for achieving a large capacity in next-generation mobile communication systems. In this section, we propose a cell selection scheme for data traffic optimization in heterogeneous wireless systems. The proposed scheme uses high-accuracy positioning information and the average signal strength for cell selection. Using positioning information, users can select a cell with the highest

K. Tsubouchi (✉) · S. Kameda · A. Taira · N. Suematsu · T. Takagi
Tohoku University, Sendai, Japan
e-mail: tsubo@riec.tohoku.ac.jp

S. Kameda
e-mail: kameda@riec.tohoku.ac.jp

N. Suematsu
e-mail: suematsu@riec.tohoku.ac.jp

T. Takagi
e-mail: t-takagi@riec.tohoku.ac.jp

H. Oguma
National Institute of Technology, Toyama College, Toyama, Japan
e-mail: oguma@nc-toyama.ac.jp

S. Asai (ed.), *VLSI Design and Test for Systems Dependability*,
https://doi.org/10.1007/978-4-431-56594-9_23

channel quality quickly and easily. It is considered that the proposed scheme will be useful for optimizing data traffic offloading in heterogeneous wireless networks.

Keywords Quasi-Zenith Satellite System (QZSS) · Global Positioning System (GPS) · Spread Spectrum Code Division Multiple Access (SS-CDMA) Heterogeneous wireless system · Synchronization

23.1 3S Network: For Space, Surface, and Sea

In recent years, communication equipment using wireless communication methods and user data traffic have been increasing with the progress of wireless communication technology. Next-generation communication systems should have the flexibility to provide various types of communication schemes from broadband visual applications to machine-to-machine (M2M) and low-data-rate sensor networks. In addition, reliability and dependability are also important factors. In particular, the social infrastructure with a universal standard clock will have ultrahigh reliability.

To achieve flexibility and dependability, an integrated heterogeneous network consisting of multiple disparate systems with different characteristics may be a major approach. In Chap. 7, we proposed Dependable Air, which performs integrated operations using “surface” communications with a wireless personal area network (WPAN), a wireless local area network (WLAN), and a mobile broadband wireless access (MBWA).

In this chapter, we propose “Extended Dependable Air” as a highly reliable wireless network [1]. Figure 23.1 shows the concept of Extended Dependable Air. Extended Dependable Air can be used in the “3S” areas: space, surface, and sea.

First “S”—Space In the case of a major disaster, the terrestrial infrastructure may have been seriously damaged. Satellite communication is expected to ensure a minimum level of reliable connection. In particular, the Quasi-Zenith Satellite System (QZSS), which is composed of one or more geostationary Earth orbit (GEO) satellites and multiple Quasi-Zenith Satellites (QZSs), can provide a continuous and accurate positioning service even in mountains and urban canyons, where the signals from existing Global Positioning System (GPS) satellites cannot be captured. The first QZS, “Michibiki”, which was launched in November 2010, is in operation and its enhanced GPS performance has been evaluated. Since the Great East Japan Earthquake in 2011, it has been discussed whether the QZSS should have some disaster response features such as safety confirmation and evacuation guidance. In the 2011 disaster, terrestrial infrastructure was seriously damaged by the huge earthquake and tsunami. Several days were needed to confirm the safety of evacuees, and the disappearance of many ships and cars caused delays in recovery and reconstruction. To resolve these issues, a location and two-way short-message communication service using QZSS has attracted interest. In September 2012, the Japanese cabinet office announced that these services

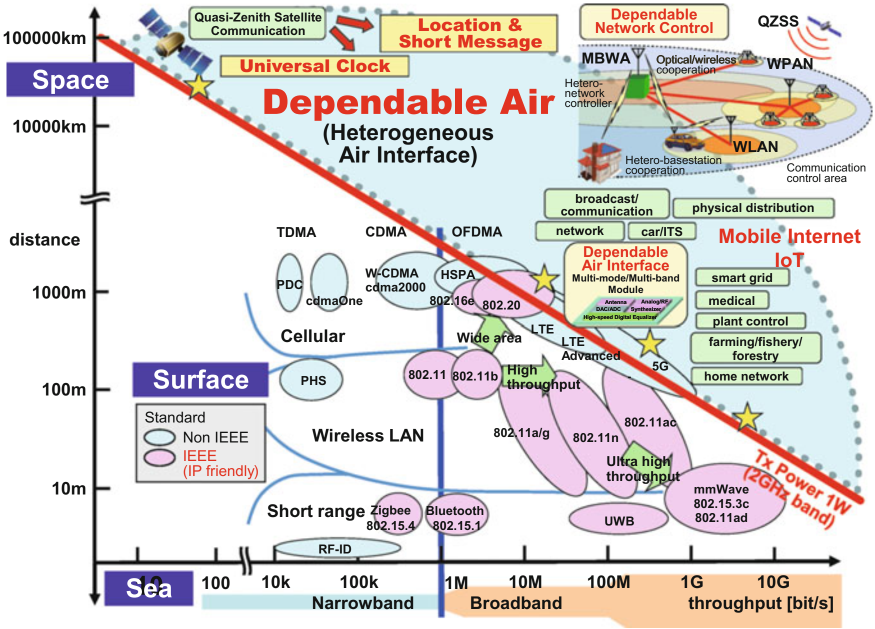


Fig. 23.1 Concept of Extended Dependable Air. There is a restriction (red solid line), which is plotted by assuming an output power of 1 W at 2 GHz from mobile terminals. A trade-off relationship exists between the throughput and cell size. To overcome this restriction and to realize both higher throughput and a larger cell size simultaneously, we have proposed Extended Dependable Air, which consists of a number of cooperating heterogeneous wireless systems. Extended Dependable Air can be used in the "3S" areas: space, surface, and sea

would be implemented in QZSS. Note that, in this system, each terminal with 1 W transmission power can communicate data at a rate of over 100 bit/s to satellites over 36,000 km away, allowing it to simultaneously realize the flexibility.

Second "S"—Surface Dependable Air consists of various heterogeneous wireless systems that are sufficiently and seamlessly connected according to the link conditions to realize greater communication capacity, a higher throughput, and better link connectivity. Moreover, Extended Dependable Air will realize ultrahigh-reliability wireless systems by using a universal standard clock. All base stations and mobile terminals will have a standard clock (with nanosecond precision) and provide highly precise positional information (with centimeter resolution) by receiving clock signals from QZSS and GPS.

Third "S"—Sea In the near future, the demand for marine communication will increase. Satellite communication is a means of communicating among land and ship terminals. Moreover, underwater communication is an important function in marine communication.

In this chapter, two technologies using QZSS that are employed to realize Extended Dependable Air will be described.

23.2 SS-CDMA: A Proposal for Disaster Message Exchange

Two-way short-message communication will be realized using personal terminals or car navigation systems. Thus, we have to establish direct long-distance access between terminals and satellites with 1 W transmission power and an omnidirectional antenna. We have proposed Spread Spectrum Code Division Multiple Access (SS-CDMA) method, which exhibits high channel gain and can accommodate several million users using long spread codes and a CDMA scheme [1–6].

Because this method provides high-density user multiplexing using long spread codes in the uplink, highly accurate timing and frequency synchronization among all terminals is the most important issue. SS-CDMA ensures this by using QZSS positioning signals and maintains the orthogonality in the time and frequency domains among all the codes transmitted from terminals.

23.2.1 SS-CDMA Method Using QZSS

23.2.1.1 Outline of SS-CDMA

Figure 23.2 shows a schematic image of the SS-CDMA system. Positioning signals are broadcast from a QZS and GPS. Each terminal can calculate its own location and time precisely and synchronize its own clock and frequency to those of the QZS. In this system, the frame length is about 300 bits. A frame includes control signals, location information, and a short message. When message data are generated, the terminal spreads the modulated data with the assigned SS code and transmits it in sync with other terminals. The uplink signal is reflected at satellite to a hub station, where despreading and demodulation processes are performed. To accommodate several million terminals for emergency use, we have to set a very high multiplexing rate. Thus, maintaining orthogonality among SS codes is very important. Because of the large round-trip delay, the synchronization scheme must be based on a feed-forward concept. Figure 23.3 presents the block diagram of an SS-CDMA terminal. Each terminal adjusts the transmit timing and carrier frequency using the location and timing information derived from positioning signals from satellites.

23.2.1.2 Example of Channel Design

Table 23.1 shows an example of channel design parameters we assumed to evaluate the SS-CDMA system. At present, these parameters have not been authorized. The satellite achieves a 35 dBi reception gain using a 2-m-diameter parabolic antenna. We assume a nondirectional antenna with a gain of −4 dBi on terminals. Channel bandwidth of 3 MHz and 20% roll-off (i.e., an equivalent noise bandwidth of 2.24 MHz) are assumed. We can derive the reception S/N at the satellite using a transmission power of 1 W as follows.

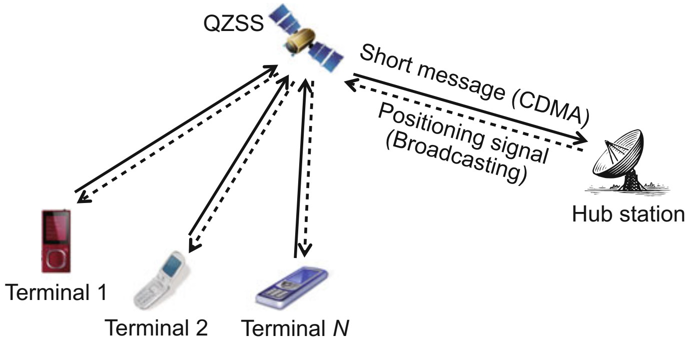


Fig. 23.2 Configuration of SS-CDMA communication system. Positioning signals are broadcast from QZS and GPS. Each terminal can calculate its own location and time precisely and synchronize its own clock and frequency to those of QZS. The system exhibits high channel gain and can accommodate several million users using long spread codes and a CDMA scheme

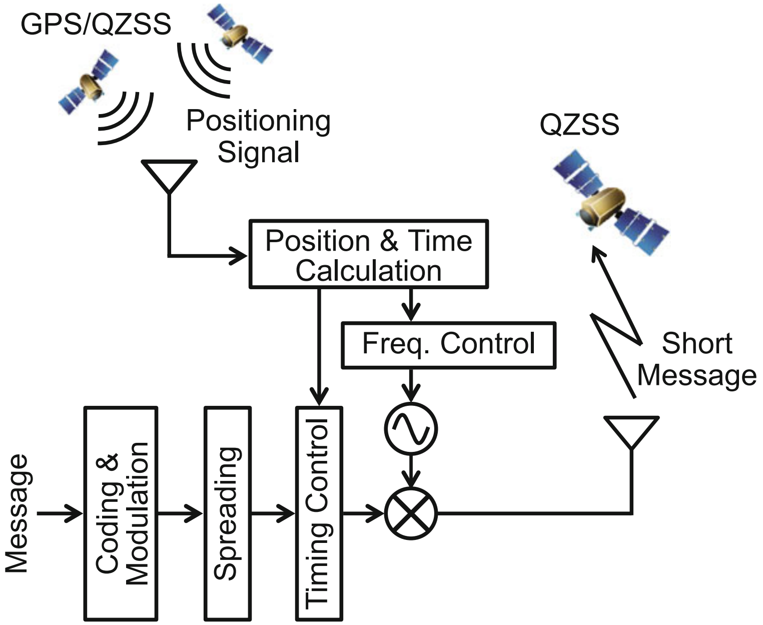


Fig. 23.3 Block diagram of SS-CDMA terminal. Each terminal adjusts the transmit timing and carrier frequency using the location and timing information derived from positioning signals from satellites (QZS and GPS)

Table 23.1 Channel design parameters of SS-CDMA

Distance of transmission	$d = 39{,}000$ km
Carrier frequency	$f_c = 2.075$ GHz
Signal bandwidth	W = 2.24 MHz
Transmission power	$A = 30$ dBm
Terminal antenna gain	$B = -4$ dBi
Path loss (free space)	$C = 190.6$ dB
Fading margin	$D = 8$ dB
Satellite antenna gain	$E = 35$ dBi
Spreading gain	G_s
Noise factor (satellite)	$F = 5$ dB
Temperature (at receiver)	$T = 300$ K
Required S/N (BPSK $R = 1/2$)	8 dB

$$\begin{aligned} S &= A + B - C - D + E + G_s \ \text{[dB]} \\ &= 30.0 - 4.0 - 190.6 - 8.0 + 35.0 + G_s \ \text{[dB]} \\ &= -137.6 + G_s \ \text{[dB]} \end{aligned} \tag{23.1}$$

$$\begin{aligned} N &= FkTW \\ &= -173.8 + 5.0 + 63.4 = -105.4 \ \text{[dB]} \end{aligned} \tag{23.2}$$

$$S/N = -137.6 + 105.4 + G_s = -32.2 + G_s \ \text{[dB]} \tag{23.3}$$

If the required S/N is 8 dB, the spreading gain G_s must be 40 dB (the spreading code length is 10,000). The SS-CDMA system aims to achieve multiplexing for 1000 to 10,000 users using a spreading code whose length is 10,000. We adopted the "accommodation rate" as an efficiency indicator, which is defined as the number of multiplexing users over a spreading code length. The users assigned to the same group transmit messages at the same time using a "time slot". One frame consists of multiple time slots and contains several million users.

23.2.1.3 Positioning Scheme Using QZSS

Figure 23.4 illustrates the high-accuracy positioning system using QZSS. QZS broadcasts positioning signals of not only L1 coarse/acquisition (L1-C/A), which is one of the basic GPS signals for civilian use, but also L1 submeter-class augmentation with integrity function (L1-SAIF), which enhance the positioning performance. In Japan, the Geospatial Information Authority of Japan (GSI) operates GPS Earth Observation Network (GEONET), which contains over 1200 reference stations to detect the measurement error of GPS signals at each location. The error is generated by many factors, such as tropospheric weather conditions, conditions of the ionosphere, and fluctuation in the satellite orbit. L1-SAIF contains the information used to correct these errors and is broadcast from QZS via the QZSS control station. The enhanced

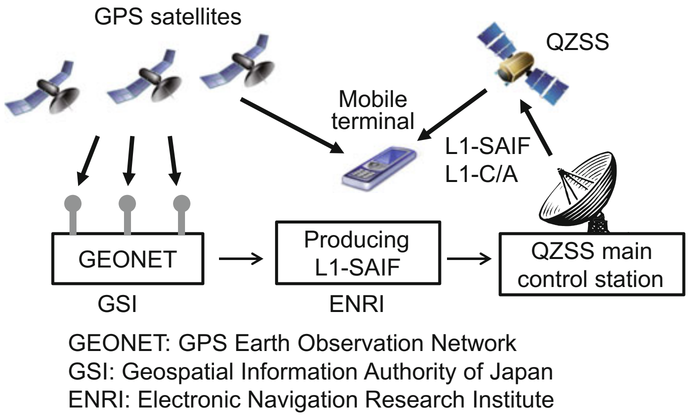

GPS satellites
QZSS
Mobile terminal
L1-SAIF
L1-C/A
GEONET
GSI
Producing L1-SAIF
ENRI
QZSS main control station
GEONET: GPS Earth Observation Network
GSI: Geospatial Information Authority of Japan
ENRI: Electronic Navigation Research Institute

Fig. 23.4 High-accuracy positioning system using QZSS. The enhanced GPS technology has been evaluated using the first QZS, Michibiki, and is expected to achieve submeter positioning accuracy

GPS technology described above has been evaluated using the first QZS, Michibiki, and is expected to achieve submeter positioning accuracy.

23.2.2 Performance Evaluation by Computer Simulation

In SS-CDMA, all terminals synchronize with each other in the time and frequency domains using the positioning signals from QZS. The synchronization procedure is as follows.

1. Each terminal calculates its own location, present time, and reference frequency. The local clock and phase locked loop (PLL) are synchronized to those of QZS.
2. The terminal precisely calculates its distance from the QZS used as a base station. Each terminal determines the propagation delay using the distance and related environmental information provided in L1-SAIF.
3. All terminals transmit a modulated signal at a suitable time so that all signals arrive at the satellite at the same time.

Because not only the chip[1] timing but also the Nyquist point is adjusted to the specific timing, as shown in Fig. 23.5, we can minimize the impact of imperfect orthogonality.

In the rest of this subsection, we will show by computer simulation that satisfactory performance in terms of BER can be obtained even in the presence of practical timing jitter and frequency offset if a long-enough code is used in the pro-

[1] The "chip" is a pulse of a direct-sequence spread spectrum (DSSS) code. Chip is also used as units of period (code length) of SS code.

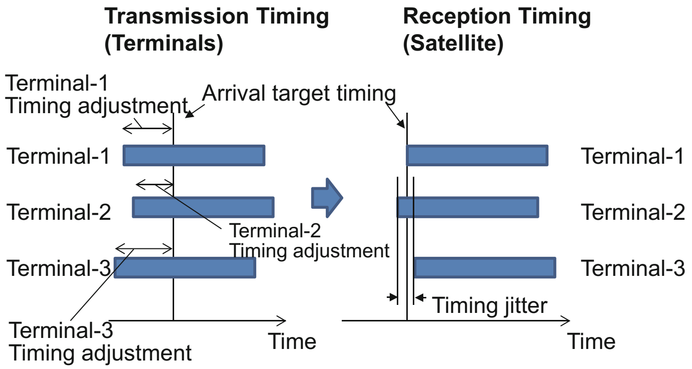

Transmission Timing (Terminals)
Reception Timing (Satellite)
Terminal-1 Timing adjustment
Arrival target timing
Terminal-1
Terminal-2
Terminal-3
Terminal-2 Timing adjustment
Terminal-3 Timing adjustment
Time
Terminal-1
Terminal-2
Terminal-3
Timing jitter
Time

Fig. 23.5 Transmission timing control. Because not only the chip timing but also the Nyquist point is adjusted to the specific timing, we can minimize the impact of imperfect orthogonality

Table 23.2 Simulation parameters

Modulation	Binary phase-shift keying (BPSK) (single carrier), Quadrature phase-shift keying (QPSK) (single carrier)
Forward error correction (FEC)	Convolutional code $R = 1/2$
Chip rate	224 kchip/s
User data rate	220 bit/s
Spreading code	Single M-sequence (rotational shift for each user)
Spreading gain	$G_s = 1024$
Number of users	500, 1000
Transmitter and receiver filters	Root cosine roll-off filter
Detection	Coherent detection (ideal channel estimation)
Channel	Additive white Gaussian noise (AWGN)

posed SS-CDMA method using QZSS. Table 23.2 shows the simulation parameters. The required code gain is 10,000 from the viewpoint of the channel design, but we adopted one-tenth scaling ($G_s = 1024$, chip rate is 224 kchip/s) for convenience of the simulation time. The SS code is a single M-sequence, and rotational shift sequences are assigned to each user. Figure 23.6 illustrates the code assignment. If the code length is $G_s = 1024$ and the number of multiplexing users is N_u, the minimum rotational shift among users is $\lfloor G_s/N_u \rfloor$, where $\lfloor x \rfloor$ denotes the maximum integer that does is not exceed x. In the case of 500 users, the number of shifts is two, and in the case of 1000 users, it is one. Each terminal uses the rotational shift code with “0” added last; these codes are referred to as the orthogonal M-sequence. From the property of the orthogonal M-sequence, the received signal power after the despreading process is G_s for the same code and 0 for other codes. The orthogonal M-sequence provides the spreading gain and interference suppression effects.

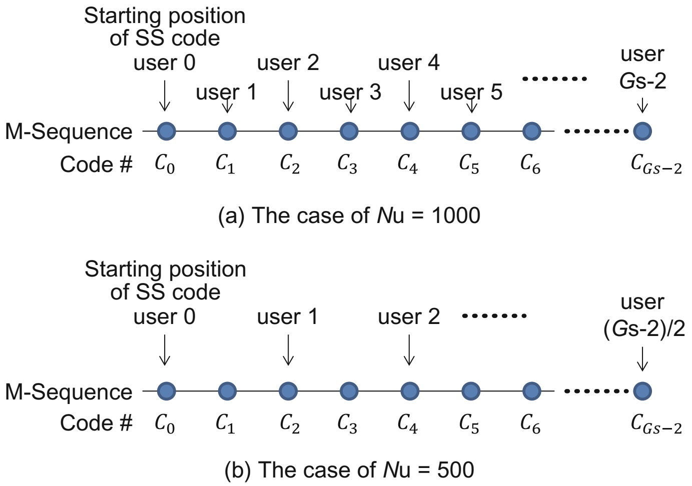


Fig. 23.6 SS code assignment for each user. From the property of the orthogonal M-sequence, the received signal power after the despreading process is the spreading gain G_s for the same code and 0 for other codes. The orthogonal M-sequence provides the spreading gain and the interference suppression effects

23.2.2.1 BER Performance with Timing Jitter

In this subsection, we will elucidate the influence of the timing jitter in the proposed SS-CDMA. In the condition with timing jitter, it is important that degradation of S/N ($E_b/N_0/G_s$ in the Fig. 23.7) is as small as possible (for example, less than 1 dB) for the system design of SS-CDMA.

Figure 23.7 shows the bit error rate (BER) performance of SS-CDMA when timing jitter exists. The horizontal axis represents energy per bit to noise power spectral density ratio (E_b/N_0) considering the spreading gain G_s. In this figure, N_u is the number of multiplexing users and T_j is the maximum jitter normalized by the chip period. The lines with open symbols show the BER with $N_u = 500$, and those with closed symbols show the BER with $N_u = 1000$. The timing jitter τ assigned to each terminal is random and τ is distributed uniformly between $-T_j$ and $+T_j$. The results in Fig. 23.7 indicate the following.

- When $N_u = 500$, performance degradation is hardly observed in the case of timing jitter of less than four-eighths chip and only appears when $T_j \geq 6/8$.
- The condition $N_u = 1000$, for which there is a short distance among the codes, exhibits performance degradation with a small T_j. The degradation of $E_b/N_0/G_s$ at a BER of 10^{-5} is about 0.5 dB with one-eighth-chip timing jitter and over 4 dB with two-eighths-chip timing jitter.

From these results, we can conclude that timing jitter does not result in performance degradation as long as the distance of the code shift among each user is kept

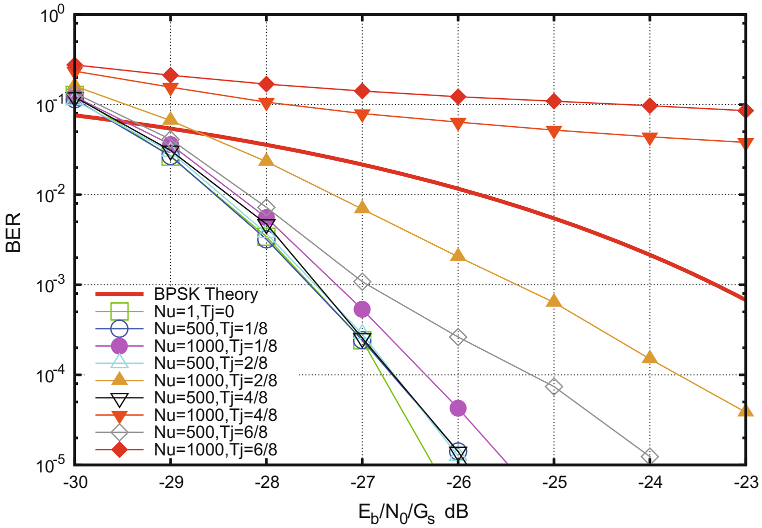


Fig. 23.7 BER performance with timing jitter (BPSK, $R = 1/2$, $G_s = 1024$). The timing jitter does not result in performance degradation as long as the distance of the code shift among each user is kept larger than one chip

larger than one chip. In other words, the timing error of the Nyquist point at the satellite is not a dominant factor and is suppressed by the despreading process using a long SS code. On the other hand, when the distance is less than one chip, the despreading process generates a large intercode interference and causes severe performance degradation.

QZSS has submeter positioning accuracy. Thus, the reference clock jitter is expected to be less than 10 ns. When we adopt the channel design parameters in Table 23.2, the chip period is 446 ns. Therefore, one-eighth-chip timing jitter will be feasible.

23.2.2.2 BER Performance with Frequency Offset

In this subsection, we will elucidate the influence of the frequency offset in the proposed SS-CDMA. In the condition with frequency offset, it is important that degradation of S/N is as small as possible (for example, less than 1 dB) for the system design of SS-CDMA.

Figure 23.8 illustrates the frequency synchronization block diagram using QZSS. Each terminal produces a reference frequency, which is synchronized with the clock on the satellite using the positioning signals. Then, the difference between the local-temperature-compensated crystal oscillator (TCXO) and the reference frequency is periodically estimated. The transmit automatic frequency control (AFC) block gives phase rotation to the modulated signals so as to cancel the frequency gap. The

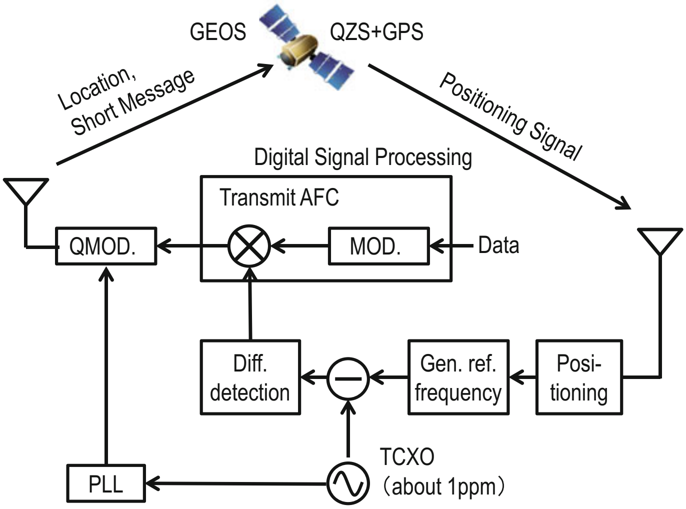


Fig. 23.8 Transmit frequency control using QZSS. Each terminal produces a reference frequency, which is synchronized with the clock on the satellite using the positioning signals

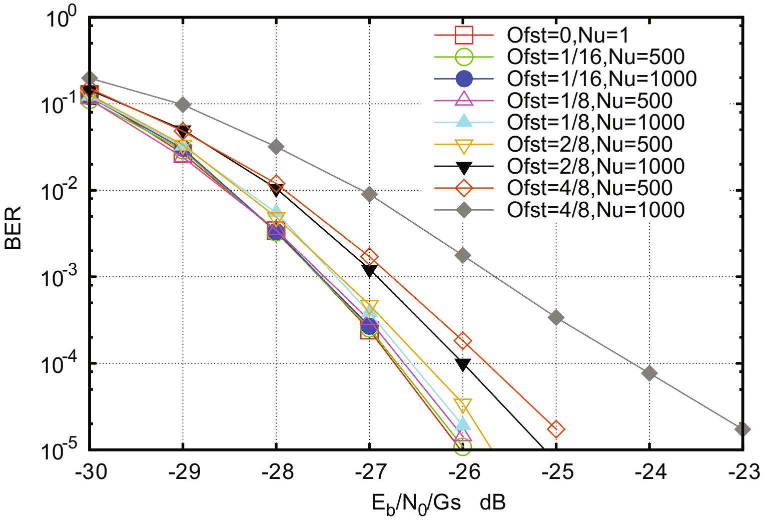


Fig. 23.9 BER performance with frequency offset (BPSK, $R = 1/2$, $G_s = 1024$). We can observe the performance degradation of $E_b/N_0/G_s$ with an increase in the frequency offset

transmit signal from each terminal contains the residual frequency offset and the phase noise in the PLL block. In this subsection, the effects of the residual frequency offset are evaluated.

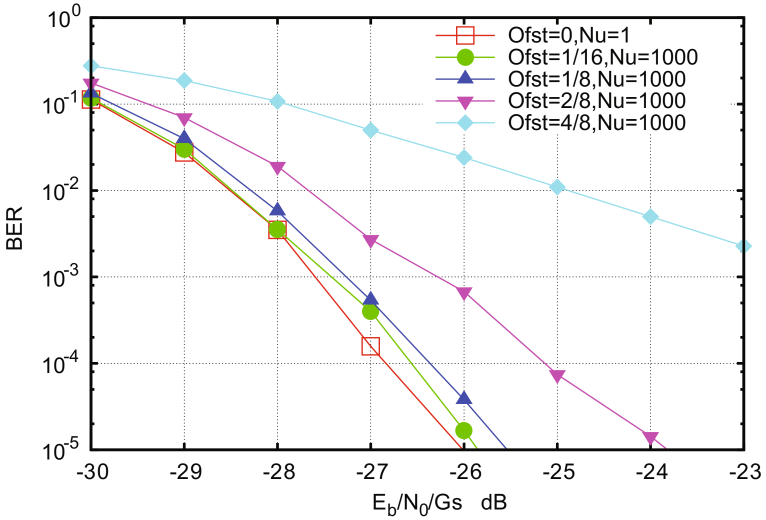


Fig. 23.10 BER performance with frequency offset (QPSK, $R = 1/2$, $G_s = 1024$). QPSK is more sensitive than BPSK owing to the shorter distance of the modulated signal constellation. To suppress the performance degradation of $E_b/N_0/G_s$ to less than 1 dB, the normalized frequency offset must be one-eighth or less. One-eighth of the normalized frequency corresponds to 28 Hz. If 2.68 GHz is assumed as the carrier frequency, 10 ppb frequency stability is required, which has been realized using a GPS-synchronized oscillator

Figures 23.9 and 23.10 show the BER performance with the frequency offset of BPSK and QPSK signals, respectively, where N_u is the number of multiplexing users and Ofst is the frequency offset normalized by the symbol period (=G_s chips). From these results, we can observe the performance degradation of $E_b/N_0/G_s$ with an increase in the frequency offset. The frequency offset breaks the orthogonality among multiplexing users and generates interference. The interference power is proportional to the number of multiplexing users; thus, the performance with 1000 users is worse than that with 500 users. The results for BPSK and QPSK show a similar tendency. However, QPSK is more sensitive than BPSK owing to the shorter distance of the modulated signal constellation. To suppress the performance degradation to less than 1 dB, the normalized frequency offset must be one-eighth or less.

One-eighth of the normalized frequency corresponds to 28 Hz (224 Hz/8). If 2.68 GHz is assumed as the carrier frequency, 10 ppb frequency stability is required, which has been realized using a GPS-synchronized oscillator (see Sect. 9.4).

From results in the subsections, the proposed SS-CDMA has a potential for being used the large capacity disaster message exchange system, even if there are timing jitter and frequency offset.

23.3 Heterogeneous Wireless System with Network Selection Scheme Using Positioning Information

The demand for broadband services involving wireless communication systems has increased and wireless data traffic has been increasing sharply. One of potential ways to satisfy the demand is to use a heterogeneous wireless system, multiple wireless systems are combined, such as MBWA and WLAN systems. Additionally, the dense deployment of small cells is effective for capacity expansion. For example, the number of WLAN access points (APs) has been increasing in recent years. In the Third-Generation Partnership Project (3GPP), small-cell enhancement (SCE) has been discussed for the fourth-generation mobile networks [7]. Upon increasing the number of small cells, multiple network cells will overlap in heterogeneous wireless systems.

For optimum data traffic offloading, users must select a cell with the highest channel quality. For cell selection, users generally discover neighboring cells by listening on the broadcast channel and measuring the instantaneous value of the signal strength, such as the received signal strength indicator (RSSI) or the reference signal received power (RSRP). However, using this scheme, network efficiency decreases in a dense small-cell environment. The reasons for this are as follows. First, users must discover a large number of cells and measure the instantaneous signal strength for each of them. More radio resources are used for cell selection in such an environment. Next, cell selection errors occur because the instantaneous signal strength fluctuates owing to fading. Users cannot select the cell with the highest channel quality because of cell selection errors. Finally, users cannot obtain traffic load information only by measuring the signal strength. Even if users select the cell with the highest signal strength among neighboring cells, the cell may be congested and the throughput may not be the highest. For example, a WLAN uses carrier sense multiple access with collision avoidance (CSMA/CA) as a multiple access scheme, for which the channel efficiency is greatly decreased when the number of users connected to the WLAN is large. Therefore, to improve the network efficiency in a dense small-cell environment, the cell selection scheme must satisfy the following requirements:

- Reduced radio resource utilization for cell selection.
- Suppression of cell selection errors.
- Provide a method of acquiring cell traffic load information.

We focus on the systems that provide high-accuracy positioning information, such as QZSS in Japan and the Global Navigation Satellite System (GLONASS) in Russia with GPS. Using these systems, we can obtain submeter-resolution positioning information. In this section, we propose a cell selection scheme using positioning information [1, 8–11]. In the proposed scheme, users select a cell using their location and channel quality information. The channel quality information at each location is provided for cell selection. Users can estimate the channel quality information by measuring the channel quality only at their location. Thus, users do not have to discover cells for cell selection. Furthermore, this channel quality information consists of the average signal strength and traffic load information. Therefore, users can suppress the cell selection error and select a cell in response to real-time variations in the traffic load.

23.3.1 Network Selection Scheme Using Positioning Information

In this section, we explain the proposed cell selection scheme. As mentioned in the introduction, the proposed scheme utilizes the user's location and channel quality information. Knowing the location of the user, channel quality information for neighboring cells is referenced, and the cell that should be selected by the user is decided. In this chapter, we call this information the channel quality map. Figure 23.11 shows an image of a channel quality map. The channel quality map tells users which cell should be selected at each location. As shown in Fig. 23.11, since mobile terminal (MT) #A is in area AP #1, the MT #A should select cell AP #1. The channel quality map uses average signal strengths as the physical channel quality of the cells. In the handover of a heterogeneous wireless system, the average signal strength is a suitable cell selection criterion. For example, in a cellular system, a high-speed closed-loop transmission power control and an adaptive modulation and coding (AMC) are used for following the fluctuation of the signal strength. However, in a self-distributed wireless system such as a WLAN, there is no such function. The user's terminal cannot cope with instantaneous fluctuations of the signal strength in a WLAN. The handover in a heterogeneous wireless systems is executed very slowly compared with the fluctuation speed of the signal strength. Therefore, the average signal strength is used in the channel quality map as a common cell selection criterion in the proposed scheme.

Thus, in the proposed scheme, it is necessary to construct a channel quality map in addition to obtaining the positioning information. Figure 23.12 shows an outline of the method used to construct the channel quality map. To construct the map, calculation of the average signal strength at each location is necessary. In this section, the user's measurement of the instantaneous value is utilized as information. The heterogeneous control server (HCS) in Fig. 23.12 gathers measurement information from the terminals of an enormous numbers of users and statistically processes the gathered information to construct the map. The HCS stores the channel quality map, and users obtain the map from this server. Hereafter, we explain the method of creating the channel quality map. The map is constructed using the following two steps:

(a) Measurement of the signal strength and location

First, to calculate the average signal strength, users measure the instantaneous signal strength of each cell. At the same time, users also measure their own location. These two pieces of information are stored by individual users. Even in the proposed scheme, users have to measure the signal strengths, but this measurement is executed by an enormous number of users and is not used for cell

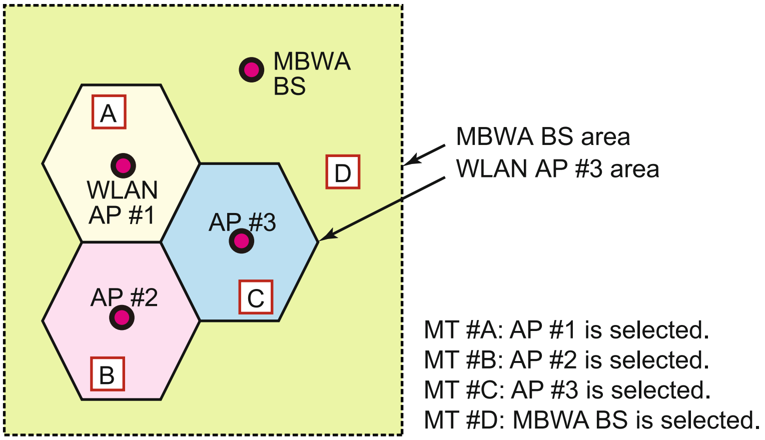

MBWA
BS
A
WLAN
AP #1
D
AP #3
AP #2
C
B
MBWA BS area
WLAN AP #3 area
MT #A: AP #1 is selected.
MT #B: AP #2 is selected.
MT #C: AP #3 is selected.
MT #D: MBWA BS is selected.

Fig. 23.11 Image of channel quality map. AP, BS, and MT are access point (WLAN), base station (MBWA) and mobile terminal, respectively. The channel quality map tells users which cell should be selected at each location

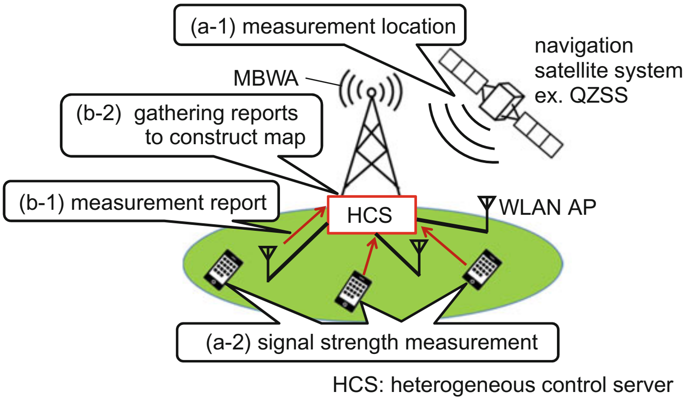


Fig. 23.12 Steps in construction of channel quality map. The map is constructed using the following two steps: **a** measurement of the signal strength and location and **b** gathering measurement reports and constructing the map

selection. Thus, users can carry out this measurement at any time. It is expected that the measurement time per user will be reduced in the proposed scheme.

(b) Gathering measurement reports and constructing the map

Next, the information discussed in (a) is gathered to construct the map. In this process, users transmit this information to the HCS. This transmission has a low real-time demand because the average signal strength is static unless the neighboring environment greatly changes. Thus, the timing when users transmit this information can be flexibly adjusted. On the other hand, the HCS executes

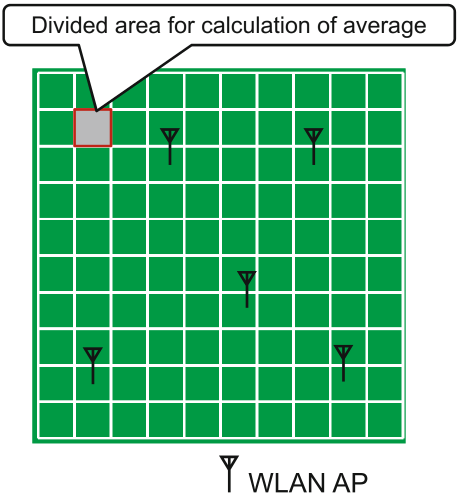


Fig. 23.13 Example of averaging to construct map. Areas are segmented into squares and the gathered information is averaged in each square

statistical information processing for every cell to construct the channel quality map. Figure 23.13 shows an example of averaging. In Fig. 23.13, areas are segmented into squares and the gathered information is averaged in each square. The square size should be decided by considering the positioning accuracy. If the squares are large, the channel quality map becomes unreliable because small cells have a narrow coverage. Therefore, high positioning accuracy is necessary to produce a reliable map. As mentioned in the introduction, users can obtain submeter-resolution positioning information by using QZSS or GLONASS with GPS.

Using proposed scheme with high-accuracy positioning information and the map information, the proposed scheme can improve the system performance in a dense small cell environment.

23.4 Readiness of Required Technologies

The readiness of the technologies required for realizing Extended Dependable Air are discussed in the following sections:

- High-frequency and high-gain antenna technologies using low-cost three-dimensional system-in-package (3D SiP) technologies (Sect. 7.3.3)
- RF circuit technologies for multiband and multimode receivers including millimeter wave band (Sects. 7.3.2, 7.4 and 7.5).
- Dependable analog-to-digital converter technologies for multiband and multimode receivers (Sect. 7.6).

- Broadband baseband signal processing technologies such as frequency domain equalization (Sect. 7.7).
- Clock and frequency synchronization technologies and high-accuracy positioning information technologies (Sect. 9.4).
- Heterogeneous wireless network technologies (Sect. 7.8).

References

1. K. Tsubouchi, Extended dependable air: heterogeneous wireless network for surface, space and sea, in *2014 Asia-Pacific Microwave Conference (APMC2014)* (Nov 2014 (invited))
2. T. Takahashi, Y. Miyake, F. Yamagata, H. Oguma, S. Kameda, N. Suematsu, T. Takagi, K. Tsubouchi, Large-capacity QZSS location and short message system using frame slotted ALOHA with flag method, in *IEEE 24rd International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC2013)* (London, U.K., Sept 2013), pp. 3280–3285
3. A. Taira, Y. Miyake, S. Kameda, N. Suematsu, T. Takagi, K. Tsubouchi, QZSS location and short message communication system against big disasters, in *Vietnam-Japan International Symposium on Antennas and Propagation (VJISAP2013)* (Jan 2014 (invited)), pp. 229–234
4. A. Taira, Y. Miyake, S. Kameda, N. Suematsu, T. Takagi, K. Tsubouchi, System stability of SS-CDMA location and short message communication using QZSS, in *2014 Asia-Pacific Microwave Conference (APMC2014)* (Nov 2014)
5. Y. Miyake, A. Taira, S. Kameda, H. Oguma, N. Suematsu, T. Takagi , K. Tsubouchi, Transmit performance with timing and frequency error of QZSS SS-CDMA short message communication system. IEICE Trans. Commun. **J98**–**B**(4), 397–405 (2015)
6. N. Suematsu, S. Kameda, Y. Miyake, T. Takahashi, A. Taira, T. Takagi, K. Tsubouchi, QZSS SS-CDMA location and short message communication system, in *2015 Vietnam-Japan MicroWave (VJMW2015)* (Ho Chi Minh City, Vietnum, August 2015 (invited))
7. 3GPP, TR36.932 (v12.1.0), *Scenarios and Requirements for Small Cell Enhancements for E-UTRA and E-UTRAN* (March 2013)
8. J. Kuboniwa, Y. Miyake, S. Kameda, A. Taira, N. Suematsu, T. Takagi, K. Tsubouchi, A novel cell selection scheme using positioning information for heterogeneous wireless system, in *The 7th International WDN Workshop on Cooperative and Heterogeneous Cellular Networks (WDN-CN2014) in conjunction with IEEE PIMRC2014*, (Washington, D.C., USA, 2014)
9. J. Kuboniwa, Y. Miyake, S. Kameda, A. Taira, H. Oguma, N. Suematsu, T. Takagi, K. Tsubouchi, High efficient network selection scheme using location information for heterogeneous wireless system, in *The 8th International WDN Workshop on Cooperative and Heterogeneous Cellular Networks (WDN-CN2015) in conjunction with IEEE WCNC2014* (LA, New Orleans, USA, 2015)
10. H. Oguma, A. Koizumi, K. Norishima, J. Kuboniwa, Y. Miyake, S. Kameda, A. Taira, N. Suematsu, T. Takagi, K. Tsubouchi, Channel quality map construction scheme using location information for heterogeneous wireless network. Stud. Sci. Tech. **4**(1), 83–90 (2015)
11. Q. Liu, J. Kuhoniwa, S. Kameda, A. Taira, N. Suematsu, T. Takagi, K. Tsubouchi, Traffic navigation using location information and channel quality map for system-wide load balancing, in *2015 Asia-Pacific Microwave Conference (APMC2015)* (Nanjing, China, Dec 2015)

Chapter 24
Responsive Multithreaded Processor for Hard Real-Time Robotic Applications

Nobuyuki Yamasaki, Hiroyuki Chishiro, Keigo Mizotani and Kikuo Wada

Abstract Distributed real-time systems such as automated factories, space-crafts, and robots are generally built with a set of hardware and software components designed for specific control functions with time constraints. Various key technologies including real-time processing architecture, real-time communication, a DVFS (Dynamic Voltage and Frequency Scaling) mechanism, and a real-time operating system are required to build these applications. A humanoid robot, which the authors have chosen as an authors' target application, requires a very small controller that consists of an SiP (System-in-Package), which is composed of an SoC (System-on-Chip), DRAMs, flash memories, and power units. In this chapter, the authors present the fundamental technology on dependable SoCs and SiPs for embedded real-time systems. In particular, D-RMTP (Dependable Responsive MultiThreaded Processor), real-time operating systems, and the co-design of SoC and SiP are introduced.

Keywords RMTP · *Responsive link* · RT-OS · Real-time control · Robots

24.1 Introduction

A distributed real-time system such as a humanoid robot has many requirements including time constraints (e.g., deadline, cycle, and jitter), size, power, etc. One of the typical robotic applications shown in Fig. 24.1 is the musculoskeletal humanoid

N. Yamasaki (✉) · H. Chishiro · K. Mizotani
Keio University, Yokohama, Japan
e-mail: yamasaki@ny.ics.keio.ac.jp

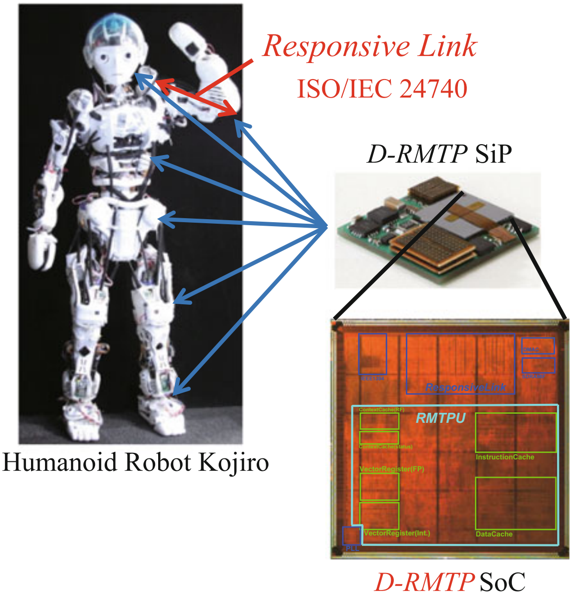
H. Chishiro
e-mail: chishiro@ny.ics.keio.ac.jp

K. Mizotani
e-mail: mizotani@ny.ics.keio.ac.jp

K. Wada
NEC Platforms, Kakegawa, Japan
e-mail: k-wada@yk.jp.nec.com

S. Asai (ed.), *VLSI Design and Test for Systems Dependability*,
https://doi.org/10.1007/978-4-431-56594-9_24

Fig. 24.1 A typical robotic application



robot named Kojiro [15] that has many processors to control local nodes which are connected with each other via a real-time network. The control period of such robot using conventional processors (e.g., Intel, AMD, ARM, and H8) and operating systems (e.g., Linux, Windows, and TRON) is on the order of 1 ms. However, this robot requires a control period of 10–100 μs. In addition, the low energy and high quality execution is required by using the remaining processor time for improving the QoS (Quality of Service). An SiP must be small size because it has to be installed in the robot such as arms and legs that have very small capacity. The SiP is composed of an SoC that must also be small in size, DRAMs, flash memories, etc.

The authors have designed and implemented D-RMTP (Dependable Responsive MultiThreaded Processor) [18] to support such fine-grained control. Two real-time operating systems for the D-RMTP have been developed to support the D-RMTP-specific features. The SoC and SiP are co-designed to meet such requirements including very small size, power control, thermal control, etc.

The remainder of this chapter is organized as follows. Section 24.2 introduces the D-RMTP as a dependable real-time processor. Section 24.3 discusses the co-design of the SoC and SiP. Section 24.4 presents two real-time operating systems for D-RMTP. Finally, Sect. 24.5 summarizes this chapter.

24.2 Responsive Multithreaded Processor (RMTP)

This section introduces an overview of the D-RMTP as a hard real-time processor and *Responsive Link* as a dependable real-time communication standard. The design concept of the D-RMTP is to execute real-time tasks simultaneously based on real-time scheduling algorithms by hardware without overhead. The design concept of *Responsive Link* is to realize real-time communication based on real-time scheduling algorithms by hardware.

Figure 24.2 shows the D-RMTP SoC implemented in the 10 mm^2 chip with TSMC 130 nm process technology. The D-RMTP SoC integrates RMT PU (Responsive Multithreaded Processing Unit) for real-time processing, *Responsive Link* for real-time communication, and following memory and various I/O peripherals:

- PLL
- Trace buffer
- SRAM (64 kB)
- SDRAM interfaces (2ch)
- Flash memory interface
- 256/32-bit DMAC
- 32-bit DMAC (20ch)

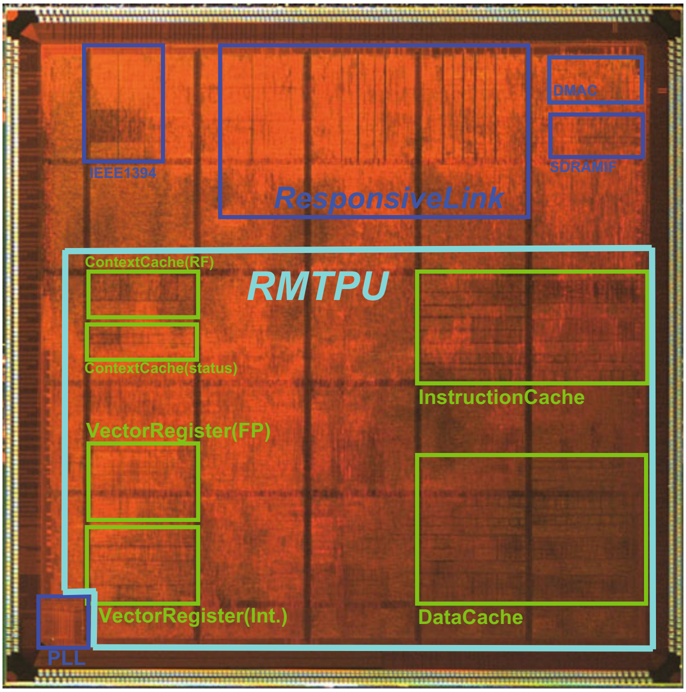


Fig. 24.2 D-RMTP SoC

- IEEE 1394
- PCI-X
- Ethernet
- UART (4ch)
- SpaceWire
- SPI (4cs × 2ch)
- PWM-in (3ch), PWM-out (12ch), encoders (4ch)
- Digital port (8ch)
- 32-bit external bus (4cs, 4dreq, 4irq)

24.2.1 Responsive Multithreaded Processing Unit (RMT PU)

The RMT PU can simultaneously execute eight prioritized threads in priority order to realize real-time processing by hardware, so that the RMT PU has multiple functional units including four ALUs and two FPUs, and eight hardware contexts. A hardware context consists of 32 GPRs (General Purpose Registers) eight FPRs (Floating Point Registers), PC (Program Counter) etc. Eight threads with 256-level priority can run simultaneously. It is built in an eight-way SMT (Simultaneous Multithreading) architecture [20] with priority (i.e., prioritized SMT architecture). The authors call the prioritized SMT execution for real-time processing the RMT execution.

A real-time operating system assigns a priority level to each thread by using a time constraint such as deadline or cycle. The fetch unit tries to fetch eight instructions of the higher priority thread per clock cycle from the instruction cache. If it cannot fetch the highest priority thread because of cache miss, branch prediction miss, etc., it fetches instructions from the next higher priority threads in priority order. Whenever the higher priority threads complete their execution, the lower priority threads can begin their execution. The execution unit executes the threads based on priority out of order by using the prioritized reservation stations, the prioritized reorder buffers, and so on.

When the number of threads is less than or equal to eight and a fixed-priority real-time scheduling algorithm including the RM (Rate Monotonic) algorithm [12] is used, the RMT PU can execute these threads in real-time by hardware alone [18]. In this case, no software scheduler is needed. Under the RM algorithm, the shorter period of the task has the higher priority.

Figure 24.3 shows the RMT execution without/with the IPC (Instruction Per Cycle) control mechanism in the D-RMTP [8, 24]. In this example, there are four running threads. The smaller thread ID has the higher priority. Thread 1 (th1) begins running with the highest priority, hence it is not interfered basically by lower priority threads. Threads 2–4 are running but their execution speeds are lower than thread 1 because of the RMT execution. However, without IPC control, the IPC (execution speed) of each thread varies. Even if the thread has highest priority in case of thread 1, its IPC varies microscopically. In order to achieve high precision

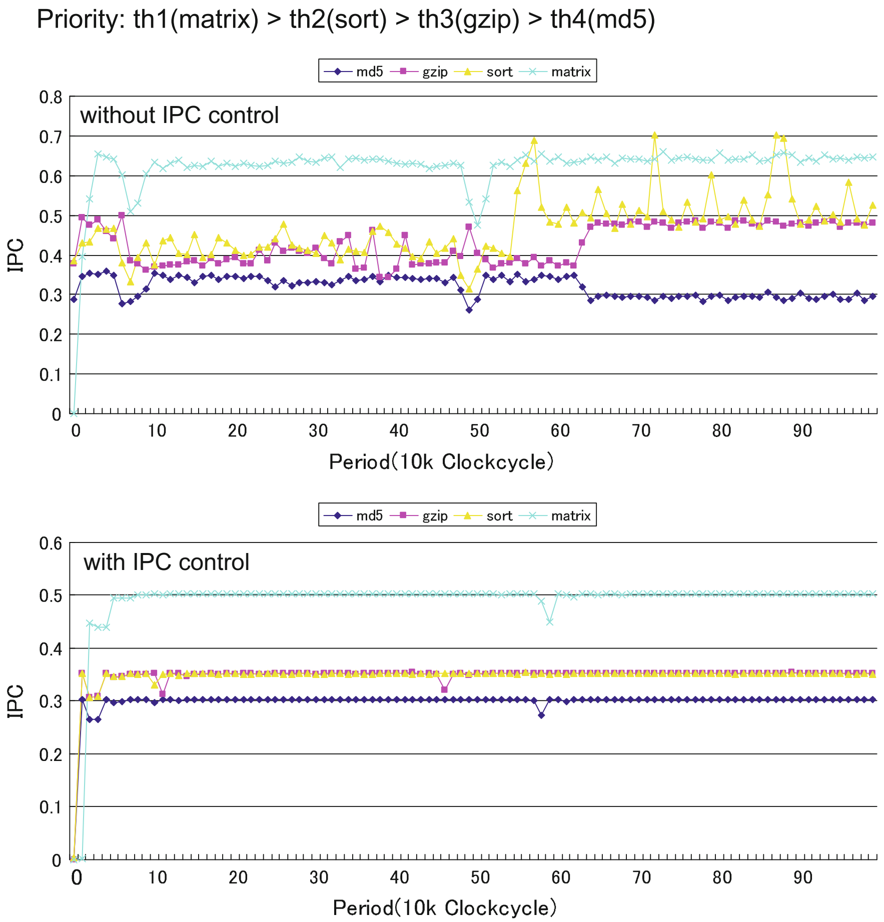


Fig. 24.3 Prioritized SMT execution without/with IPC control mechanism on D-RMTP

real-time processing, the IPC control mechanism that stabilizes each thread execution speed assigned by software (RT-OS) is designed and implemented. With IPC control shown in Fig. 24.3, the IPC of each thread is kept constant. The IPC of each thread is controlled by feedback regulation (PID control). When a thread completes the specified number of instructions during the IPC control period, the fetch of the thread is stopped. Note that the IPC control period is enough shorter than the periods of tasks.

In order to execute more threads in real-time by hardware and to be able to utilize a dynamic real-time scheduling algorithm such as the EDF (Earliest Deadline First) algorithm [12], the on-chip context cache that can save up to 32 hardware contexts is designed and implemented. Under the EDF algorithm, the shorter absolute deadline of the task has the higher priority. Only four clock cycles are needed to switch (swap) the thread contexts between the hardware context (register set) and the context cache. The total overhead of context switching for real-time execution has been remarkably reduced, thanks to the context cache.

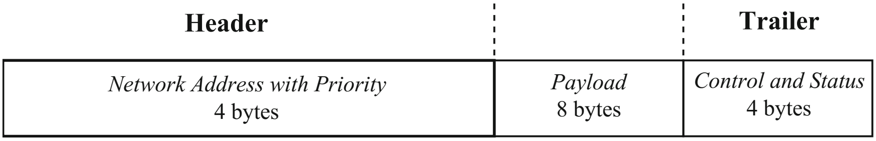
Since current real-time applications require high-performance computing for multimedia processing such as image processing and voice processing, flexible vector units are designed for multimedia processing in the D-RMTP. As multiple threads are executed in parallel on the RMT PU, vector registers are shared by multiple threads efficiently by reserving the size required for the executing vector operation. An FP (Floating-Point) vector unit executes four 64-bit IEEE754 FP SIMD operations (64 bit × 1 or 32 bit × 2) and an integer vector unit executes eight 32-bit integer SIMD operations (32 bit × 1, 16 bit × 2, or 8 bit × 4) per clock cycle. Two FP vector units that share 512-entry 64-bit FP vector registers and two integer vector units that share the 512-entry 32-bit integer vector registers are implemented. Each vector unit is used independently by different threads simultaneously. A single thread can also use all vector units at the same time.

The RMT PU executes simultaneously real-time tasks prioritized by a real-time scheduler with high efficiency, making the time granularity of real-time processing finer.

24.2.2 Responsive Link

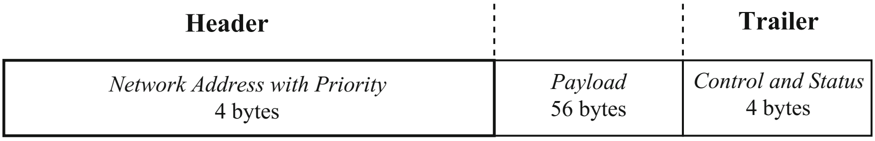
Responsive Link [23] is a communication standard as specified in ISO/IEC 24740 for distributed real-time systems. *Responsive Link* has multiple features to meet the requirements of both hard and soft real-time communications. Under the hard real-time requirement, packets must meet their deadlines (e.g., control command). In contrast, under the soft real-time requirement, some packets are allowed to miss their deadlines (e.g., multimedia). *Responsive Link* has two communication links: Event Link and Data Link. The Event Link is used to transmit packets with hard real-time requirements, while the Data Link is used to transmit packets with soft real-time requirements. *Responsive Link* supports variable link speeds (800, 400, 200, 100, 50, 25, 12.5 Mbaud), plug and play, and topology-free, which is an important feature because some robotic applications have complex topologies. It is not easy to use conventional fixed topology communication standards for such applications.

Generally, real-time systems are controlled by real-time scheduling, which guarantees completing real-time tasks by their deadlines. In real-time scheduling, higher priority tasks preempt lower priority tasks. Therefore, the most important feature of *Responsive Link* is to support preemption capability on communication. In order to achieve this preemption in real-time communication, *Responsive Link* is designed so that higher priority packets overtake lower priority packets at each node. Each packet in *Responsive Link* is assigned with a priority level calculated by a real-time scheduling algorithm such as a fixed-priority scheduling algorithm [6] and a semi-fixed-priority scheduling algorithm [3, 4], which can be adapted to packet scheduling for real-time communication.



Header		Trailer
Network Address with Priority 4 bytes	*Payload* 8 bytes	*Control and Status* 4 bytes

Fig. 24.4 Event packet



Header		Trailer
Network Address with Priority 4 bytes	*Payload* 56 bytes	*Control and Status* 4 bytes

Fig. 24.5 Data packet

Responsive Link supports two kinds of packets for hard and soft real-time communication: event packet and data packet, respectively. Figures 24.4 and 24.5 show the formats of the event packet and the data packet. An event packet is 16-byte length and consists of a 4-byte header (a 4-byte network address with an 8-bit priority), an 8-byte payload, and a 4-byte trailer. The main use of event packets is to transmit inter-node interruptions, control commands, and operations with hard real-time requirements. A data packet is 64-byte length and consists of a 4-byte header, a 56-byte payload, and a 4-byte trailer. The main use of data packets is to transmit bulky data such as image and sound data with soft real-time requirements. Using event and data packets, both hard and soft real-time communications are achieved together. By the separate transmission of Event Link and Data Link, *Responsive Link* can support hard and soft real-time communications more easily than other communication standards such as CAN [9] and FlexRay [5] can.

Responsive Link achieves an end-to-end real-time connection by setting the routing tables of all nodes along the transmission path from a source node to a destination node. Each node has a routing table to control the route of the packet and the priority exchange function. In addition, *Responsive Link* supports prioritized routing. When multiple packets with different priorities are sent to the same destination, a different route can be set to realize exclusive communication links or detours.

24.3 Co-design of SoC and SiP

This section explains the co-design of D-RMTP SoC and SiP using FFCSP (Flexible carrier Folded real Chip Size Package) [25]. The FFCSP approach is constructed by stacking very thin single chip packages of real chip size on top of another. Each single chip package consists of an LSI chip and a small piece of a flexible printed circuit, which has an insulating layer made of thermoplastic resin. The connection and wiring are optimized by SI/PI (Signal Integrity/Power Integrity) simulations to

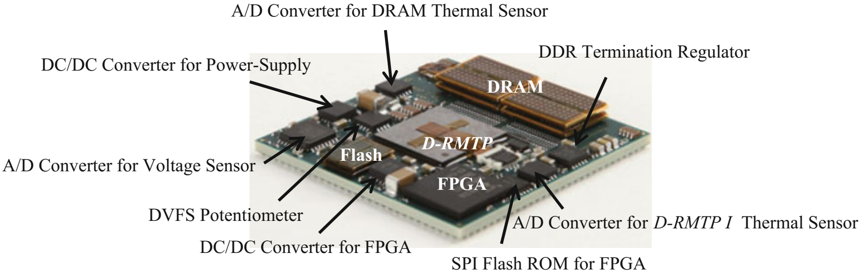

A/D Converter for DRAM Thermal Sensor
DDR Termination Regulator
DC/DC Converter for Power-Supply
DRAM
D-RMTP
Flash
FPGA
A/D Converter for Voltage Sensor
DVFS Potentiometer
DC/DC Converter for FPGA
A/D Converter for *D-RMTP I* Thermal Sensor
SPI Flash ROM for FPGA

Fig. 24.6 The 30 mm square D-RMTP SiP

overcome the inherent problem, while seeking to downscale the size of the SiP in robots. The authors have developed a 30 mm square D-RMTP SiP that meets the scaling and performance requirements, which can be installed inside a high power leg robot.

Figure 24.6 shows the 30 mm square D-RMTP SiP that integrates sixteen LSIs while satisfying small size requirements [22]. The detail of sixteen LSIs is as follows.

- D-RMTP SoC
- FFCSP DRAM × 4
- FPGA
- FFCSP flash memory × 2
- Analog-to-digital converter for DRAM thermal sensor
- Analog-to-digital converter for voltage sensor
- Analog-to-digital converter for D-RMTP thermal sensor
- DC-to-DC converter for power-supply
- DC-to-DC converter for FPGA
- DVFS potentiometer
- SPI flash ROM for FPGA
- DDR termination regulators

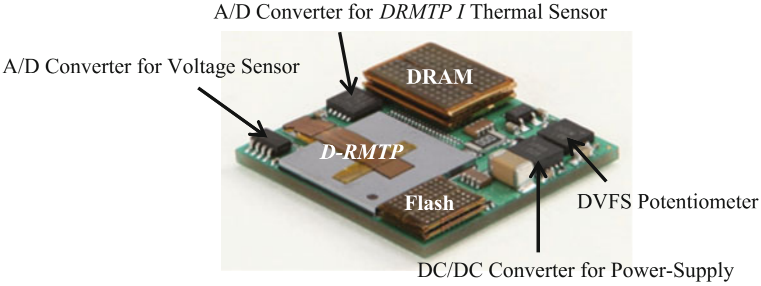

A/D Converter for *DRMTP I* Thermal Sensor
A/D Converter for Voltage Sensor
DRAM
D-RMTP
Flash
DVFS Potentiometer
DC/DC Converter for Power-Supply

Fig. 24.7 The 20 mm square D-RMTP SiP

Figure 24.7 shows the 20 mm square D-RMTP SiP that integrates nine LSIs to achieve further downscaling, compared with the 30 mm square D-RMTP SiP. The detail of nine LSIs is as follows.

- D-RMTP SoC
- FFCSP DRAM × 2
- FFCSP flash memory × 2
- Analog-to-digital converter for voltage sensor
- Analog-to-digital converter for D-RMTP thermal sensor
- DC-to-DC converter for power-supply
- DVFS potentiometer

Both these 30 and 20 mm square D-RMTP SiPs have the DVFS (Dynamic Voltage and Frequency Scaling) function. In addition, the TA-DVFS (Temperature-Aware Dynamic Voltage and Frequency Scaling) [10] ensures that the package will continue to operate robustly under the severe conditions inside robots. Especially, robots require low energy consumption under high temperature. The 3D-stacked FFCSP approach is used to implement 3D-stacked DRAMs and flash memories to achieve greater miniaturization. The advantage of this approach is that the organic interposer provides a greater degree of freedom in implementing inter-chip wiring. The length of interconnections between chips should be as short as possible, which requires that the interposer substrate be thinned to the extent possible. The detail of the D-RMTP SoC is described in Sect. 24.2.

24.4 Real-Time Operating Systems

The authors have developed two real-time operating systems to support the D-RMTP-specific features. One is an originally designed operating system and the other is an ITRON-specified operating system.

24.4.1 Favor Operating System

Figure 24.8 shows the overview of the Favor operating system [14]. The Favor operating system has been originally developed from scratch on the D-RMTP. The main purpose of the Favor operating system is to support the D-RMTP-specific features by original APIs.

For example, to switch contexts, the Favor operating system issues the `swapth` instruction that directly controls the context switch function for the context cache on the D-RMTP. Using the `swapth` instruction, the overhead of the context switch by the context cache is remarkably reduced compared with that by the normal software load/store instructions. The thread-control instructions on the D-RMTP are given as follows:

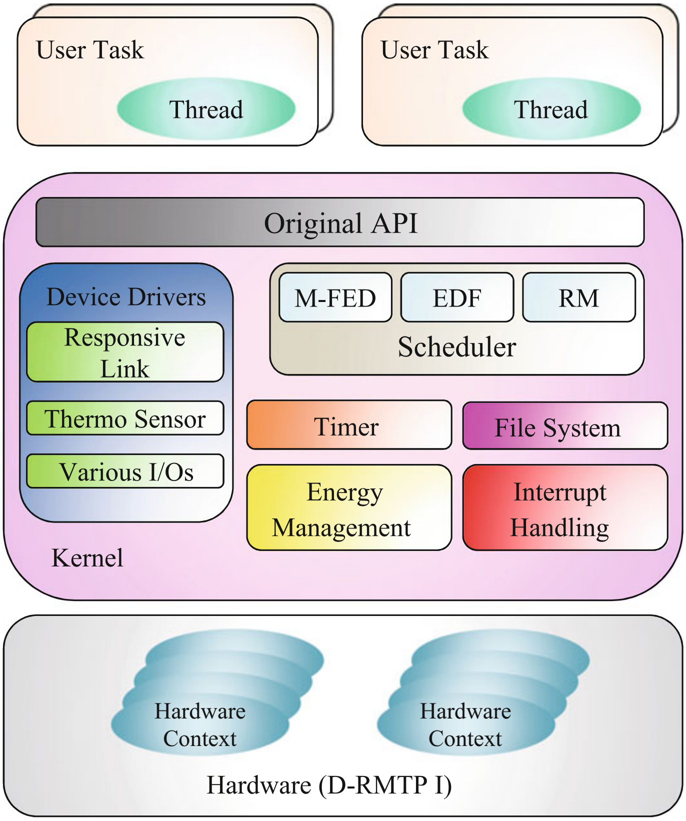


Fig. 24.8 Favor operating system

- `mkth` instruction creates a new thread.
- `delth` instruction deletes the specified thread.
- `runth` instruction makes the specified thread run.
- `stopth` instruction makes the specified thread stop.
- `stopslf` instruction makes the thread itself stop.
- `bkupth` instruction saves the specified thread to the context cache.
- `bkupslf` instruction saves the thread itself to the context cache.
- `rstrth` instruction restores the specified thread from the context cache.
- `swapth` instruction swaps the specified running thread for the cached thread.
- `swapslf` instruction swaps the thread itself for the cached thread.

The Favor operating system implements real-time scheduling algorithms including the RM and EDF algorithms [12]. In addition, the Favor operating system supports an imprecise computation model [11], which is an effective technique to improve the QoS making use of the remaining processor time. The imprecise computation model has a mandatory real-time part and an optional non-real-time part. The execution of the optional part is restricted only after the completion of the mandatory part. Therefore, real-time applications based on the imprecise computation model can provide the correct result with lower quality to terminate the optional part of each task, which avoids its deadline miss. The Favor operating system also implements the M-FED (Mandatory-First with Earliest Deadline) [2], which is an EDF-based real-time scheduling algorithm in the imprecise computation model. Under the M-FED algorithm, mandatory and optional parts are both scheduled by the EDF algorithm. The mandatory parts have higher priorities than the optional parts so that the Favor operating system has a real-time ready queue for mandatory parts and a non-real-time ready queue for optional parts.

The Favor operating system implements multiprocessor partitioning policies (e.g., first-, next-, best-, and worst-fit), which assign tasks to a logical processor (a hardware context) statically and do not allow them to migrate among logical processors dynamically. The Favor operating system implements the PM (Partitioned Rate Monotonic) algorithm [16] and the P-EDF (Partitioned Earliest Deadline First) algorithm [13] to achieve high real-time capacities.

The Favor operating system has device drivers including *Responsive Link* for real-time communication, thermosensors for the TA-DVFS [10], and various computer I/O peripherals for control. In addition, the Favor operating system supports not only the TA-DVFS but also the DVFS because there is a trade-off with respect to the energy consumption and overhead between the TA-DVFS and the DVFS. The TA-DVFS usually has lower energy consumption and higher overhead than the DVFS because the TA-DVFS changes the temperature, which incurs non-negligible overhead.

The Favor operating system supports the experimental environment of trade-off between the energy consumption by TA-DVFS and the quality of task by the imprecise computation. If the energy consumption is lower, the quality of task is lower and vice versa. Using the Favor operating system, robotic applications can be performed with proper energy consumption and quality of tasks. For example, if the robotic application requires very low energy consumption and is allowed to perform in low quality of task, the application developers can set low levels for energy consumption and quality of task.

24.4.2 RTRON Operating System

Figure 24.9 shows the overview of the RTRON (Responsive TRON) operating system [21]. The RTRON operating system, which is based on the Hyper Operating System [7] with the ITRON specification [19], has been developed. The goal of the RTRON operating system is to support the D-RMTP-specific features from the ITRON-specification APIs so that ITRON users can develop and maintain such applications easily. Examples of the ITRON APIs in the RTRON operating system are as follows.

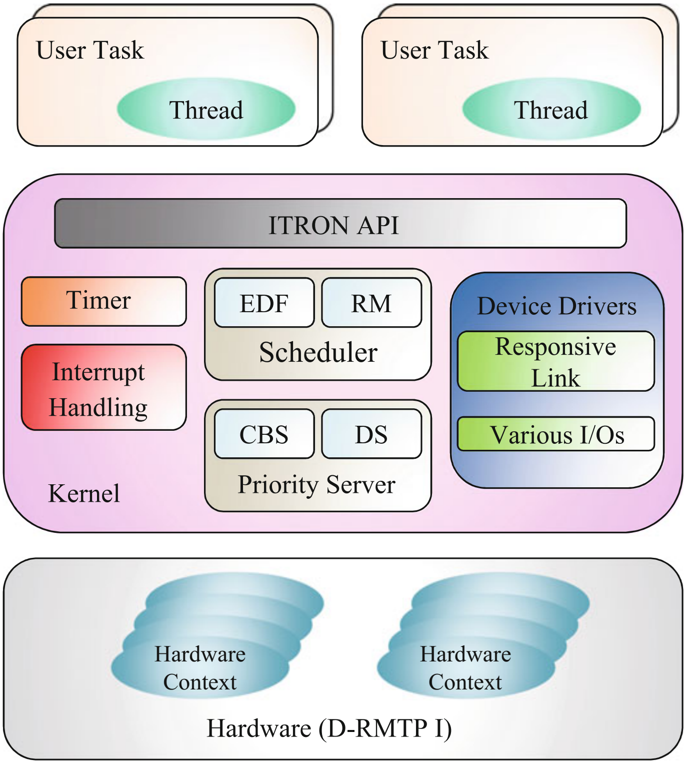


Fig. 24.9 RTRON operating system

- `act_tsk` function creates tasks (i.e., issues the `mkth` instruction in the D-RMTP-specific features).
- `pol_sem` function gets the semaphore by polling.
- `wup_tsk` function wakes up task.
- `sig_sem` function puts the semaphore to operating system.
- `ter_tsk` function terminates the task forcefully.

The RTRON OS, as well as the Favor OS, implements traditional real-time scheduling algorithms such as the RM and EDF algorithms and multiprocessor partitioning policies such as the P-RM and P-EDF algorithms.

In addition, the RTRON operating system supports priority servers, which schedule aperiodic tasks by priority to improve *response time*. The definition of response time is the time from when the task releases till when the task finishes. If the response time is shorter, the performance of the priority server is higher. The DS (Deferrable Server) [17] and CBS (Constant Bandwidth Server) [1] algorithms are implemented in the RTRON operating system. The DS algorithm is a fixed-priority server and creates a periodic task for serving aperiodic tasks with respect to polling service. Under the DS algorithm, periodic tasks are scheduled by the RM algorithm. In contrast, the

CBS algorithm is a dynamic-priority server and efficiently implements a bandwidth preserving strategy to improve the response time. Under the CBS algorithm, periodic tasks are scheduled by the EDF algorithm. There is a trade-off between response time and overhead in the DS and CBS algorithms. The response time of the DS algorithm is longer than that of the CBS algorithm and the overhead of the DS algorithm is lower than that of the CBS algorithm.

The RTRON operating system manages periodic and aperiodic tasks scheduled by these algorithms to meet their deadlines and improve response time. Since there are eight hardware contexts on the D-RMTP, the RTRON operating system manages the hardware contexts as follows.

- Hardware context 1: The hardware context dedicates the timer interrupt for scheduler invocation.
- Hardware context 2: The hardware context dedicates other timer interrupts except the timer interrupt for assigning aperiodic tasks to the hardware contexts 3–8.
- Hardware contexts 3–8: The hardware contexts execute periodic and aperiodic tasks as user tasks.

The purpose of the scheduler-dedicated and interrupt-dedicated hardware contexts (hardware contexts 1 and 2) is to reduce the interrupt response time for real-time processing. Using these dedicated hardware contexts, the worst-case interrupt response time is almost constant regardless of the number of tasks. In addition, the user hardware contexts (hardware contexts 3–8) execute periodic and aperiodic tasks scheduled by the RM and DS algorithms or the EDF and CBS algorithms, respectively.

24.5 Summary

This chapter introduced the D-RMTP SoC/SiP, *Responsive Link*, and the Favor and RTRON operating systems for dependable distributed real-time systems.The D-RMTP has the RMT PU to achieve real-time processing and high-throughput enabled by the prioritized SMT architecture with the IPC control mechanism for dependable processing. The D-RMTP supports *Responsive Link* to have the distributed nodes (processors) networked for dependable real-time communication. The Favor and RTRON operating systems implement real-time scheduling algorithms including the RM and EDF and various QoS techniques on the D-RMTP. These operating systems can make use of the D-RMTP-specific features to achieve dependable processing and communication. These technologies will prove to be useful in realizing hard real-time applications including robotics.

References

1. L. Abeni, G. Buttazzo, Integrating multimedia applications in hard real-time systems, in *Proceedings of the 19th IEEE Real-Time Systems Symposium* (1998), pp. 4–13
2. S.K. Baruah, M.E. Hickey, Competitive On-line Scheduling of Imprecise Computations. IEEE Trans. Comput. **47**, 1027–1033 (1996)
3. H. Chishiro, A. Takeda, K. Funaoka, N. Yamasaki, Semi-fixed-priority scheduling: New priority assignment policy for practical imprecise computation, in *Proceedings of the 16th IEEE International Conference on Embedded and Real-Time Computing Systems and Applications* (2010), pp. 339–348
4. H. Chishiro, N. Yamasaki, Global semi-fixed-priority scheduling on multiprocessors, in *Proceedings of the 17th IEEE International Conference on Embedded and Real-Time Computing Systems and Applications* (2011), pp. 218–223
5. F. Consortium, FlexRay Communications System—Protocol Specification v3.0. (2009), http://www.flexray.com/
6. Y. Fujita, S. Kato, N. Yamasaki, Real-time communication and admission control over responsive link, in *The IASTED International Conference on Parallel and Distributed Computing and Networks* (2008), pp. 131–138
7. Hyper Operating System (ITRON Specification OS). Cited 7 July 2014, http://sourceforge.jp/projects/hos/
8. B. Inagaki, N. Yamasaki, An IPC control mechanism for real-time system on a prioritized smt processor. IPSJ J. **51**(12), 2206–2215 (2010)
9. ISO 11898, Road vehicles—Interchange of digital information—Controller area network (CAN) for high-speed communication (1993)
10. D. Li, H.C. Chang, H.K. Pyla, K.W. Cameron, System-level, Thermal-aware, Fully-loaded Process Scheduling, in *Proceedings of the IEEE International Parallel and Distributed Processing Symposium* (2008), pp. 1–7
11. K. Lin, S. Natarajan, J. Liu, Imprecise results: Utilizing partial computations in real-time systems, in *Proceedings of the 8th IEEE Real-Time Systems Symposium* (1987), pp. 210–217
12. C.L. Liu, J.W. Layland, Scheduling algorithms for multiprogramming in a hard real-time environment. J. ACM **20**(1), 46–61 (1973)
13. J.M. Lopez, M. Garcia, J.L. Diaz, D.F. Garcia, Worst-case utilization bound for EDF scheduling on real-time multiprocessor systems, in *Proceedings of the 12th Euromicro Conference on Real-Time Systems* (2000), pp. 25–33
14. K. Mizotani, Y. Hatori, Y. Kumura, M. Takasu, H. Chishiro, N. Yamasaki, An integration of imprecise computation model and real-time voltage and frequency scaling on responsive multithreaded processor. Int. J. Comput. Appl. **22**(3), 127–135 (2015)
15. I. Mizuuchi, Y. Nakanishi, Y. Sodeyama, Y. Namiki, T. Nishino, N. Muramatsu, J. Urata, K. Hongo, T. Yoshikai, M. Inaba, Advanced Musculoskeletal Humanoid Kojiro, in *Proceedings of the 2007 IEEE-RAS International Conference on Humanoid Robots* (2007), pp. 294–299
16. D. Oh, T.P. Baker, Utilization Bounds for N-Processor Rate Monotone Scheduling with Static Processor Assignment. Real-Time Systems **15**(2), 183–192 (1998)
17. J.K. Strosnider, J.P. Lehoczky, L. Sha, The deferrable server algorithm for enhanced aperiodic responsiveness in hard real-time environments. IEEE Trans. Comput. **44**(1), 73–91 (1995)
18. K. Suito, R. Ueda, K. Fujii, T. Kogo, H. Matsutani, N. Yamasaki, Dependable Responsive Multithreaded Processor for Distributed Real-Time Systems. IEEE Micro **32**(6), 52–61 (2012)
19. H. Takada, μ ITRON 4.0 Specification. TRON Institute (2004)
20. D.M. Tullsen, S.J. Eggers, H.M. Levy, Simultaneous multithreading: maximizing on-chip parallelism, in *Proceedings of the 22nd Annual International Symposium on Computer Architecture* (1995), pp. 392–403
21. R. Ueda, K. Fujii, H. Chishiro, H. Matsutani, N. Yamasaki, Implementation of ITRON specification OS for RMT processor. IPSJ J. **54**(7), 1835–1848 (2013)

22. K. Wada, S. Hino, N. Yamasaki, Three-dimensional packaging structure for 3d-NOC, in *EDAPS 2013–2013 IEEE Electrical Design of Advanced Packaging Systems Symposium* (2013), pp. 72–75. https://doi.org/10.1109/EDAPS.2013.6724392
23. N. Yamasaki, Responsive link for distributed real-time processing, in *Proceedings of the 10th International Workshop on Innovative Architecture for Future Generation High-Performance Processors and Systems* (2007), pp. 20–29
24. N. Yamasaki, I. Magaki, T. Itou, Prioritized SMT architecture with IPC control method for real-time processing (2007)
25. T. Yamazaki, Y. Sogawa, R. Yoshino, K. Kata, I. Hazeyama, S. Kitajo, Real chip size three-dimensional stacked package. IEEE Trans. Adv. Packag. **28**(3), 397–403 (2005)

Chapter 25
A Low-Latency DMR Architecture with Fast Checkpoint Recovery Scheme Using Simultaneously Copyable SRAM

Masahiko Yoshimoto, Go Matsukawa, Yohei Nakata, Hiroshi Kawaguchi, Yasuo Sugure and Shigeru Oho

Abstract This chapter presents a novel architecture for a fault-tolerant and dual modular redundancy (DMR) system using a checkpoint recovery approach. The architecture features exploitation of SRAM with simultaneous copy and instantaneous compare function. It can perform low-latency data copying between dual cores. Therefore, it can carry out fast backup and rollback. Furthermore, it can reduce the power consumption during data comparison process compared to the Cyclic Redundancy Check (CRC). Evaluation results show that compared with the conventional checkpoint/restart DMR, the proposed architecture reduces the cycle overhead by 97.8% and achieves a 3.28% low-latency execution cycle even if a one-time fault occurs when executing the task. The proposed architecture provides high reliability for systems with a real-time requirement.

Keywords Dual modular redundancy • Checkpoint recovery • Fault-tolerance Dual-core lock-step • Simultaneous copy

25.1 Introduction

Microprocessors are key components used widely for various applications. Particularly, those used in safety-critical systems such as vehicles and social infrastructure are required to operate with high reliability. Nevertheless, processors are

M. Yoshimoto (✉) · G. Matsukawa · Y. Nakata · H. Kawaguchi
Kobe University, Kobe, Japan
e-mail: yosimoto@cs.kobe-u.ac.jp

Y. Sugure
Hitachi, Ltd., Kokubunji, Japan

S. Oho
Nippon Institute of Technology, Minami-Saitama, Saitama, Japan

S. Asai (ed.), *VLSI Design and Test for Systems Dependability*,
https://doi.org/10.1007/978-4-431-56594-9_25

becoming increasingly more sensitive to soft errors, power supply noise, and temperature fluctuation with technology scaling of device sizes. These factors engender faults in the processor so that it is necessary to detect faults and to recover from a faulty state even if faults occur in the processor.

Dual Modular Redundancy (DMR) with a recovery scheme has been applied to reliable processor designs to detect faults [1–4]. Two cores in the DMR processor execute the same task in parallel. The processor detects faults by comparing states of the cores (register values and stored data in the memory) at every checkpoint. If the states match, then the register values of the cores are copied into backup shadow registers for subsequent recovery process. If the states differ, then the cores load the shadow register values to recover the recent fault-free state. The checkpoint and recovery technique enables detection of faults, but the loading of these values for recovery implies additional latency. A conventional DMR architecture uses a Cyclic Redundancy Check (CRC) code for comparison and bus transfer for the copying of register values [5]. Fault detection capability by means of the comparison of CRC code depends on the fault location. The bus transfer is processed sequentially so that the bus transfer latency increases with increasing number of registers. Therefore, CRC code is not suitable for real-time applications such as vehicle control systems.

Several time-redundancy methods for fault-tolerant systems have been proposed [6, 7]. Although the use of time-redundancy is superior to modular redundancy such as DMR and triple module redundancy (TMR) with respect to area overhead, time-redundancy methods have a large cycle penalty. Thus, it is not practical either to use time-redundancy methods to microprocessors for real-time systems.

Herein, we propose a DMR architecture that has a low-latency recovery scheme. To realize low latency, the proposed DMR architecture exploits block-level simultaneously copyable SRAM. In addition, this architecture improves the fault detection capability.

25.2 Proposed DMR Architecture with a Recovery Scheme

In this section, we present an overview of the proposed DMR architecture with a recovery scheme. Then, the checkpoint/restart scheme is explained. Finally, we explain the differences from conventional DMR. Figure 25.1 portrays the proposed DMR architecture, which consists of two cores, an instantaneous comparison buffer, and a DMR controller. The proposed architecture executes the normal operation using data stored in working memory, store queue, and working register. Then, store data and write data to register are written to the store queue or working register, respectively, and are written simultaneously in the instantaneous comparison buffer. As shown in Fig. 25.2, normal operations are performed during

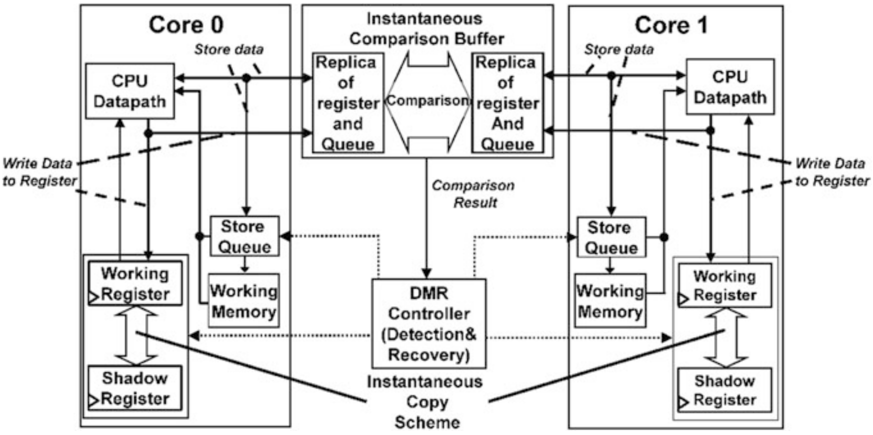


Fig. 25.1 Proposed DMR architecture with recovery scheme

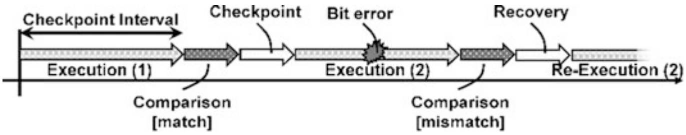


Fig. 25.2 Execution with checkpoint and recovery

checkpoint intervals. The instantaneous comparison buffer compares both replicas of the register and queue in the core during a comparison period. Figure 25.3 depicts a data transfer between the store queue and the working memory. Store queue has a dirty bit for each block of store queue and the dirty bit indicates whether the corresponding block of store queue has been overwritten or not. If data required for processing exists in store queue and the corresponding dirty bit is “1”, the data in store queue are used for processing. If data required exists in store queue and the corresponding dirty bit is “0”, the data in work memory are used because new data should be used for processing. The comparison result is transferred to the DMR controller. If the result of the comparison is a match, then all the data of the store queue are written in the working memory in the next normal operation (Fig. 25.3a). Data of the working register are copied in the shadow register using the simultaneous data copy and dirty bits remain unchanged. If the result of the comparison is a mismatch, then the store queue data are erased and the data of the shadow register are transferred to the working register (Fig. 25.3b). Dirty bits are set to “0” because there is the possibility that errors have occurred in the store queue. Then, the process restarts from the latest checkpoint.

The conventional copying between the working register and shadow register is executed via the shared bus, but the latency rises in proportion to the number of

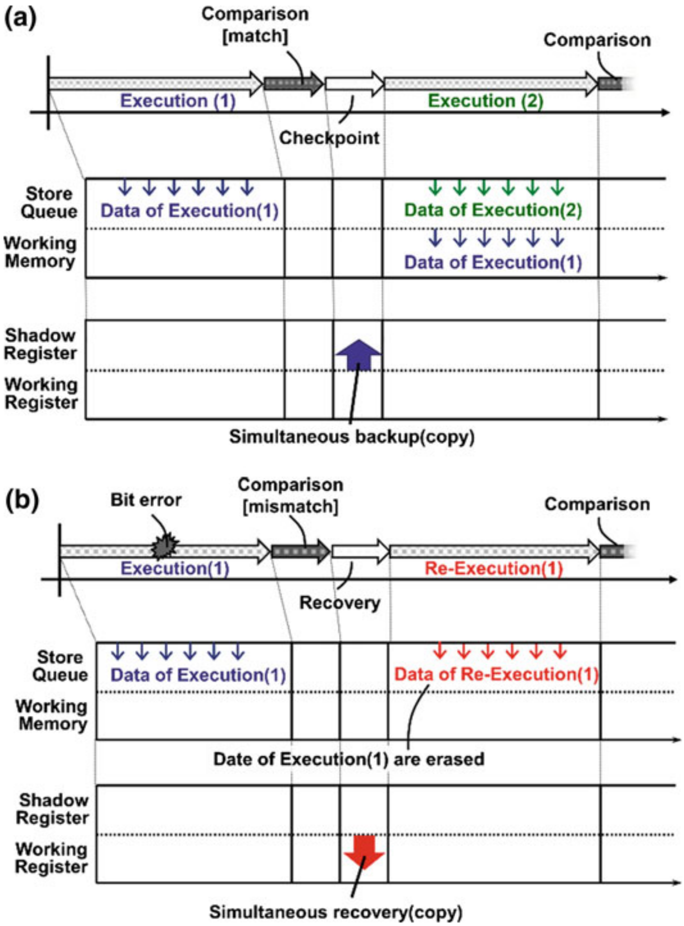


Fig. 25.3 Data transfer between store queue and working memory: **a** comparison match and **b** comparison mismatch

registers. Moreover, normal comparison data between the dual cores is performed via the bus, so that the latency increases with increasing size. Although the comparison of CRC codes is also often used to reduce the number of comparison cycles, CRCs may be useless in case of multi-bit errors.

The proposed architecture is effective against transient faults such as soft errors and read/write margin failures. On the other hand, permanent fault cannot be recovered, because this architecture will repeat the fault detection and recovery process in the event of a permanent fault. There are some cases that a transient error causes an infinite loop. For example, when a comparison results in a mismatch and a transient error upsets a flip-flop in the DMR controller, this architecture will enter an infinite loop. However, the probability that a transient error occurs in the DMR controller while the comparison results in a mismatch is extremely low.

25.3 Instantaneous Comparison and Simultaneous Copy

A. SRAM with simultaneous copy and compare function

Figure 25.4 illustrates a schematic of a pair of 6T bitcells, which realizes a simultaneous copy and the instantaneous comparison function [8]. The pair of 6T bitcells mutually is connected with each other in their internal nodes using pMOS transistors. The area overhead of the bitcell pairs relative to a conventional 6T bitcell pair is 11%.

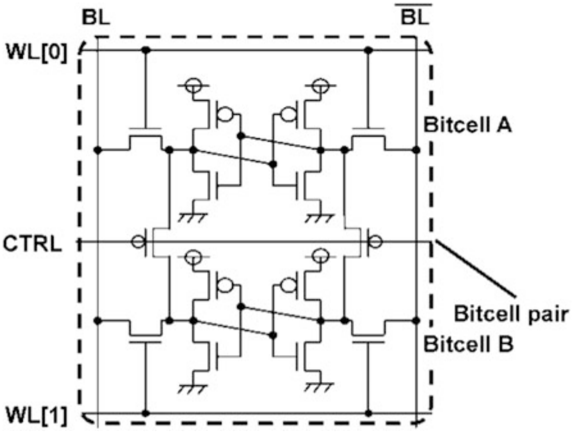
B. Instantaneous comparison

The instantaneous comparison process is explained using Fig. 25.5. In comparing data, the connecting pMOS transistors are turned on by lowering the CTRL signal [9]. If a 6T bitcell pair retains different data, then supply current flows into the ground. On the contrary, if it retains the same data, then the supply current does not flow through the bitcell pair because no current paths exist. The comparison is made instantly in all 6T bitcell pairs. The details of compare operation are presented in [9]. It takes four cycles to realize an instantaneous comparison independent of the size of the comparison buffer. The conventional data comparison using the CRC code can be accomplished in two cycles so that allowing shorter cycle overhead. On the other hand, a simulation has revealed that the proposed comparison scheme consumes only 0.21% of power required for a CRC comparison circuit because it does not require complex calculation [10]. However, the drawback of this comparison scheme is that its area overhead increases in proportion to the size of the instantaneous comparison buffer.

C. Simultaneous copy scheme

The simultaneous copy scheme is extremely effective for the reduction of latency for the checkpoint and recovery state. Figure 25.6 depicts the simultaneous copy scheme between the working register and shadow register. The process of copy

Fig. 25.4 Schematic of SRAM



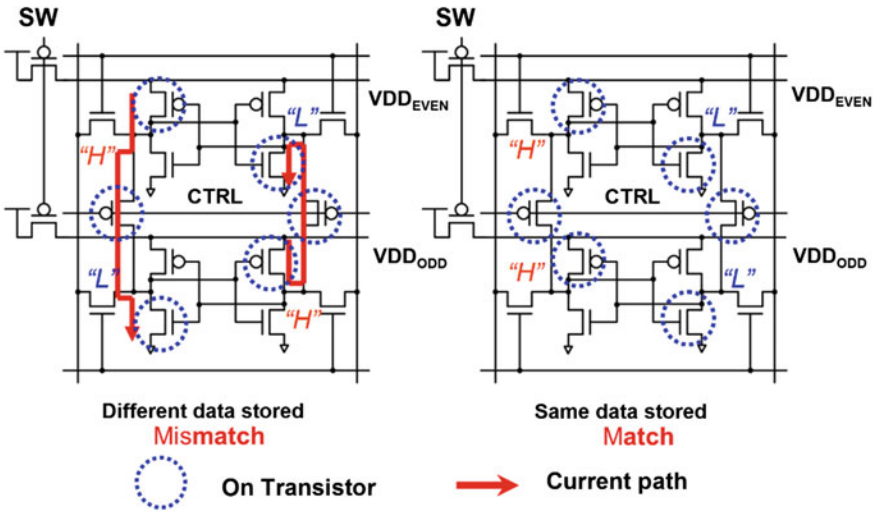


Fig. 25.5 A 6T bitcell pair performing an instantaneous comparison

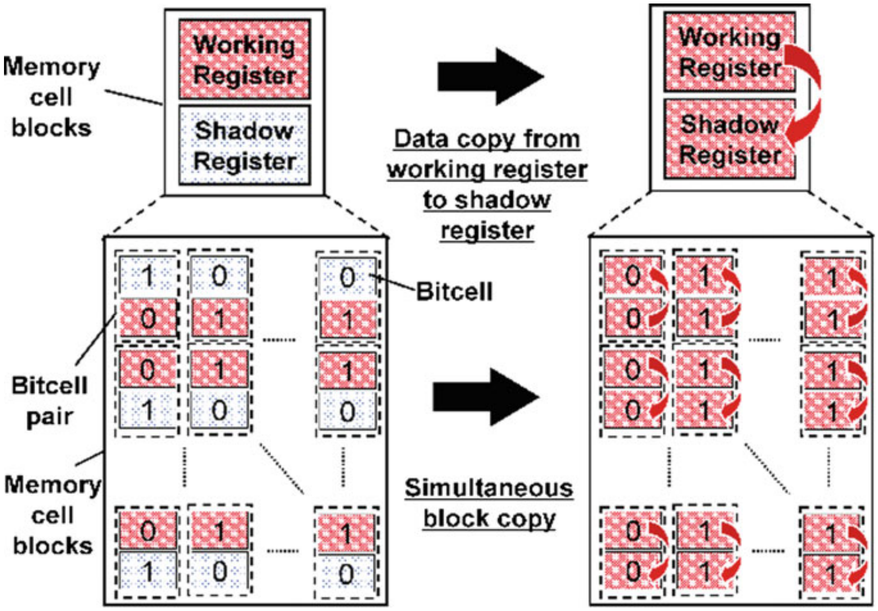


Fig. 25.6 Simultaneous copy scheme

operation between 6T bitcell pair is explained in [10] in detail. The checkpoint data can be backed-up or restored simultaneously using no shared bus, but all 6T bitcell pairs. Consequently, the proposed SRAM structure requires only four cycles regardless of the size of registers for the simultaneous block copy.

25.4 Evaluation Results

The evaluated cycle overhead in the DMR phase is presented in Fig. 25.7. The number of registers is set to 360 so that the processor performs high-speed interrupt handling for real-time system. The conventional DMR executes a comparison using CRC. Although the conventional copying between the registers via a shared bus requires 360 cycles, the proposed DMA takes four cycles to copy using a SRAM with simultaneous copy function. Totally the conventional DMR architecture needs 362 cycles in the DMR phase. In contrast, the proposed architecture requires eight cycles for comparison and copy, and thus reduces the number of clock cycles required down to the 0.2% of that required for the conventional DMR using the shared bus.

In Figs. 25.8a, b, the y-axis shows the cycle penalty with the checkpoint recovery approach and the x-axis shows the checkpoint interval, which is the number of cycles between two consecutive checkpoints. Here it is assumed that the execution time of the task is 500 μs and the cycle time is 16 ns. Figure 25.8a represents the cycle penalty of execution of a task that is fault-free. As the checkpoint interval decreases, the cycle penalty increases rapidly because comparison and copy are performed frequently. In the proposed architecture, cycle penalty increases slightly when the checkpoint period is short because it dramatically reduces the cycle overhead in the copy operation. When the checkpoint interval increases, both the cycle penalties of conventional and proposed architectures are low. Figure 25.8b shows the case where a fault occurs in executing the task once. Since a failure occurs in the working register and the comparison result is "unmatched", a rollback checkpoint period (re-execution) has to be inserted. Figure 25.8b shows that the cycle penalty increases as the checkpoint interval becomes longer because the re-execution time is proportional to the checkpoint interval. The minimum cycle penalty of the conventional DMR and proposed DMR are 22.6% and 3.28%, respectively, in this case.

Figure 25.9 shows the cycle penalty when multiple mismatches occur. The number of mismatches stands for a comparison result mismatches while executing a

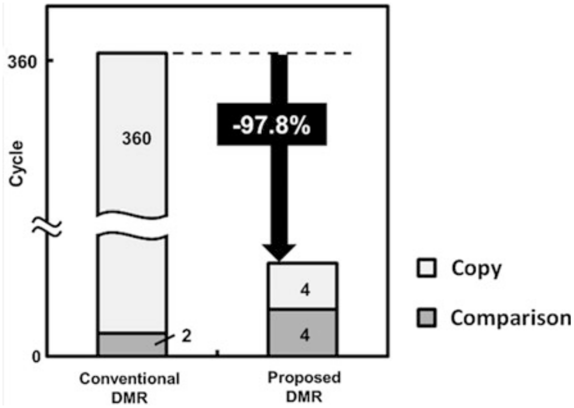


Fig. 25.7 The number of machine cycles for copy and comparison, where the number of working registers is 360

Fig. 25.8 Cycle penalty with respect to the checkpoint interval: **a** fault-free and **b** occurrence fault once

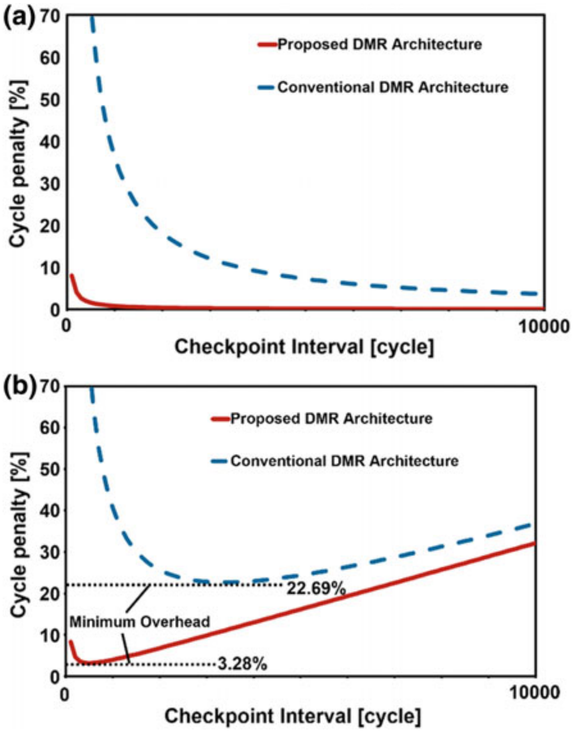
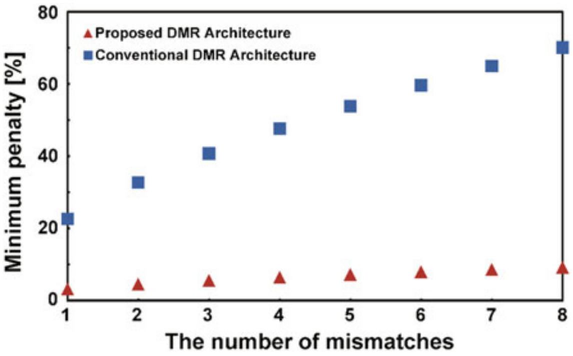


Fig. 25.9 Cycle penalty with respect to the checkpoint interval: multiple mis-matches occur



task, which is equal to the number of times that rollback is done. The figure shows that the conventional DMR requires a larger cycle penalty under more frequently soft errors or power supply noise. However, the proposed DMR can keep minimum cycle penalty low, even if the rollback is performed many times. Here, we assume the checkpoint interval is set to the optimal checkpoint interval for each the number of mismatches. Table 25.1 gives the optimal checkpoint intervals when the number

Table 25.1 The optimal checkpoint interval that minimizes the cycle penalty

No. of mismatches	Optimal checkpoint interval [cycle]	
	Prop. architecture	Conv. architecture
1	500	3363
2	354	2378
3	289	1941
4	250	1682
5	224	1504
6	204	1373
7	189	1271
8	176	1189

of mismatches is varied; in the proposed DMR, the optimal checkpoint interval is much smaller than the conventional DMR. The cycle penalty is given by Eq. (25.1):

$$\text{cyclepenalty} = \left(\frac{T_{DMR}}{T_{checkpoint}} + N \times \frac{T_{DMR} + T_{checkpoint}}{T_{task}}\right) \times 100, \tag{25.1}$$

where T_{DMR} is a cycle count overhead in the DMR phase, $T_{checkpoint}$ is a cycle count of the checkpoint interval, T_{task} is an execution cycle count of the task with fault-free, and N is the number of mismatches. If the checkpoint interval of the proposed DMR is set to be 500 cycles, the cycle penalty is 14.6% when a mismatch occurs 8 times. On the other hand, in the conventional DMR, the respective optimal checkpoint intervals are remarkably different from one another, so it is difficult to get closer to a minimum cycle penalty. For example, if the checkpoint interval is set to be 3363 cycles which is the optimal interval when one mismatch occurs, the cycle penalty is 106% when a mismatch occurs eight times. Thus, the proposed architecture is suitable for real-time system because it can keep the cycle penalty lower.

25.5 Conclusion

We have proposed a DMR architecture that can conduct an instantaneous comparison and a simultaneous copy scheme using novel SRAM cell configuration. The proposed DMR architecture realizes high-speed copying using a simultaneous copy scheme and low power consumption using instantaneous comparison. The proposed architecture can execute operations with low latency even if the checkpoint interval becomes short. Consequently, the proposed DMR architecture provides benefits for real-time system s. Simultaneous copy scheme is useful for applications which requires high-speed data backup. It is expected that the proposed architecture is implemented to microcontroller for automobile application including collision detection of airbag systems.

References

1. J. Teifel, Self-voting dual-modular-redundancy circuits for single-event-transient mitigation. IEEE Trans. Nucl. Sci. (TNS) **55**, 3435–3439 (2008)
2. A. Ziv, J. Bruck, Performance optimization of check-pointing schemes with task duplication. IEEE Trans. Comput. (TC) **46**, 1381–1386 (1997)
3. Y. Zhang, K. Chakrabarty, Energy-aware adaptive checkpointing in embedded real-time systems, in *Proceedings of Design Automation and Test in Europe (DATE)*, pp. 918–923 (2003)
4. T. Sakata, T. Hirotsu, H. Yamada, T. Kataoka, A cost-effective dependable microcontroller architecture with instruction-level rollback for soft error recovery, in *Proceedings of IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, pp. 256–265 (2007)
5. J.C. Smolens, B.T. Gold, B. Falsafi, J.C. Hoe, Reunion: complexity-effective multicore redundancy, in *Proceedings of IEEE/ACM International Symposium on Microarchitecture (MICRO)*, pp. 223–234 (2006)
6. W.J. Townsend, J.A. Abraham, E.E. Swartzlander, Quadruple time redundancy adders, in *Proceedings of IEEE International Symposium on Defect and Fault Tolerance in VLSI Systems (DFT*), pp. 250–256 (2003)
7. J. Chen, Y. Yang, A minimum proportional time redundancy based checkpoint selection strategy for dynamic verification of fixed-time constraints in grid workflow systems, in *Proceedings of Asia-Pasific Software Engineering Conference (APSEC)*, pp. 299–306 (2005)
8. S. Okumura, S. Yoshimoto, K. Yamaguchi, Y. Nakata, H. Kawaguchi, M. Yoshimoto, 7T SRAM enabling low-energy simultaneous block copy, in *Proceedings of IEEE Custom Integrated Circuits Conference (CICC)* (2010)
9. H. Fujiwara, S. Okumura, Y. Iguchi, H. Noguchi, H. Kawaguchi, M. Yoshimoto, A 7T/14T dependable SRAM and its array structure to avoid half selection, in *Proceedings of International Conference on VLSI Design*, pp. 295–300 (2009)
10. S. Okumura, Y. Nakata, K. Yanagida, Y. Kagiyama, S. Yoshimoto, H. Kawaguchi, M. Yoshimoto, Low-power block-level instantaneous comparison 7T SRAM for dual modular redundancy, in *Proceedings of IEEE Custom Integrated Circuits Conference (CICC)* (2011)

Chapter 26
A 3D-VLSI Architecture for Future Automotive Visual Recognition

Mitsumasa Koyanagi, Hiroaki Kobayashi, Takafumi Aoki, Toshinori Sueyoshi and Tadashi Kamada

Abstract 3D-VLSIs are indispensable to achieve future high-performance and low-power systems for automotive application which should be highly dependable. An image sensor system module with visual recognition function is required for future automatic driving vehicles. On the basis of the research being done by the authors, a conceptual 3D-VLSI image sensor system module for future automatic driving vehicle has been developed that uses heterogeneous 3D integration technology and 2.5D technology where a pair of 3D-stacked image sensors and 3D-stacked multicore processors are integrated on a silicon interposer. A 3D-stacked image sensor with four layers of CMOS image sensor layer, analog circuit layer, ADC layer, and interface circuit layer was designed and an extremely high frame rate of 10,000 flames/s was achieved by introducing a block-parallel architecture. A high-performance 3D-stacked multicore processor was designed for visual recognition and the possibility of achieving the high-performance of 5 TFlops and the low-power consumption of 5 W was evaluated using the fabricated prototype 3D-stacked multicore processor. In addition, it was also evaluated whether the high dependability of 80 Fit was achieved by introducing the self-test and self-repair function in the 3D-stacked multicore processor. A prototype multicore processor was built to demonstrate the basic feasibility of 3D integration.

Keywords 3D-VLSIs • 3D-VLSI image sensor • 3D-stacked multicore processor • System-level supervisor processor (Sys-SVP) • Triple modular redundant (TMR)

M. Koyanagi (✉) · H. Kobayashi · T. Aoki
Tohoku University, Sendai, Japan
e-mail: koyanagi@bmi.niche.tohoku.ac.jp

T. Sueyoshi
Kumamoto University, Kumamoto, Japan

T. Kamada
Denso Corporation, Kariya, Japan

S. Asai (ed.), *VLSI Design and Test for Systems Dependability*,
https://doi.org/10.1007/978-4-431-56594-9_26

26.1 3D-VLSI Image Sensor System for Automatic Driving Vehicle

Future automobiles will be equipped with various kinds of LSIs and sensors as shown in Fig. 26.1a. These LSIs and sensors will be eventually integrated into compact intelligent system modules to save spaces and reduce power consumption. A conceptual example of such intelligent system modules is a 3D-VLSI image sensor system module for automatic driving vehicle as shown in Fig. 26.1b where two 3D-stacked image sensors and 3D-stacked multicore processors are integrated on a silicon interposer [1, 2]. A 3D-stacked image sensor consists of CMOS image sensor layer, analog circuit layer, ADC layer, and interface circuit layer. A pair of 3D-stacked image sensors is necessary for the stereovision which is essential for the visual recognition such as obstacle detection. The baseline length which is the distance between the right image sensor and the left image sensor is a key factor in the stereovision using two 3D-stacked image sensors. A short baseline length of 12 mm was adopted to achieve a compact module size in our 3D-VLSI image sensor system module. Sufficient range accuracy is hard to obtain with such a short baseline length using conventional image sensors at the frame rate of 30 frames/s. A high frame rate of 10,000 frames/s was assumed to achieve the 3 m resolution at 100 m ahead in the distance measurement. Such a high frame rate is achieved by employing a 3D-stacked structure and a block-parallel architecture in image sensors. The resolution of image sensor was assumed SXGA (1280 × 1024 pixels). One frame of SXGA was divided into 5120 blocks. Each block consists of four layers (an image sensor block with 16 × 16 pixels, an analog circuit block, an ADC and an interface circuit block). These 5120 image sensor system blocks simultaneously operate in parallel to achieve the performance of 10,000 frames/s without increasing the power consumption. The assumed maximum power of 3D-stacked image sensor was 3 W.

Image processing is very important for future automatic driving vehicles. We adopted a new phase-only correlation (POC) method for the obstacle detection based on the stereovision since the POC gave rise to better accuracy than other methods such as SAD and NCC [3–5]. A high-performance and low-power

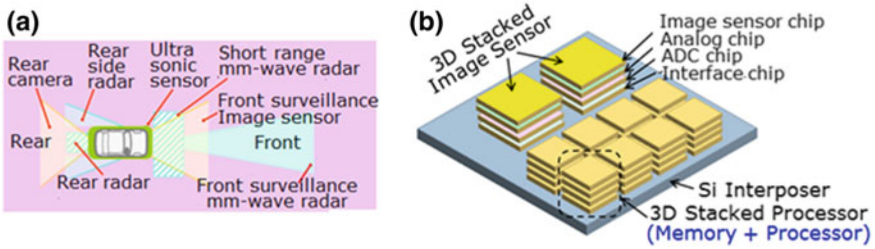


Fig. 26.1 Future automobile equipped with various LSIs and sensors (**a**) and 3D-VLSI image sensor system for automatic driving vehicle (**b**)

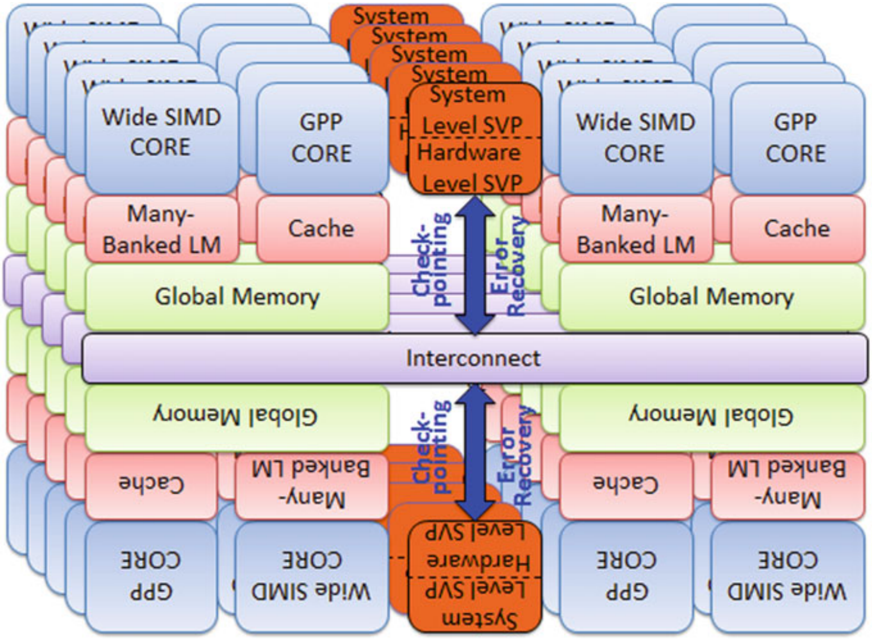


Fig. 26.2 Configuration of 3D-stacked multicore processor

processor is required to execute the real-time obstacle detection using a huge amount of data output from these 3D-stacked image sensors. A new multicore processor with a vector architecture and 3D-stacked structure as shown in Fig. 26.2 is proposed to achieve a high-performance of 5 TFlops and a low-power consumption of 5 W. It was confirmed by a software simulation that the performance of 5 TFlops and the power consumption of 5 W can be achieved in the 3D-stacked multicore processor which was designed specifically for the POC algorism with the 8 nm CMOS technology node [6, 7]. In addition to the high-performance and low power, a high dependability is very important in a processor for automobile application. We have therefore added the self-test and self-repair functions into the 3D-stacked multicore processor to achieve the high dependability of 80 Fits which was allotted considering the dependability of whole electronic system in an automobile. One of the core processors was used as a system-level supervisor processor (Sys-SVP) as shown in Fig. 26.3 to control the self-test and self-repair function and to supervise the task allocation and scheduling among core processors. The Sys-SVP was backed up by the hardware-level supervisor processor (HW-SVP) which was composed of reconfigurable circuits (FPGA) to guarantee the high dependability as shown in Fig. 26.4. The HW-SVP is highly fault tolerant based on a triple modular redundant (TMR) architecture where CPU and peripheral circuits are relocatable to spare regions and soft-errors are recovered by the recovery module [8, 9]. In such a 3D-stacked multicore processor with Sys-SVP and

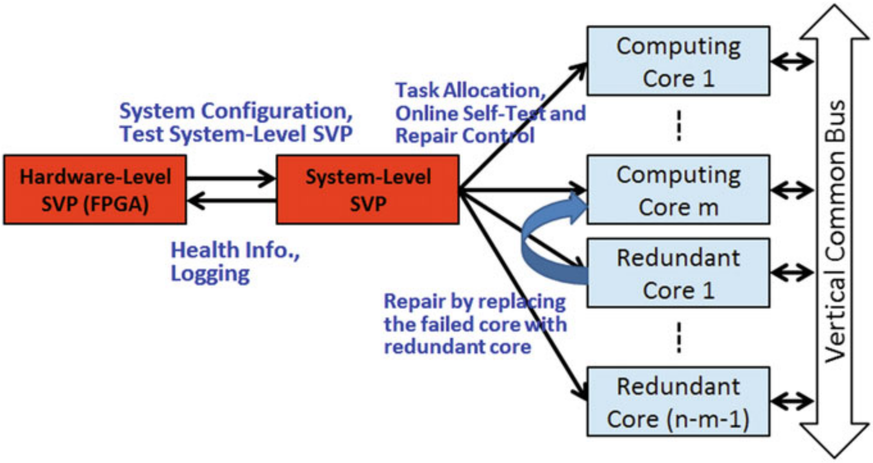

Hardware-Level SVP (FPGA)
System-Level SVP
System Configuration, Test System-Level SVP
Health Info., Logging
Task Allocation, Online Self-Test and Repair Control
Repair by replacing the failed core with redundant core
Computing Core 1
Computing Core m
Redundant Core 1
Redundant Core (n-m-1)
Vertical Common Bus

Fig. 26.3 Improvement of dependability by Sys-SVP and HW-SVP in 3D-stacked multicore processor

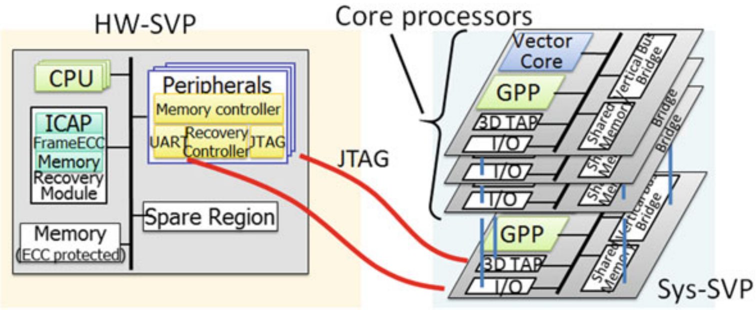


Fig. 26.4 Configuration of highly dependable 3D-stacked multicore processor using SVP for image processing

HW-SVP, built-in self-test (BIST) circuits are controlled through TAP (Test Access Port: JTAG) interface and failure cores are replaced by redundant cores [10]. We have introduced a new on-line self-test method called a cyclic test to increase the test coverage for self-test minimizing the overhead to performance. A sequence of task allocation in the cyclic test is shown in Fig. 26.5 where a frame period allocated to a core processor in each tier consists of test period, pop and push period, and processing period, and the test period is cyclically shifted to core processors in other tiers. We can increase the total test time by accumulating a number of the cyclic test periods and consequently increase the test coverage, and yet minimizing the overhead to performance. The checkpoint-restart function [11] was employed in the task allocation and scheduling for the cyclic test. However, the goal of 80 Fits was not achieved only by the cyclic test and then we introduced the TMR in

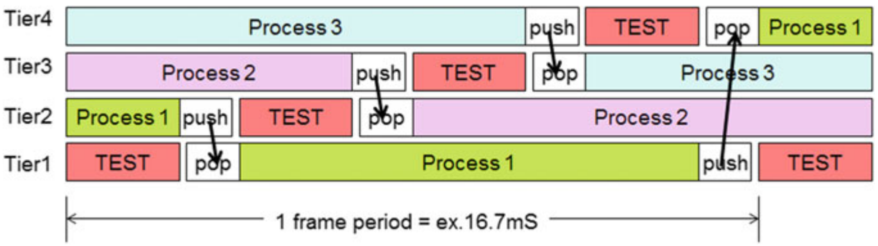
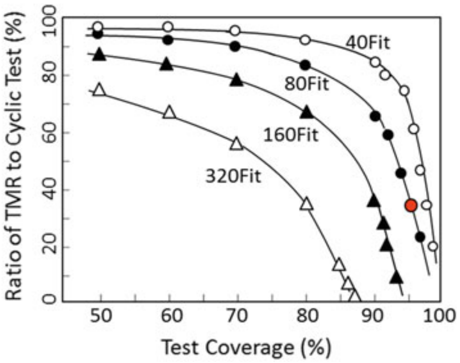


Fig. 26.5 Sequence of task allocation with cyclic test

Fig. 26.6 Relation between test coverage and ratio of TMR to cyclic test to obtain a specific fit number



addition to the cyclic test. As a result, it was confirmed that the goal of 80 Fits can be achieved by using BIST circuits with the test coverage of 95% and by combining TMR and cyclic test with the TMR ratio to cyclic test of 30% as shown in Fig. 26.6.

26.2 3D-Stacked Image Sensor for Stereo Vision

A prototype 3D-stacked CMOS image sensor with the resolution of QVGA (320 × 240 pixels) and the frame rate of 10,000 frames/s has been fabricated by the 3D integration technology with the backside via to evaluate its fundamental characteristics [12]. A configuration of a prototype 3D-stacked CMOS image sensor with a block-parallel architecture which contains a number of image signal processing elements is shown in Fig. 26.7 [13–17]. The 3D-stacked CMOS image sensor consists of four layers of image sensor, correlated double sampling (CDS) with programmable gain amplifier (PGA) array, ADC array, and interface circuit array. These layers are connected vertically by high density of TSVs. More detailed circuits for one image signal processing element which includes one-pixel block with 255 (16 × 16 − 1) pixels, one analog CDS/PGA, and one ADC with digital CDS are depicted in Fig. 26.8 where operational waveforms were also shown. To realize a global shutter function, optical signal charge integration takes place on all

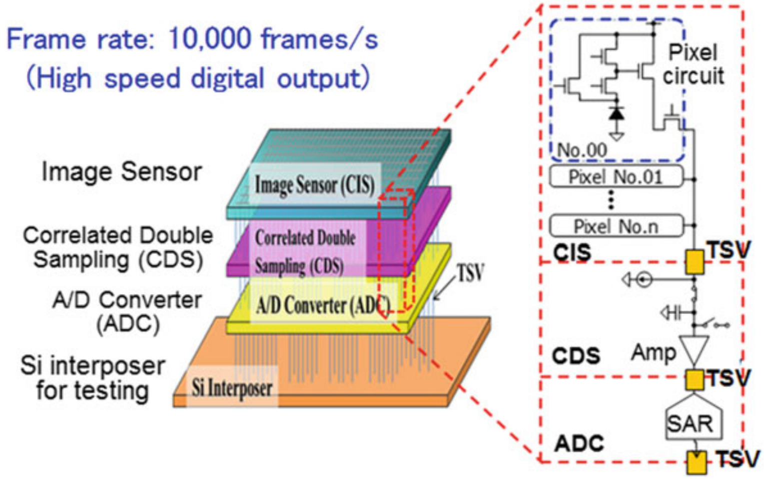


Fig. 26.7 Configuration of 3D-stacked CMOS image sensor

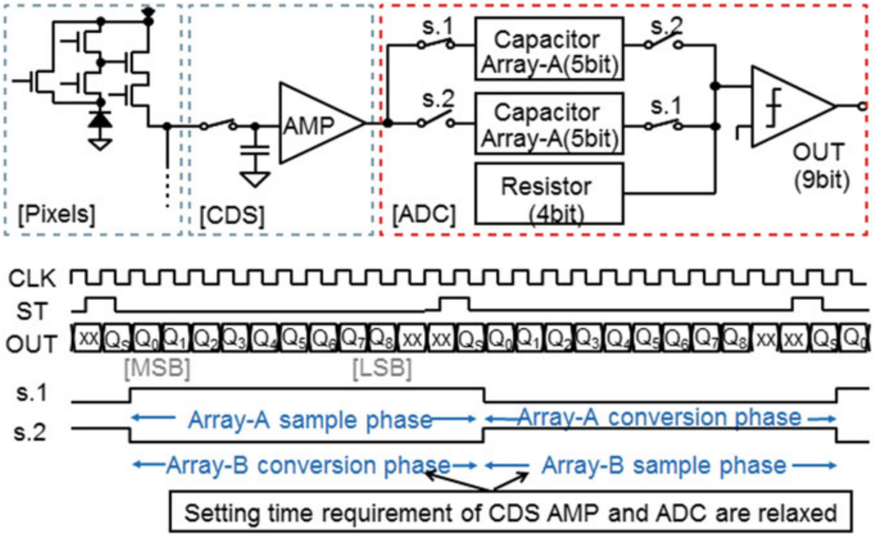


Fig. 26.8 Circuit configuration of one image signal processing element and operational waveforms

pixels in parallel. All pixels are light sensitive during the same period of time. In the readout phase, all pixel values are transferred simultaneously on the floating capacitor (diffusion capacitance) C_{FD} inside each pixel. All photodiodes PDs in one-pixel block are reset simultaneously after the signal charge integration. The signal charge integration and readout cycles can occur in parallel. The CMOS image sensor (CIS) layer and CDS layer were designed with a standard 0.18-μm CMOS image sensor and mixed-signal technologies, respectively. In our 3D-stacked CMOS image sensor, a fixed pattern noise (FPN) of pixel output is removed by analog CDS circuit, and in addition digital CDS is used to eliminate the FPNs (i.e., offset voltages) of CDS amplifier, PGA, and ADC in the digital domain. Such hierarchical double CDS has a high noise suppression capability because FPN cancellation is executed two times, once in the analog CDS and once in the digital CDS. We have employed a block-parallel architecture for ADC to convert a large amount of analog data from image sensors to digital data with high speed. This block-parallel ADC architecture employs a 9-bit time-interleaved successive approximation (SAR) ADC with digital noise cancellation circuit which includes a 9-bit register for data memory (signal register), a 9-bit register for stored FPN value (reference register), and a subtraction circuit. To eliminate the FPN, a digital CDS circuit is implemented for each ADC. For the A/D conversion, two data are used. First, FPN of the CDS source follower amplifier, PGA, and ADC stores a converted digital value into the reference register. During the A/D conversion, an image signal including FPN is converted into a digital signal, and the digital signal is stored into the signal register. The corrected output is obtained by subtracting the FPN value from the converted value. Since the pixel-level FPN is already removed within the analog CDS, the overall FPN is successfully suppressed by such hierarchical CDS method. The ADC was designed with a standard 90-nm 1-Poly 9-Metal CMOS technology. The designed chip consists of a 480 ADC array (one ADC unit including eight ADCs × 60). In our ADC, 9-bit resolution has been achieved in a small layout area of 150 × 160 μm^2. A set of ADC unit consists of eight ADCs, one ladder resistor, one reference circuit, and one timing controller for SAR logic, and then the ladder resistor, reference circuit, and timing controller are shared by eight ADCs [16]. The total circuit area for a set of ADC unit is 1280 × 160 μm^2. Consequently, the equivalent area of one ADC occupies 160 × 160 μm^2. The three-dimensional structure of designed 3D-stacked image sensor is depicted in Fig. 26.9. This 3D-stacked image sensor consists of four layers of image sensor, CDS, ADC, and interface (I/F) circuit and is integrated on a silicon interposer with redistribution lines (RDLs). Figure 26.10 shows X-ray CT scan image and SEM cross-sectional view of 3D-stacked image sensor fabricated by 3D integration

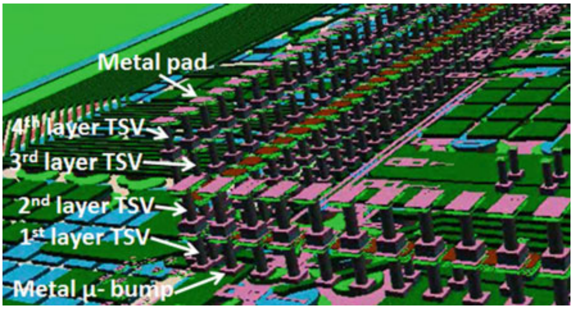


Fig. 26.9 Three-dimensional structure of designed 3D-stacked image sensor

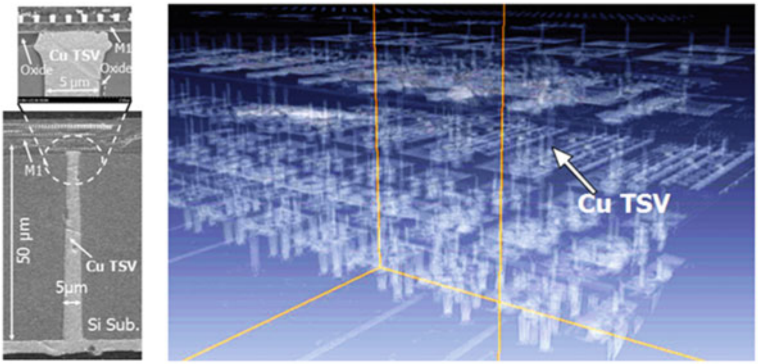


Fig. 26.10 X-ray CT scan image and SEM cross-sectional view of fabricated 3D-stacked image sensor

technology with the backside via. It is clearly seen in the X-ray CT scan image that four layers with many TSVs are vertically stacked. The die size of each layer is 5 × 5 mm^2 and each layer has approximately two thousands of TSVs. The thickness of Si substrate and the diameter of TSV are approximately 50 µm and 5 µm, respectively as is obvious from the SEM cross-sectional view.

Measured output waveforms from one-pixel block and one pixel are shown in Fig. 26.11. In this measurement, the amplitude of the output signal is about 250 mV which can be observed from reset level and the signal level. For this signal,

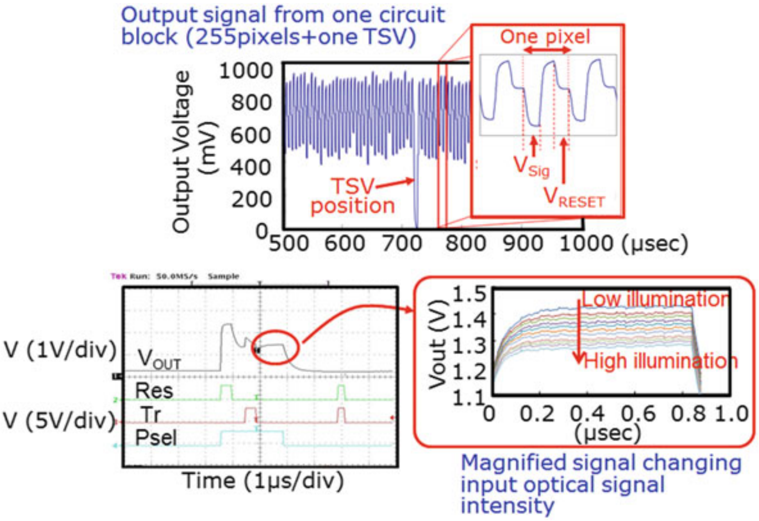


Fig. 26.11 Measured output waveforms from one-pixel block and one pixel in fabricated 3D-stacked image sensor

it was easy to perform analog CDS so as to achieve FPN cancellation. Fundamental characteristics of ADC in the fabricated 3D-stacked image sensor were also evaluated and it was confirmed that the differential nonlinearity (DNL) was within the range of −1.49/+1.89 LSB whereas the integral nonlinearity (INL) was within −1.92/+1.89 LSB. Furthermore, the peak Signal-to-Noise-and-Distortion ratio (SINAD) of 44.5 dB was obtained from the measured output spectrum of the ADC. In addition, it was confirmed that the FPN of about 10 mV offset voltage (digital code = 8–9 LSB) was eliminated by the digital CDS function. The power consumption of the ADC was as low as 387 μW at a supply voltage of 1 V and conversion rate of 4 MS/s. Thus, we confirmed the successful operation of fabricated prototype 3D-stacked image sensor.

26.3 3D-Stacked Dependable Multicore Processor

A prototype 3D-stacked dependable multicore processor has been fabricated by the 3D integration technology with the backside via to evaluate its fundamental characteristics [18–20]. The conceptual structure of this 3D-stacked multicore processor is illustrated in Fig. 26.12 which is a simplified structure of 3D-stacked multicore processor shown in Fig. 26.2. One of the core processors was used as a system-level supervisor processor (Sys-SVP) to control the self-test and self-repair function and to supervise the task allocation and scheduling among core processors. We designed a core processor for this prototype 3D-stacked multicore processor. A circuit block diagram and a die photo of core processor fabricated by a standard 90-nm 1-Poly 9-Metal CMOS technology are shown in Fig. 26.13. The die size is 5×5 mm^2. Several new circuits specific for 3D-stacked multicore processor such as vertical system bus bridge, 3D shared memory controller, and on-line self-test

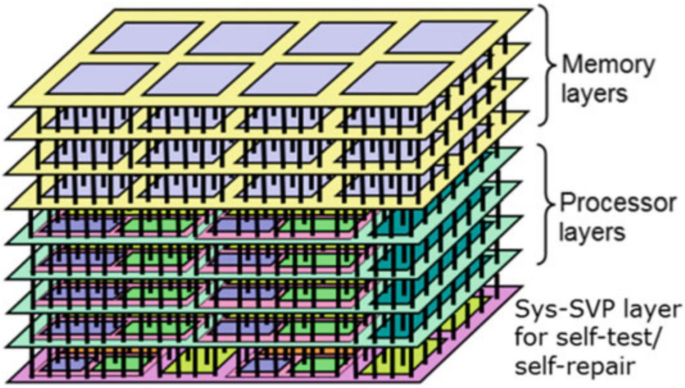


Fig. 26.12 Configuration of dependable 3D-stacked multicore processor with self-test and self-repair function

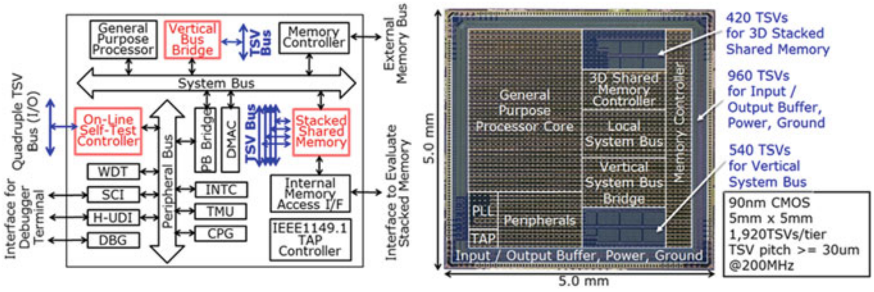

General Purpose Processor
Vertical Bus Bridge
TSV Bus
Memory Controller
External Memory Bus
System Bus
Quadruple TSV Bus (I/O)
On-Line Self-Test Controller
Peripheral Bus
PB Bridge
DMAC
TSV Bus
Stacked Shared Memory
WDT
SCI
H-UDI
DBG
INTC
TMU
CPG
Internal Memory Access I/F
IEEE1149.1 TAP Controller
Interface for Debugger Terminal
Interface to Evaluate Stacked Memory
5.0 mm
General Purpose Processor Core
3D Shared Memory Controller
Local System Bus
Vertical System Bus Bridge
Memory Controller
PLL
TAP
Peripherals
Input / Output Buffer, Power, Ground
5.0 mm
420 TSVs for 3D Stacked Shared Memory
960 TSVs for Input / Output Buffer, Power, Ground
540 TSVs for Vertical System Bus
90nm CMOS
5mm x 5mm
1,920TSVs/tier
TSV pitch >= 30um
@200MHz

Fig. 26.13 Circuit block diagram and die photo of core processor fabricated by a standard 90-nm CMOS technology

controller were added to standard circuits of conventional core processor. Approximately two thousand TSVs per each core processor layer were assigned to form the system bus, memory bus and test bus including TSVs in I/O circuits. This core processor chip exhibited the performance of 350 Mips (Dhrystone 2.1) at a clock frequency of 200 MHz.

We designed a prototype 3D-stacked multicore processor with eight layers of core processors and four layers of cache memories. BIST circuits, scan chains, and test wrappers are embedded in each core processor as shown in Fig. 26.14. TSVs are tested by a boundary scan which extends from the upper die to the lower die. Then, failures TSVs are replaced by redundant TSVs when failure TSVs is detected.

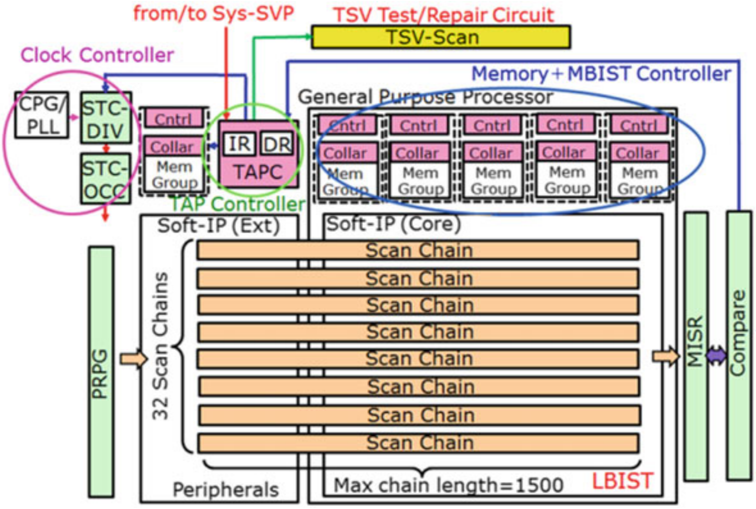


Fig. 26.14 BIST circuits, scan chains, and test wrappers embedded in each core processor

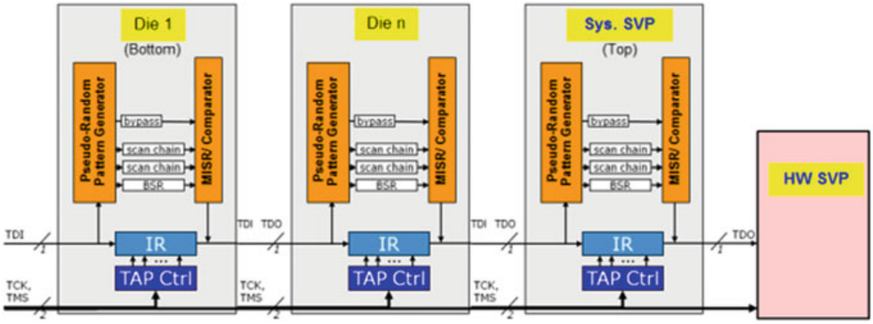


Fig. 26.15 New 3D DfT architecture for on-line self-test of dies in 3D-stacked multicore processor based on IEEE 1149.1

Function of each die is tested through scan chains using BIST circuits. Input and outputs of test data are manipulated through test wrappers. One of core processors is used as a system-level supervisor processor (Sys-SVP) in the 3D-stacked multicore processor. The Sys-SVP supervises the total function of 3D-stacked multicore processor including the test function. All test results are sent to the Sys-SVP chip as shown in Fig. 26.15 where a 3D DfT (Design for Testability) architecture for on-line self-test of dies based on IEEE 1149.1 is shown. When failure information is obtained, Sys-SVP replaces a failure block or chip by a redundant block or chip on time [21]. To achieve higher dependability, a hardware-level supervisor processor (HW-SVP) is prepared to maintain the dependability of Sys-SVP sufficiently high in the 3D-stacked multicore processor. The HW-SVP is not stacked on 3D-stacked multicore processor and consists of reconfigurable circuits with repair function and TMR (Triple Modular Redundant) circuits to achieve a high dependability.

We fabricated a four-layer stacked multicore processor and a four-layer stacked cache memory as shown in Figs. 26.16 and 26.17 by the 3D integration technology with the backside via. The system bus, memory bus, and test bus are formed through four processor layers using TSVs in the 3D-stacked multicore processor and the internal memory bus and external memory bus are formed using TSVs in the 3D-stacked cache memory. Figure 26.18 shows the X-ray CT scan image and SEM cross-sectional view of fabricated 3D-stacked multicore processor. It is clearly seen in the figure that the stacked structure with many TSVs is successfully formed. Figure 26.19 demonstrates output waveforms from the 3D-stacked multicore processor which were obtained by the functional test of internal memories using the memory BIST circuits. It is clear from the figure that the fabricated prototype 3D-stacked multicore processor exhibits excellent characteristics. Thus, we confirmed the successful operation of fabricated prototype 3D-stacked multicore processor.

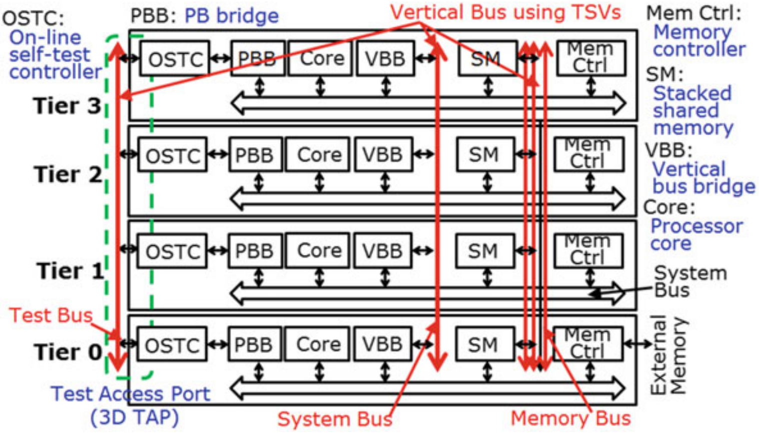


Fig. 26.16 Circuit block diagram of fabricated four-layer stacked multicore processor

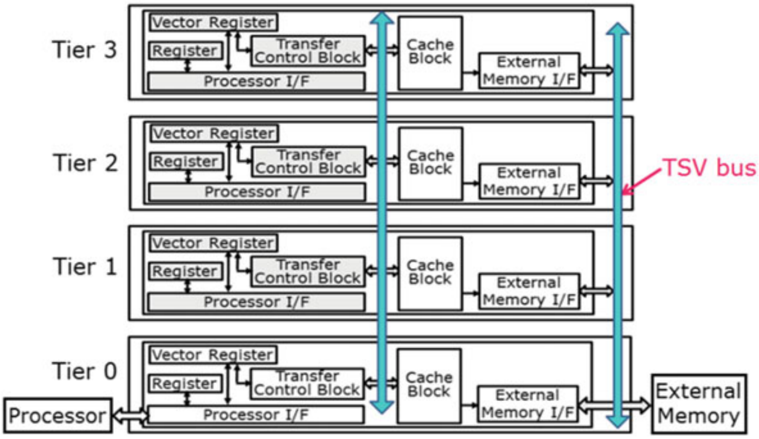


Fig. 26.17 Circuit block diagram of fabricated four-layer stacked cache memory

26.4 Conclusions and Future Work

A conceptual 3D-VLSI image sensor system module for future automatic driving vehicle has been developed where a pair of 3D-stacked image sensors and 3D-stacked multicore processors are integrated on a silicon interposer. A 3D-stacked image sensor with four layers of CMOS image sensor layer, analog circuit layer, ADC layer, and interface circuit layer was designed and fabricated in which an extremely high frame rate of 10,000 flames/s was achieved by introducing a block-parallel architecture. A prototype of 3D-stacked multicore processor with four processor layers was designed and fabricated by 90 nm CMOS technology and

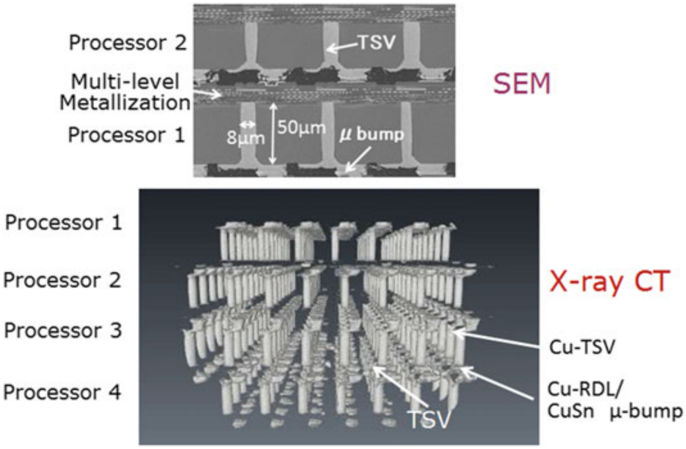


Fig. 26.18 X-ray CT scan image and SEM cross-sectional view of fabricated 3D-stacked multicore processor

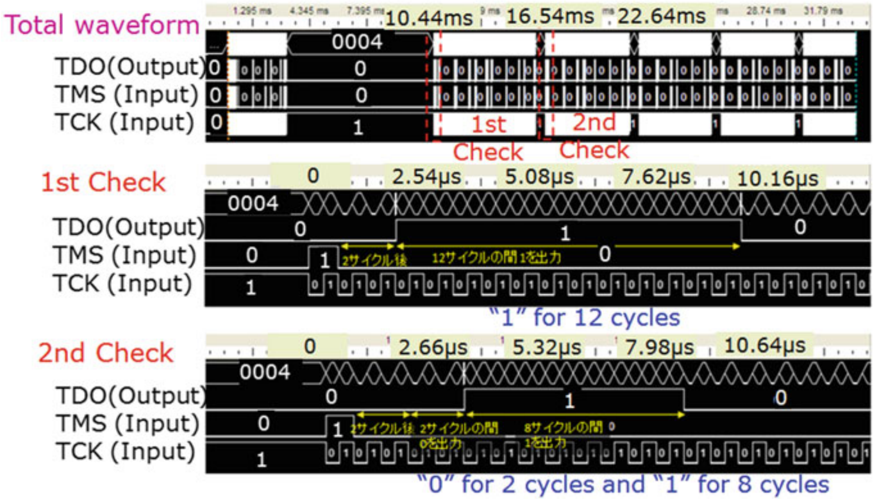


Fig. 26.19 Output waveforms from the 3D-stacked multicore processor obtained by the functional test of internal memories using the memory BIST circuits

3D integration technology. Approximately two thousand TSVs per each core processor layer were assigned to form the system bus, memory bus, and test bus including TSVs in I/O circuits. We introduced a new on-line self-test method called a cyclic test to increase the test coverage for self-test minimizing the overhead to performance. We confirmed that the processor core has a performance of 150 Mips at 200 MHz and simultaneous data transfer and memory access among four processor layers were successfully executed through the vertical system bus and the vertical memory bus in the fabricated 3D-stacked multicore processor. It is estimated from these evaluation results and the system simulation that a highly dependable 3D-stacked multicore processor for with the performance of 5 TFlops, the power consumption of 5 W, and the dependability of 80 Fit can be achieved using 3D integration technology and 8 nm CMOS technology.

The production of 3D-VLSI has already started in 3D-DRAMs which are called HMC (Hybrid Memory Cube) and HBM (High Bandwidth Memory). For further increasing the production volume of 3D-VLSI including 3D-DRAM and 3D-processor, it is required to improve the dependability of 3D-VLSI by solving reliability-related issues such as interconnection and device degradations caused by the mechanical stress, metal contamination and crystal defects in addition to the thermal issues such as hot spots in stacked chips. There are still many challenges for future 3D-VLSI.

References

1. M. Koyanagi, in *IEEE International Electron Devices Meeting (IEDM)* (2013), pp. 8–15
2. M. Koyanagi, in *IEEE International Solid State Circuits Conference (ISSCC) 3D-Forum* (2014)
3. M. Miura, K. Ito, T. Aoki et al., in *IEEE Symposium on Low-Power and High-Speed Chips (COOL Chips XIV)*, No. 19 (2011)
4. K. Ito, T. Aoki et al., *First Asian Conference on Pattern Recognition* (2011), pp. 515–519
5. M. Miura, K. Ito, T. Aoki et al., in *SICE Annual Conference 2012*, No. TuA11-04 (2012), pp. 307–312
6. R. Egawa, H. Kobayashi et al., in *IEEE International 3D System Integration Conference (3DIC)* (2010), pp. 1–8
7. J. Tada, R. Egawa, H. Kobayashi, in *IEEE Computer Society Annual Symposium on VLSI (ISLVLSI2013)* (2013), pp. 218–223
8. Y. Ichinomiya, T. Sueyoshi et al., J. Next Gener. Inf. Technol. (2011)
9. Q. Zhao, T. Sueyoshi et al., IEEE Embed. Syst. Lett. **3**(3), 89–92 (2011)
10. H. Hashimoto, M. Koyanagi et al., in *International Conference on Solid State Devices and Materials (SSDM)* (2011), pp. 168–169
11. H. Takizawa, H. Kobayashi et al., in *IEEE International Parallel and Distributed Processing Symposium (IPDPS2011)* (2011), pp. 846–876
12. K-W Lee, M. Koyanagi et al., in *IEEE International Electron Devices Meeting (IEDM)* (2012), pp. 785–788
13. K. Kiyoyama, M. Koyanagi et al., in *International 3D System Integration Conference (3DIC)* (2009)
14. K. Kiyoyama, M. Koyanagi et al., in *International 3D System Integration Conference (3DIC)* (2010)
15. K. Kiyoyama, M. Koyanagi et al., in *International Conference on Solid State Devices and Materials (SSDM)* (2011), pp. 1055–1056
16. K. Kiyoyama, M. Koyanagi et al., in *International 3D System Integration Conference (3DIC)*, 5.1 (2012)
17. K. Kiyoyama, M. Koyanagi et al., in *International 3D System Integration Conference (3DIC)* (2013)

18. T. Fukushima, M. Koyanagi et al., in IEEE *International Electron Devices Meeting (IEDM)* (2008), pp. 499–502
19. T. Fukushima, M. Koyanagi et al., in *IEEE International Electron Devices Meeting (IEDM)* (2009), pp. 349–352
20. T. Fukushima, M. Koyanagi et al., in IEEE *International Electron Devices Meeting (IEDM)* (2012), pp. 789–792
21. H. Hashimoto, M. Koyanagi et al., in *International 3D System Integration Conference (3DIC)* (2013)

Chapter 27
Applications of Reconfigurable Processors as Embedded Automatons in the IoT Sensor Networks in Space

Hiroki Hihara, Akira Iwasaki, Masanori Hashimoto, Hiroyuki Ochi, Yukio Mitsuyama, Hidetoshi Onodera, Hiroyuki Kanbara, Kazutoshi Wakabayashi, Tadahiko Sugibayashi, Takashi Takenaka, Hiromitsu Hada and Munehiro Tada

Abstract This chapter introduces the applications of the Flexible Reliability Reconfigurable Array (FRRA) processors, which is presented in Sect. 3.4, in a non-von Neumann architecture, and discusses its advantages when it is used in the Internet of Things (IoT) applications. FRRA is an embodiment of the concept of embedded automaton that we introduce as an essential element for building the IoT. We will start by looking at the role played by embedded system processors and point out that employing non-von Neumann architecture is inevitable (essential) to accomplish the speed/power performance required for embedded system applications. The major target application of embedded microprocessor is the IoT, and space-born sensor applications are quoted in this chapter as examples of the IoT. Space systems are somewhat special but are typical IoT applications which require dependability as an essential feature. Another important aspect of the embedded automaton based on the FRRA architecture is the contribution of behavioral

H. Hihara (✉) · A. Iwasaki
The University of Tokyo, Tokyo, Japan
e-mail: hihara@sal.rcast.u-tokyo.ac.jp

M. Hashimoto
Osaka University, Suita, Japan

H. Ochi
Ritsumeikan University, Kusatsu, Japan

Y. Mitsuyama
Kochi University of Technology, Kami, Japan

H. Onodera
Kyoto University, Kyoto, Japan

H. Kanbara
ASTEM RI, Kyoto, Japan

K. Wakabayashi · T. Sugibayashi · T. Takenaka · H. Hada · M. Tada
NEC Corporation, Kawasaki, Japan

S. Asai (ed.), *VLSI Design and Test for Systems Dependability*,
https://doi.org/10.1007/978-4-431-56594-9_27

synthesis technology. Practical application implementation on the reconfigurable processor is realized with the maturity of a high-level behavioral synthesis technology called CyberWorkBench (CWB).

Keywords Embedded automaton • Non-von Neumann architecture
Behavioral synthesis • Flexible reconfigurable reliability architecture (FRRA)
Internet of Things (IoT)

27.1 Introduction

Sensor nodes are now rapidly becoming an important element of social information infrastructure [1], with increasing requirement for intelligent processing capabilities such as selection, compression, and optimization on the vast amount of data gathered from the sensors prior to forwarding them to be collected at cloud systems.

We will begin this chapter by identifying the differences between the embedded computers that are based on von Neumann architecture, on the one hand, and those based on non-von Neumann architecture on the other. The latter includes Field Programmable Gate Array (FPGA) and Flexible Reliability Reconfigurable Array (FRRA), a reconfigurable processor architecture discussed in [2]. The necessity of employing non-von Neumann architecture is deduced from consideration of the characteristics of processors required for embedded system applications. The requirements for prompt response and low power consumption are the essential factors that call for non-von Neumann architecture—a liberation from the performance bottleneck of software-programmed controller. The FRRA architecture comprises the processing elements (PEs) at the bottom of hierarchy that allows the same high speed and low power consumption as FPGA does and higher levels of hierarchy that accommodate functions of higher abstraction as well as dependability.

Readers will see typical use cases of embedded processors in space systems applications discussed in this chapter. Other applications such as medical and automotive may require similarly high levels of dependability, and yet have different characteristics from space applications in that they require lower costs, volume production, more customization variety, shorter order-to-delivery lead times, etc. The reliability, as well as these other performance characteristic of the FRRA architecture, is dynamically reconfigurable, as will be explained below.

A new computation model, which is called "Embedded Automaton" is introduced in this chapter. The inherent overhead of the implementation of finite automaton found in the conventional microcontroller unit (MCU) is easily identified in comparison with Embedded Automaton, and the basic architecture of required processing element is discussed. The architecture derived is different from the so-called von Neumann architecture. Differences between an MCU and an FPGA from the processor point of view are also clarified in light of the concept of the Embedded Automaton. An Embedded Automaton consists of exchangeable finite state machines and data paths as well as the context tracing capability for high-level programming languages, which is not accommodated in an unstructured FPGA. Notwithstanding, or rather because of the difference, MCUs, and FPGAs are expected to be integrated eventually because flexible programming capability and efficient implementation are often required at the same time in a system. Such technology trend tells us that an MCU is not the only choice for developing intelligent sensors of Internet of Things (IoT) applications. A dynamically reconfigurable processor is a powerful alternative because it accommodates both flexible programming capability and implementation efficiency. It is also explained in this chapter that practical implementation of Embedded Automaton in FRRA is realized by using a matured behavioral synthesis tool called CyberWorkBench (CWB) [3–5] that can handle high-level programming language ANSI-C and SystemC. It will be shown that, although MCUs are suitable for many applications, dynamically reconfigurable processors with behavioral synthesis technology have added a powerful alternative for embedded system design.

Another advantage of the dynamically reconfigurable architecture is ultra-low power consumption. One-hundredth of power consumption is expected against a conventional MCU for equivalent amount of computation as reported in [6] because most of the area of a chip can be used for computational resources.

This chapter focuses on sensor applications for IoT because the major target of embedded system applications is considered to be intelligent sensors. The adaptation scheme of FRRA dynamically reconfigurable processor [2] for deploying it toward IoT application is described as a main theme in this chapter. This is because the Embedded Automaton computation model has been established through the development of application using a FRRA dynamically reconfigurable processor.

27.2 Intelligent Sensors for IoT Applications—Target Applications

The IoT has been envisioned as a fundamental infrastructure that will bring about useful information and knowledge resulting in efficiency and growth in industry and improved comfort and safety in human life. Everything is to be connected through Machine to Machine (M2M) network anytime and anywhere to realize the IoT framework. Wide range of information is collected and accumulated in a system using embedded processors as shown in Fig. 27.1, which will result in accumulating, sharing, and using various kinds of know-how and social knowledge [1].

Sensors, networks, information technology (IT), and robotics are distinguished as key technology elements to make IoT a practical knowledge framework. IoT can be used for supporting so-called lifeline as energy supply, waterworks, traffic control, logistics, broadcasting, and telecommunication. IoT is used for constructing social infrastructure such as roads, airports, railways, power plants, factories, etc.

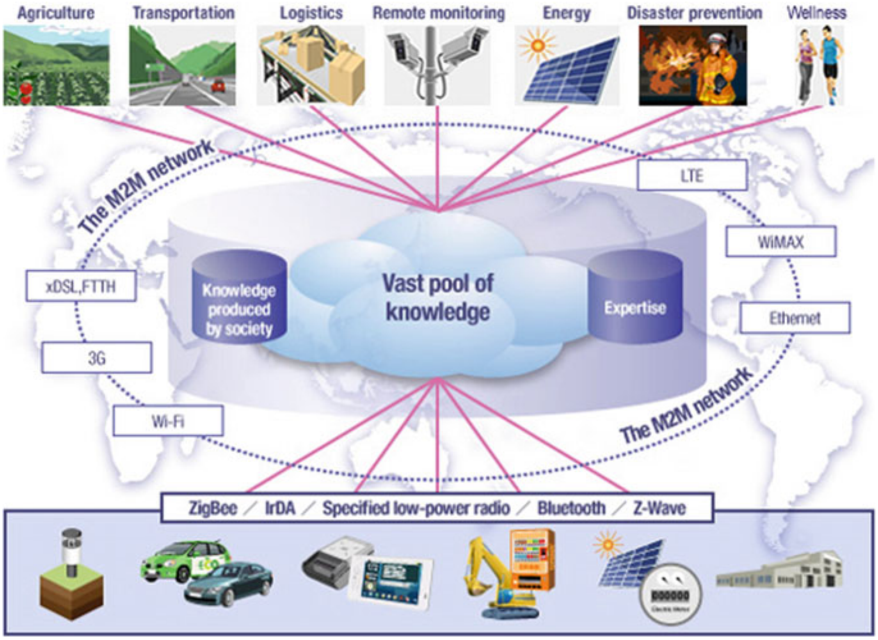


Fig. 27.1 IoT using embedded microprocessors. http://www.nec.com/en/global/solutions/nsp/m2m/concept/ [1]

Dependability is a mandatory requirement for social infrastructures such as transportation, nuclear power plants, and space systems.

This chapter exemplifies the IoT in space systems in which the authors are engaged and highlights the requirements for embedded processors used in sensors for IoT. Space systems, such as satellites can be identified as sensor nodes and relay nodes among IoT applications, whereas the node size and complexity might be different from the nodes for environment monitoring, traffic monitoring, home security, etc., and are probably the most demanding in terms of dependability among other subsystems of the IoT. Space systems will be integrated with ground network systems that consist of high-performance computers and high-performance network appliances as shown in Fig. 27.2 [7].

Satellites are placed and utilized in outer space as shown in Fig. 27.3 [8, 9], hence the limitation of the capacity of transmission channels between satellites and ground stations must be considered in the system integration. Needless to say, the functionality of the space system must be available at all times even in harsh environment with high-level radiation and wide temperature range. Soft errors often found in semiconductor devices must be taken into account during the operation of the space system.

In order to exploit large amount of data storage in data centers on the Earth, on-demand data acquisition capability is required in addition to periodical data

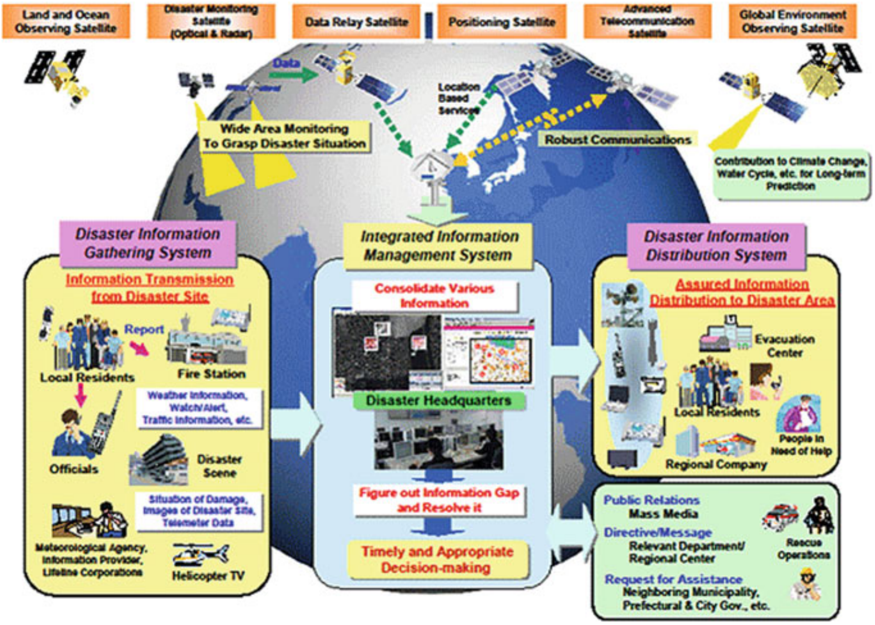

Land and Ocean Observing Satellite
Disaster Monitoring Satellite (Optical & Radar)
Data Relay Satellite
Positioning Satellite
Advanced Telecommunication Satellite
Global Environment Observing Satellite
Data
Location Based Services
Wide Area Monitoring To Grasp Disaster Situation
Robust Communications
Contribution to Climate Change, Water Cycle, etc. for Long-term Prediction
Disaster Information Gathering System
Information Transmission from Disaster Site
Report
Local Residents
Fire Station
Weather Information, Watch/Alert, Traffic Information, etc.
Officials
Disaster Scene
Situation of Damage, Images of Disaster Site, Telemeter Data
Meteorological Agency, Information Provider, Lifeline Corporations
Helicopter TV
Integrated Information Management System
Consolidate Various Information
Disaster Headquarters
Figure out Information Gap and Resolve it
Timely and Appropriate Decision-making
Disaster Information Distribution System
Assured Information Distribution to Disaster Area
Evacuation Center
Local Residents
People in Need of Help
Regional Company
Public Relations
Mass Media
Directive/Message
Relevant Department/ Regional Center
Rescue Operations
Request for Assistance
Neighboring Municipality, Prefectural & City Gov., etc.

Fig. 27.2 IoT implementation using space systems [7]. http://www.nec.com/en/global/solutions/space/remote_sensing/

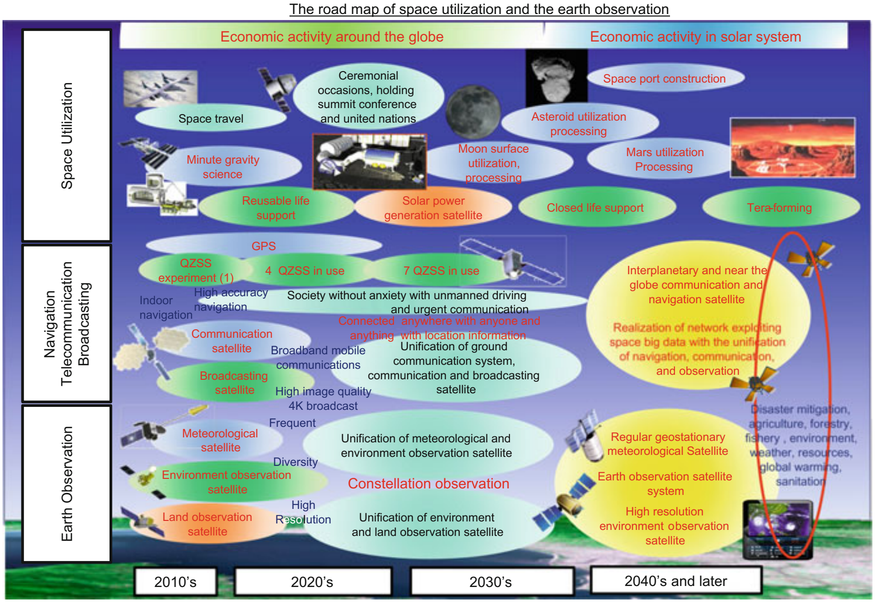

The road map of space utilization and the earth observation
Economic activity around the globe
Economic activity in solar system
Space Utilization
Space travel
Ceremonial occasions, holding summit conference and united nations
Space port construction
Asteroid utilization processing
Minute gravity science
Moon surface utilization, processing
Mars utilization Processing
Reusable life support
Solar power generation satellite
Closed life support
Tera-forming
Navigation Telecommunication Broadcasting
GPS
QZSS experiment (1)
4 QZSS in use
7 QZSS in use
High accuracy navigation
Indoor navigation
Society without anxiety with unmanned driving and urgent communication
Connected anywhere with anyone and anything with location information
Interplanetary and near the globe communication and navigation satellite
Realization of network exploiting space big data with the unification of navigation, communication, and observation
Communication satellite
Broadband mobile communications
Unification of ground communication system, communication and broadcasting satellite
Broadcasting satellite
High image quality 4K broadcast
Earth Observation
Frequent
Meteorological satellite
Unification of meteorological and environment observation satellite
Diversity
Environment observation satellite
Constellation observation
High Resolution
Land observation satellite
Unification of environment and land observation satellite
Regular geostationary meteorological Satellite
Earth observation satellite system
High resolution environment observation satellite
Disaster mitigation, agriculture, forestry, fishery , environment, weather, resources, global warming, sanitation
2010's
2020's
2030's
2040's and later

Fig. 27.3 The road map of space systems application and the Earth observation system [8, 9]. http://www.scj.go.jp/ja/member/iinkai/kanji/pdf22/siryo201-5-10-7.pdf

collection capability. Therefore, sensor units for data acquisition are required to accommodate intelligent functions as data manipulation, data selection, and data compression.

Dependability and intelligence are demanded for the sensor units because a great number of sensors are going to be deployed in the field for IoT applications. The same characteristics are required for processors embedded in those sensor units to provide intelligent functionalities in the harsh environment of outdoor. Especially, the soft errors of semiconductor memories caused by noise and background radiation are our major concern. Even though the dependable and intelligent operation is demanded on embedded microprocessors used in the sensor modules, small footprint, and reduced power consumption are mandatory for IoT applications. These requirements have been reflected in the reduced size of semiconductor memories and their control circuits in our new processor architecture.

We can exploit the characteristic of embedded systems applications which is different from the premises of microprocessors for enterprise applications and field programmable gate arrays (FPGAs) for network appliances in order to reduce memory related circuitry. Once an application program is written in programmable read-only memories (PROMs) of a product deployed into markets, the modification is seldom expected. This means that implementing applications as hardware logic does not affect the productivity, while flexibility is required in the development environment.

We have distinguished two issues in conventionally embedded microcontrollers (MCUs) that prevent sensor nodes from satisfying the demands mentioned in the preceding section.

The first issue comes from the fact that a conventional MCU is based on the stored program (von Neumann) architecture. The stored program architecture has the following overheads. A large portion of a microprocessor die area is occupied by peripheral circuitries, such as memory system and memory controllers, other than the resources for arithmetic and logic operations. As a consequence, power consumption is increased and operation speeds are limited. A possible solution to this issue is to use a dynamically reconfigurable processor. It is reported that power consumption decreased to one hundredth for the same amount of operations compared to the conventional microprocessor based on stored program architecture [6].

The second issue is related to the behavioral synthesis technology, which is widely used for improving SoC design productivity. Conventionally, a compiler runs on the processor to generate executable binary codes from the given user program written in a high-level language such as C or C++. The binary codes which consist of sequential instructions are fed to on-chip Instruction Set Processor (ISP) to be executed by either the on-chip logic units and I/O interfaces, or handed over to external logic chips such as coprocessors. In contrast, in the proposed dynamically reconfigurable architecture, the behavioral synthesis can generate a data path and its state machine controller dedicated to the given user programs, which means that the behavioral synthesis can generate a tailored hardware in which the user program is implemented and embedded as a state machine.

The flexibility is much improved compared to conventional software compilation for fixed ISP hardware, which is expected to result in significant improvement of footprint and power efficiency.

Programmability is also required on hardware circuitry because iterative and incremental design with high-level language is required for developing embedded processor applications. Such programmability can also be maintained by adopting both behavioral synthesis technology and a dynamically reconfigurable processor architecture. The dynamically reconfigurable processor architecture exploiting the behavioral synthesis technology can replace conventional embedded MCUs and enable efficient and high-performance implementations for IoT applications. The architecture is an embodiment of what we call an Embedded Automaton, which will be described in Sect. 27.3 in more detail.

27.3 Choosing Proper Processor Architecture for IoT Applications

This section discusses the computation model to investigate architecture suitable for sensors in the IoT application. In order to figure out the specific development issues for the system requirement described in the preceding section, we set up a dedicated computation model. The following four premises can be made from the IoT application development point of view:

(a) The number of program modifications of deliverables is limited. Once an application program is written into PROMs of a product and is distributed into markets, the program is not modified frequently in most cases.
(b) Input sequences for embedded systems come from the real world, and the input data for Processing Elements (PEs) are given serially. Backward data access is not necessary.
(c) An application program does not have to be implemented as software. It can be implemented as hardware circuitry because a specific design of an embedded processor is often limited within a certain lot without any chance of modifications.
(d) Input data are distinguished with time tags of a real-time clock.

Taking the above four premises into account, we set up a novel computation model, which is named Embedded Automaton. It is defined as a computation model aiming at the development of embedded systems for IoT applications.

The input data of Embedded Automaton are physical signals from real world, and they are modeled as Input/Output (I/O) signals, interface signals from adjacent PEs and time data. The comparison of Embedded Automaton with the conventional finite automaton is shown in Fig. 27.4.

In Fig. 27.4, b denotes a blank, q denotes a finite state controller of a conventional finite automaton, and s denotes a finite state controller of Embedded Automaton.

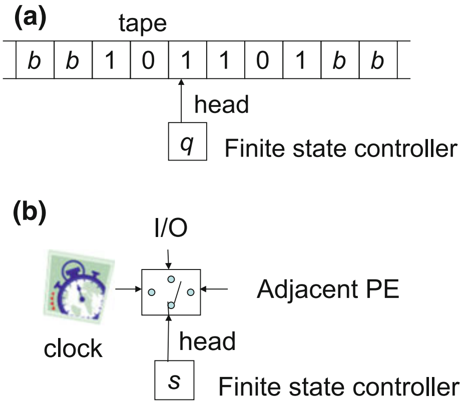


Fig. 27.4 Finite automaton (**a**) and Embedded Automaton (**b**)

Embedded Automaton (EA) is defined by the following five-term set in the same way as a conventional finite automaton.

$$\mathrm{EA} = (S, \Sigma, \delta, s_o, F) \tag{27.1}$$

In Eq. (27.1), S denotes a set of possible states, Σ a possible input data set, δ a set of state transition functions, s_o an element which corresponds to an initial state, and F a set of states in which the input sequences are accepted. S and δ are finite states and finite numbers of state transition functions, respectively. Σ is a digital value whose precision is defined in advance in system design or is the output of an analog to digital converter. In consequence, Σ is also a finite set. F is a candidate set of final states, which come from S. Therefore, F is a subset of a finite set. An initial time and a final time of inputs are designated as time itself. In consequence, the computability of EA is evaluated in the same way as that of a conventional finite automaton, and hence it is computable.

The tape model of a conventional finite automaton consists of input data and parameters of state machines. In other words, the states of a conventional finite automaton are defined by parameters shown in input data modeled as parameters on a tape and states in a finite state controller q. On the other hand, the states of an EA are only defined by states in a finite state controller s, which means that the state machines implied by application programs are integrated with the primitive state machines of a finite state controller s. The difference explains the inherent overhead of the implementation of conventional MCUs based on von Neumann architecture, and we can identify two issues of conventional MCUs by evaluating EA, which prevents sensor modules from satisfying the demands mentioned in the preceding section.

The first issue comes from the fact that conventional MCUs are based on the conventional finite automaton shown in Fig. 27.4a. Virtual finite state machines implied by application programs are implemented in memory cells with linear addresses, which are modeled as a tape, on conventional MCUs. State machine transitions extracted from application programs are simulated as addressing operations over linearly addressed memory cells by the finite state controllers. In other words, the processor implementation based on stored program architecture of a conventional finite automaton is a kind of simulator using addressing functions of the linearly addressed memory cells. Two levels of state machines exist, and one state machine described on the memory cells is emulated on another state machine inside the finite state controller. The finite state controller is used as a simulator, rather than a processor. If the state machine inside the finite state controller is programmable, the virtual state machine on the memory cells is not necessary and the finite state controller can be used as a processor. Interrupt handling and concurrent processes are often processed by software. An interrupt handling is realized as register access operations in software, and concurrent processes are realized as serialized processes handled by a multiprocess operating system or a multitask operating system. This is due to so-called von Neumann architecture, and its performance limitation is often called von Neumann bottleneck. It aims at consolidating the implementation of a PE design for mass production with unlimited program modification capability, which is not mandated in embedded system applications.

The second issue is that the stored program architecture has the following overheads. Large area of an MCU die is occupied with peripheral circuitries for memory controllers other than arithmetic and logic operation resources in order to simulate state transitions, interrupt handling, and concurrent processes. Power consumption increases as a result.

If the direct implementation of interactions with the stimulus from outer world and concurrent processing could be implemented as hardware circuitry, the overhead of simulation can be eliminated. The programmability of the finite state machine thus eliminates the overhead of simulation. Power consumption and timeliness operation are improved significantly. The architecture based on EA is realized as FRRA described in the following section. State transitions are realized by replaceable state machines using behavioral synthesis tools. This feature is also different from conventional FPGAs. The novel processing characteristics of FRRA is realized as stated above based on EA. This is a natural implementation of non-von Neumann architecture that is suitable for IoT applications.

27.4 The FRRA Implementation of Embedded Automatons

This section presents a four-layer structure for implementing EA proposed in the previous section. Each layer corresponds to I/O layer, fine-grained layer, coarse-grained layer, and switch layer, from the bottom to the top. The detailed explanation of these layers is as follows.

The bottom layer is I/O interface circuitry, which is implemented in random logic primitives and mixed-signal circuits. These elements are connected to the fine-grained blocks in the above layer.

The fine-grained layer includes the Lookup Tables (LUTs) that are used to implement data paths and finite state machines. A context signal and a state signal are characteristic signals of FRRA and are also distributed from LUTs in the fine-grained layer. The CWB [3–5], which is used to design this layer, is a matured behavioral synthesis tool and the overhead of derived circuit size is a few percent compared with hardware description language (HDL) implementation. Intellectual properties (IPs) implemented using the CWB are efficient enough for the fine-grained layer design.

The coarse-grained layer is located on top of the fine-grained layer. This layer includes operation units like Arithmetic and Logic Units (ALUs). The function of an operation unit defined in the coarse-grained layer corresponds to an instruction of a conventional MCU. In addition to that, once an Fast Fourier Transform (FFT) or an image compression operation is implemented as an operation unit of the coarse-grained layer, designers can use its function as an instruction of ALUs. The function can be specified by an independent mnemonic in program source codes. The CWB and/or other logic synthesis tools can be used for designing ALUs and other operation units on this layer. The IPs in the operation units can be designed as well using custom Application Specific Integrated Circuit (ASIC) design tools. In other words, primitive operations for the ALU can also be implemented as the hard macros of IPs through optimized design process of ordinary custom ASICs.

I/O blocks, fine-grained function blocks, and coarse-grained function blocks are connected to each other on the topmost layer. Designers can place simple bypass switches on the coarse-grained layer, which provides configurable connections between inputs and outputs for PEs in the bottommost layer. This capability is used to realize routers on the coarse-grained layer conveniently. An n-dimensional router can be implemented by using a group of n-dimensional bypass switches, course-grained blocks, fine-grained blocks and I/Os. This scheme does not affect the behavioral synthesis capability, and n-dimensional fabrics with routing capabilities can be designed using CWB.

The feasibility of designing embedded processors is confirmed with FRRA [2, 10, 11] by adopting the four-layer implementation framework described above. This means that an embedded MCU that does not have a program memory can be realized. Even though this architecture is different from the so-called von Neumann architecture, the mathematical model of a finite automaton is maintained and a practical MCU can be implemented. Note that the MCUs without program memories might not correspond to the conventional definition of a microcontroller or a microprocessor. However, any user programs can be executed on this four-layer architecture using CWB. In consequence, practical embedded processors are implemented using FRRA.

The above implementation uses LUTs as a conventional FPGA does, and the configuration memories still consist of Static Random Access Memories (SRAMs). A new solution, which is called atomic switch and is a kind of irreversible switches, has been proposed [12, 13] in order to provide programmability without SRAMs. Both program memories and configuration memories are no longer required using the atomic switch. This feature is highly suitable for space system use because it can avoid soft errors induced by radiation in orbits.

27.5 An Example Implementation and Result

This section describes the requirement specifications for the design flow of a FRRA-based processor. The design flow considered here is for the onboard equipment of space systems. Dependability is a mandatory requirement for this application and hence the reliability design must be included in the design flow.

27.5.1 Design Flow of a Space System Based on Embedded Automaton

The following six steps compose a design flow to realize advanced functions and high performance of intelligent sensors using FRRA.

Step 1: Describe a system in high-level programming language as C language. The language should be used for software development as well.

Step 2: Define coarse-grained function blocks. Function blocks can be implemented as optimized hard macros using ASIC design tools. Typical dedicated functions as image compression, image recognition, and signal processing like FFT are implemented in addition to basic arithmetic operations. It is required on behavioral synthesis tools that the operations provided by coarse-grained function blocks are used as mnemonics in program source codes. CWB realized this feature as functionalization.

Step 3: Generate source codes written in hardware description language (HDL) through behavioral synthesis. The hard macros defined in step 2 should be exploited for generating circuitry. This requirement specification is applied for the optimization of CWB during our study.

Step 4: This is a logic synthesis step, and this step is the same as in conventional LSI and FPGA logic synthesis design process.

Step 5: This is a layout design step, and this is the same as conventional LSI and FPGA layout design process.

Step 6: The verification and validation step includes delay analysis of layout design and back annotation based on the result of delay analysis. Iterations are considered in step 5 and step 6. The back annotation going back to step 3 is also anticipated. Since the back annotation should be able to be handled in high-level language, step 1 is also considered in back annotations.

The implementation example of step 2 has already been demonstrated in our previous work [14]. The implementation is realized by software with FPGA for optimized operations. Image compression operations and basic operation elements of image recognition are specified as mnemonics for its interpreter type language description, and its effectiveness is validated. Such kinds of functions are expected to be implemented as hard macros in FRRA and included in the requirement specifications. In consequence, the fine-process rules of recent semiconductors substrates are exploited as much as possible from the standpoint of performance and power consumption.

27.5.2 Design Flow for Dependability Based on Embedded Automaton

The high-reliability design method is now applied to the four individual layers of the FRRA architecture. Fault detection, isolation, and reconfiguration (FDIR) can be taken into account in the Switch and Coarse grain layers. The requirement of the reliability design flow is shown in Table 27.1.

The design scheme of the robust fabric is described in [10, 11, 19]. The design method is incorporated in I/O primitives in the bottom layer for high-reliability design flow. Specifically, radiation hardened primitives like flip-flops are considered and implemented at circuit design level or semiconductor fabrication process design level in this layer. The radiation hardened primitives can be exploited as primitives for high-reliability logic design.

Robust fabric design scheme is also useful for high-reliability design of the fine-grained layer. High-reliability circuit implementations such as Triple Modular Redundancy (TMR), etc. are adopted on susceptible function blocks automatically. If such kind of redundancy is adopted all over the chip, the high implementation

Table 27.1 The requirement specification of reliability design scheme

Layer	Implementation	Remarks
Switch	Routing by SpaceWire regulations [15]	Implementation by system FDIR design
Coarse grained	Comparison decision using TMR [2], CRAFTSYSTEM [16, 17], software communication [18], etc.	Implementation by system FDIR design
Fine grained	Triple modular redundancy with a voter (TMR), etc.	Implementation by system FDIR design, and the framework of robust fabric [19]
I/O (random logic)	Radiation hardened libraries, etc.	The framework of robust fabric [19]

density cannot be expected. The selective redundancy scheme is included in FRRA design process, and the excessive resource overhead of power consumption, layout area, and processing speed caused by redundancy is avoided.

As for course-grained layer, a redundancy scheme for each function block is selected from the system FDIR design point of view. The use of TMR, CRAFT-SYSTEM described in [16, 17] and/or software communication method described in [18] can be selected for gaining high reliability effectively in accordance with the reliability estimation results for a certain system FDIR design.

Proven communication network protocol is applicable on the topmost layer, which is the switch layer, in order to realize high reliability. The routing mechanism specified in the SpaceWire standard [15] is one candidate for implementing high reliability because many off-the-shelf devices for space applications are available. It is another advantage that the system design can be performed in the scope of the open international standard.

27.6 Discussion

The FRRA incorporating full compatibility with the four-layer implementation scheme is explained in this chapter. The following advantages have been identified in the design phase.

The tape model used in conventional finite automaton is replaced with a new computation model named as EA for the implementation using FRRA. The tape model with von Neumann architecture assumes the implementation using the sequence of machine codes which is re-writable infinite times substantially, and the machine code is implemented in physical program memories for conventional MCUs. On the other hand, system application algorithm is implemented as hardware through behavioral synthesis process in EA architecture, and program memories are no longer required. It reduces the soft error occurrence rate of random access memories in space applications dramatically. Some limitation exists for modifying application programs, and dynamic program loading is not easy at the moment, whereas the premises of embedded system are different from those of conventional embedded system programming and no fundamental difficulties have so far been found that limit the FRRA EA architecture from the use cases in embedded system applications. A few times of modifying application programs is sufficient for the fabrication of embedded system products before shipment.

Since program memories are no longer required, the remarkable advantage of low power consumption, which is found in conventional dynamically reconfigurable processors [6], is expected as well. The peripheral circuitries related to program memories, such as memory controllers, are no longer needed on processor chips, and most area of processors is used for computation. In consequence, remarkable reduction of power consumption can be achieved.

A distinctive feature of this processor architecture is that the definition of ISP itself is included in the standard design process. This feature comes from the advantage of the latest behavioral synthesis technology and allows optimized hard macros to be implemented for dedicated ISPs. The software development process using this architecture does not have to take care of compatibility with de facto standard microprocessor architecture with specific ISPs.

The compatibility and interoperability in the FRRA architecture are maintained in the input/output communication protocol level between PEs rather than in the level between ISPs. Open standard of the SpaceWire can be employed for FRRA architecture as stated above. In consequence, the latest fabrication technology can be used for implementing FRRA device, since designs described with high-level languages are technology independent thanks to behavioral synthesis. The compatibility through this scheme and design heritage is maintained even though the latest design innovation is adopted in the fabrication process of each PE because the design of each PE is independent as long as the inputs and outputs of each PE maintain compatibility.

As for the system performance of the processors based on the FRRA architecture, two kinds of simplification are realized, and real-time performance is improved. First, time is handled as basic data by the system. Therefore, the virtualization of time using software procedure as time-interruption is no longer necessary. Second, concurrency inhered in system design is realized as physically concurrent process, hence virtualization using serialization of processes or tasks by multiprocess operating systems or multitask operating systems is no longer required. Barrier synchronization of concurrent processes can be performed on fine-grained or coarse-grained implementation of FRRA. In consequence, simplified synchronization of multiple processes is anticipated for the implementation of concurrent real-time systems.

In the technological roadmap point of view, standardization of programmable devices is forecasted to appear after the era of System-on-a-chip (SoC) and System in package (SiP) by the extended Makimoto's Wave [20] shown in Fig. 27.5. That is called as "Highly flexible super integration (HFSI)" in [20]. FRRA accommodates the characteristics required for HFSI.

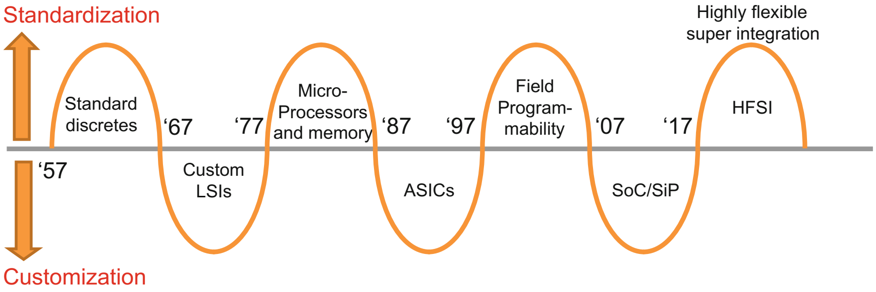


Fig. 27.5 Extended Makimoto's wave [20]

Aknowledgement The right-most surge in the Makimoto's waves shown in [20] is considered as one of the design target of the FRRA architecture implementation and the establishment of the requirement specification because the technology trend shown by the Makimoto's waves still holds. Authors thank Dr. Makimoto for his precious advice. We proceed the evaluation of FRRA architecture as a candidate for the Highly Flexible Super Integration (HFSI) shown in the technology trend in the waves.

Authors also thank Dr. Asai, who was Research Supervisor, CREST DVLSI Program, and staff members of JST for their arrangement of the CREST symposium of DVLSI (Dependable VLSI).

References

1. http://www.nec.com/en/global/solutions/nsp/m2m/concept/
2. Y. Mitsuyama, M. Hashimoto, T. Onoye, H. Ochi, K. Wakabayashi, *Soft-Error-Tolerant Reconfigurable Architecture*, Section 3.4
3. K. Wakabayashi, B.C. Schafer, "All-in-C" SoC synthesis and verification with CyberWorkBench, in *High-Level Synthesis from Algorithm to Digital Circuit*, vol. XVI, ed. by P. Coussy, A. Morawiec (Springer, 2008), Chapter 7, pp. 113–127. ISBN: 978-1-4020-8587-1
4. K. Wakabayashi, T. Okamoto, C-based SoC design flow and EDA tools. IEEE Trans. CAD 1507–1522 (2000)
5. K. Wakabayashi, CyberWokBench: integrated design environment based on C-based behavior synthesis and verification, in *IEEE VLSI-TSA* (2005), pp. 173–176
6. T. Awashima, Full software implementation of real-time ISDB-T modulator on dynamically reconfigurable SoC using practical co-design environment, in *Invited Talk, CoolChips XIV, Yokohama Industrial Development Corporation, 20th* (2011)
7. http://www.nec.com/en/global/solutions/space/remote_sensing/
8. H. Oyama, M. Sakurai (The Japan Society for Aeronautical and Space Sciences), A. Iwasaki (the University of Tokyo), Y. Takahashi, M. Toyoshima (National Institute of Information and Communications Technology), *The 201st Board of Governors Materials, Science Council of Japan*, 19 September 2014
9. http://www.scj.go.jp/ja/member/iinkai/kanji/pdf22/siryo201-5-10-7.pdf
10. D. Alnajjar, H. Konoura, Y. Mitsuyama, H. Shimada, K. Kobayashi, H. Kanbara, H. Ochi, T. Imagawa, S. Noda, K. Wakabayashi, M. Hashimoto, T. Onoye, H. Onodera, Reliability-configurable mixed-grained reconfigurable array supporting C-to-array mapping and its radiation testing, in *Proceedings of the IEEE Asian Solid-State Circuits Conference (A-SSCC 2013),* November 2013, pp. 313–316
11. H. Konoura, D. Alnajjar, Y. Mitsuyama, H. Shimada, K. Kobayashi, H. Kanbara, H. Ochi, T. Imagawa, K. Wakabayashi, M. Hashimoto, T. Onoye, H. Onodera, Reliability-configurable mixed-grained reconfigurable array supporting C-based design and its irradiation testing. IEICE Trans. Fundam. Electron. Commun. Comput. Sci. **E97-A**(12), 2518–2529 (2014)
12. M. Miyamura, T. Sakamoto, M. Tada, N. Banno, K. Okamoto, N. Iguchi, H. Hada, Low-power programmable-logic cell arrays using nonvolatile complementary atom switch, in *15th International Symposium on Quality Electronic Design* (2014), pp. 330–334
13. M. Tada, T. Sakamoto, M. Miyamura, N. Banno, K. Okamoto, N. Iguchi, H. Hada, Improved off-state reliability of nonvolatile resistive switch with low programming voltage. IEEE Trans. Electron Devices **59**(9) (2012)
14. H. Hihara, K. Iwase, J. Sano, H. Otake, T. Okada, R. Funase, R. Kashikawa, I. Higashino, T. Masuda, SpaceWire-based thermal-infrared imager system for asteroid sample return mission HAYABUSA2. J. Appl. Remote Sens. **8**, 084987-1-13 (2014)
15. ECSS-E-ST-50-12C, SpaceWire—Links, nodes, routers and networks, in *ECSS Secretariat, ESAESTEC, Requirements & Standards Division* (2008)

16. H. Hihara, M. Ohtsuka, Y. Mizushima, T. Morisato, T. Ohshima, H. Miyoshi, K. Baba, Space-born Fault tolerant Computers. Inf. Process. **35**(6), 497–503 (1994)
17. H. Hihara, K. Yamada, M. Adachi, K. Mitani, M. Akiyama, K. Hama, *Autonomous Fault Tolerant Computer for SERVIS-2 Satellite*. Technical Report of IEICE, DC2002-75, vol. 102, no. 492, December 2002, pp. 19–24
18. N. Kanekawa, K. Ihara, Space computer systems. Onboard space computers using state-of-art-LSIs. J. IEICE **73**(11), 1209–1214 (1990)
19. H. Onodera, *Overview of Device Variations*, Chapter 5.1
20. T. Makimoto, Implications of Makimoto's wave. IEEE Comput. **46**(12), 32–27 (2013). http://doi.ieeecomputersociety.org/10.1109/MC.2013.294

Chapter 28
An FPGA Implementation of Comprehensive Security Functions for Systems-Level Authentication

Daisuke Suzuki, Koichi Shimizu and Takeshi Fujino

Abstract In this chapter, we present a self-contained security coprocessor architecture that using a "Glitch PUF" and a block cipher, efficiently integrates functions necessary for secure key storage and challenge-response authentication. Based on the fact that a Glitch PUF uses a random logic for the purpose of generating glitches, the presented architecture is designed around a block cipher circuit such that its round functions can be shared with a Glitch PUF as a random logic. As a concrete example, a circuit structure using a Glitch PUF and an AES circuit is presented, and evaluation results for its implementation on FPGA are provided. In addition, a physical random number generator using the same circuit is presented. Evaluation results by the two major test suites for randomness, NIST SP 800-22, and Diehard are provided, proving that the physical random number generator passes the test suites. The self-contained security coprocessor ensures that the software it runs does not contain malicious code, the accessories are genuine, and the network devices it connects to are not cloned ones.

Keywords Physical unclonable function · Physical random number generator
FPGA · AES · Authentication

28.1 Introduction

Physical[1] Unclonable Functions (PUFs) [2, 3] have become an important option to provide a tampering countermeasure in general-purpose ICs such as ASIC and FPGA. A PUF is a function that returns a response for a given challenge depending on physical characteristics of an artificial object on which it is implemented. It is

[1] A Full version was presented at [1] Copyright © 2014 IEICE.

D. Suzuki (✉) · K. Shimizu
Mitsubishi Electric Corporation, Kamakura, Japan
e-mail: suzuki.daisuke@bx.mitsubishielectric.co.jp

T. Fujino
Ritsumeikan University, Kusatsu, Japan

S. Asai (ed.), *VLSI Design and Test for Systems Dependability*,
https://doi.org/10.1007/978-4-431-56594-9_28

difficult to clone artificial objects because their physical characteristics arise from manufacturing variation. Thus, in combination with Fuzzy Extractors [4], which enable to extract information stably from noisy data, PUFs can be used for generating device unique secret keys that are difficult to clone [5]. From the viewpoint of implementation in digital ICs, this chapter focuses on intrinsic PUFs that can be implemented as digital circuits. In this context, types of PUF are categorized mainly in two [6]: memory-based PUFs, which uses characteristics of memory cells such as SRAM PUFs [7], and delay-based PUFs, which uses variations of circuit delays such as Arbiter PUFs [8]. Much research has been conducted on realization of PUFs in general-purpose ICs and on generation of device unique keys [2–16].

For actual security applications, however, more functions are required than PUFs and Fuzzy Extractors can offer. For example, device authentication by a general challenge-response procedure requires block cipher operations or keyed one-way functions, and random number generation for use as challenges. In order to fill the gap, this chapter presents a security coprocessor architecture that efficiently unifies necessary functions for secure key storage and challenge-response authentication by using a Glitch PUF. Glitch PUFs [14, 15] are a kind of delay-based PUF, and thus have the merit of being able to operate and generate a PUF output any time while the system is on, and to be implemented by a standard method of circuit design.

Focusing on the fact that a Glitch PUF uses a random logic as a source of device unique information, the presented architecture is designed around a block cipher circuit such that its round functions can be shared by a Glitch PUF as a random logic while the normal cipher operation can be performed. This chapter also presents a physical random number generator using the same circuits by exploiting the property that the error rate of a Glitch PUF increases as the random logic becomes complex.

This chapter presents a unified coprocessor architecture for secure key storage and challenge-response authentication with low implementation overhead. The basic idea of the proposal is for encryption, key generation, and random number generation to share circuits. In order to implement the idea, a random number generator using a Glitch PUF is also presented. A concrete circuit structure using an AES cipher and a Glitch PUF is presented, and empirical results for implementation in FPGAs are provided. As to the basic performance as a PUF for key generation, the results show that the proposal has sufficient performance in Spartan-3A while it does not in Spartan-6. As to the performance of a physical random number generator, the results show that the proposal passes two major statistical test suites for randomness: NIST SP 800-22 and Diehard.

28.2 Overview of Glitch PUFs

Glitch PUFs [14, 15] are a delay-based PUF that exploits glitch phenomenon attributed to delay difference between gates of a logic circuit. Figure 28.1 shows the basic composition of a Glitch PUF. The glitch generator is a circuit for generating glitches. A random logic like the S-box of AES can be used as a glitch genera-

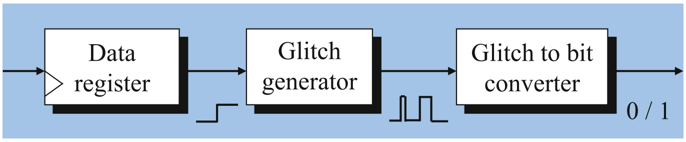


Fig. 28.1 Basic composition of a Glitch PUF

tor. By changing the input signals of the glitch generator, its output signals start to transition. Due to delay difference between gates of the glitch generator, there arise narrow pulses in the output signals until the transition finishes, and the output signals become stable. This phenomenon and the corresponding pulses are called glitches. A generated glitch is converted to a bit 0 or 1 according to, for example, whether the number of rising edges in it is even or odd.

As the glitch generator becomes complex, the number of glitches to be generated increases. As a consequence, the amount of information that the Glitch PUF can extract increases while the error rate of the Glitch PUF also increases. Therefore, for key generation using a Fuzzy Extractor, it is necessary to design a glitch generator that balances the rate of information and the rate of error. One possible solution is the evaluation methodology proposed in [14, 15], by which it is possible to estimate at design stage the rate of information and the rate of error by evaluating them by simulation. Note that in this chapter the error rate of a PUF is defined to be the average probability that each response bit includes an error, which is calculated as the rate of the number of bit errors in response to the same challenge.

28.3 Physical Random Number Generator

Random number generation is one of essential functions for cryptographic systems in which it is used for generating, for example, initialization vectors, session keys, and a random sequence for challenge-response authentication. In the cryptographic context, it is especially important to use random bits that are unpredictable even by an unlimited computational power. Thus, physical random number generators are desired for introducing true randomness.

From viewpoints of feasibility and cost, many works have been conducted on physical random number generators that can be implemented by digital circuits without need for analog circuits [17–19]. In combination with PUFs, [20, 21] propose random number generators that are efficiently implemented with part of their circuit shared with PUFs. In addition to a PUF and a random number generator, this chapter proceeds further to also unifying a cipher circuit, in which a Glitch PUF is used as a basic building block.

In this section and the next sections, a physical random number generator using a Glitch PUF is presented. This section presents the basic idea, and the next section shows a concrete circuit structure for implementation.

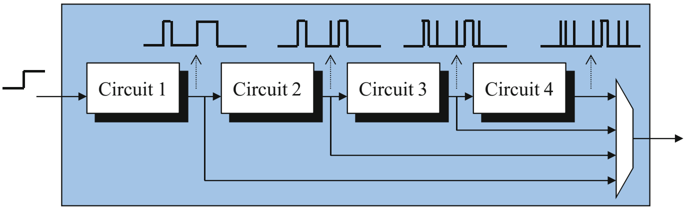


Fig. 28.2 Selectable glitch generator

28.3.1 Glitch Generators for More Randomness

If, instead of taking a balance, the error rate of responses becomes nearly 50%, there is a potential to view the responses as random numbers. In this sense, glitch generators for generating random numbers must introduce a larger amount of glitches than those for usual key generating purposes. The glitch generator in this chapter is, therefore, designed to be able to be switched by a selector for different purposes.

The idea is shown by an example structure in Fig. 28.2. In Fig. 28.2, four component circuits, either the same or different, are serially connected, each output of which is connected to a selector. As a result, four glitch generators can be selected from outside. In general, a more complex glitch generator is expected to introduce a larger amount of glitches. It is, however, not always the case because there is a possibility that some glitches become so narrow as a result of passing through a complex circuit that they are eventually suppressed. The advantage of the glitch generator lies in its configurability that permits finding a glitch generator suitable for each purpose.

28.3.2 Error Accumulation

Although it is now possible to select a glitch generator that produces more glitches and thereby contributes to high error rate, it is difficult to ensure error rate of nearly 50% with a single response. Hence, error accumulation is introduced by repeating generating responses to the same challenge. The procedure of error accumulation is as follows. First, the internal state is defined to be

$$\begin{aligned} r_1 &:= 0, \\ r_{k+1} &:= r_k \oplus b_k, \end{aligned}$$

where starting with the initial state $r_1 = 0$, r_k is XORed by the k-th response bit b_k, thus updated to be r_{k+1}. After $\mathsf{cnt}_{\mathsf{re}}$ repetitions, $r_{\mathsf{cnt}_{\mathsf{re}}+1}$ is the final response bit.

Assume, for example, that the correct response bit for a given challenge is 0, and the error rate is p. Then, for each k, $b_k = 0$ with probability $1 - p$, and $b_k = 1$ with probability p, implying that $r_{k+1} = r_k$ with probability $1 - p$, and $r_{k+1} = r_k \oplus 1$ with

Fig. 28.3 Error accumulation with the initial value zero

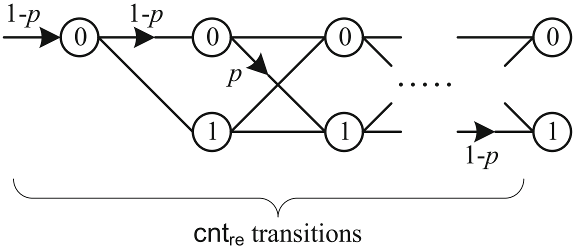
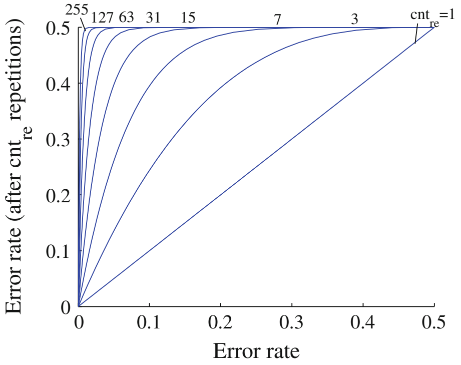


Fig. 28.4 Effect of error accumulation



probability p. In other words, r_k keeps its value with probability p and flips its value with probability $1-p$. Figure 28.3 displays how r_k transitions as k advances like a binary symmetric channel.

In the example above, if the number of errors occurring during $\mathsf{cnt}_{\mathsf{re}}$ transitions is even, the final state $r_{\mathsf{cnt}_{\mathsf{re}}+1}$ is 0, which, as a result, represents the correct response bit. Conversely, if the number of errors is odd, the resultant final state is 1, which represents the wrong response bit. The error rate after the error accumulation is therefore calculated as

$$\sum_{k=0}^{\lfloor \mathsf{cnt}_{\mathsf{re}}/2 \rfloor} \binom{\mathsf{cnt}_{\mathsf{re}}}{2k+1} p^{2k+1}(1-p)^{\mathsf{cnt}_{\mathsf{re}}-(2k+1)}.$$

The same holds for the case of the initial state 1. The effect of error accumulation by the above equation is shown in Fig. 28.4. The graph in Fig. 28.4 permits estimation that, for example, if the error rate per repetition is 10%, the total error rate after error accumulation with $\mathsf{cnt}_{\mathsf{re}}$ being 31 is almost 50%.

28.3.3 Repetition Function of Glitch PUFs

In relation with the error accumulation introduced above, Glitch PUFs have a repetition function that is intended for lowering error rate. It is notable that the error accumulation can be implemented by the same circuit as the repetition function. The details will be explained in Sects. 3.3 and 3.4. Below is an overview of the repetition function.

Assume that response generation for the same challenge is repeated $\mathsf{cnt}_{\mathsf{re}}$ times, out of which 1 is generated n times. If no error occurs at all, $n = 0$ implies that the response bit is 0, and $n = \mathsf{cnt}_{\mathsf{re}}$ implies that the response bit is 1. Because, however, errors occur in practice, a threshold parameter denoted as $\mathsf{th}_{\mathsf{err}}$ is employed to define how many errors are acceptable during the repetition. As a consequence, if $n = 0, \ldots, \mathsf{th}_{\mathsf{err}}$, the response bit is determined to be 0, and if $n = (\mathsf{cnt}_{\mathsf{re}} - \mathsf{th}_{\mathsf{err}}), \ldots, \mathsf{cnt}_{\mathsf{re}}$, the response bit is determined to be 1. For example, when $\mathsf{cnt}_{\mathsf{re}} = 7$, and $\mathsf{th}_{\mathsf{err}} = 2$, the following criteria will be applied to determine the value of the response bit and its stability.

- $n = 0, 1, 2$: The value is 0 (Stable).
- $n = 3, 4$: The value is undecidable (Unstable).
- $n = 5, 6, 7$: The value is 1 (Stable).

28.4 Unified Security Coprocessor

This section presents a security coprocessor architecture for challenge-response authentication, unifying the physical random number generator presented in the previous section, the key generator proposed in [16], and the AES cipher.

28.4.1 Architecture

The architecture of the proposed coprocessor is shown in Fig. 28.5. The key generator, which consists of the lower two blocks in Fig. 28.5, is basically the same as [16]. The Reed–Muller code used is RM(1, 6), which has the order of 1 and the length of 6. The decoder is a maximum likelihood one. The Toeplitz hash is a construction of a universal family of hash functions that can be implemented using an LFSR. Refer to [16] for details.

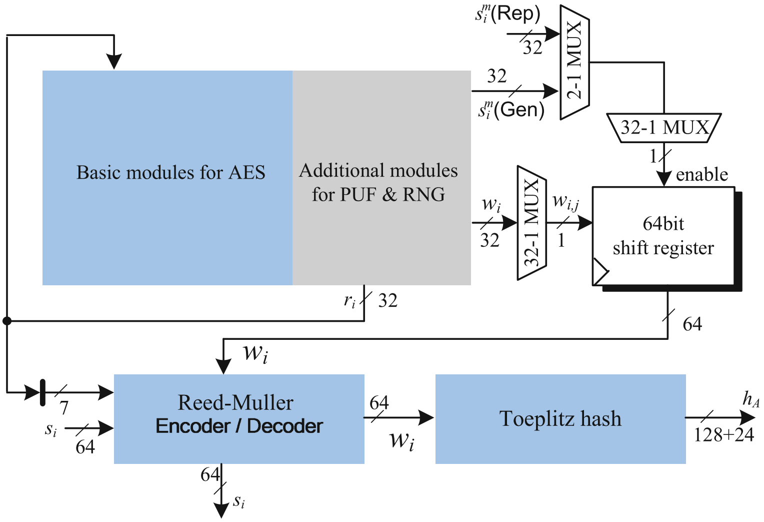


Fig. 28.5 Architecture of the proposed coprocessor

28.4.2 Design of the AES and the Glitch PUF

The design of the AES and the Glitch PUF circuits in the upper part of Fig. 28.5 is as follows. The Glitch PUF proposed in [14, 15] used a SubBytes circuit of AES as a glitch generator, which contributes to good performance as a PUF implemented in Spartan-3A. Thus, this chapter also bases a glitch generator on a SubBytes circuit. In addition, the glitch generator is designed to be selectable from even more complex one than SubBytes for the purpose of using it to generate random numbers. In case a logic even simpler than SubBytes is needed, intermediate outputs in SubBytes can also be selected. There have already been many works on implementation of AES, among which this chapter uses the implementation of [22]. Thus, the intermediate outputs in SubBytes to be selected are those of each component blocks of a SubBytes represented by composite field arithmetic.

The completed circuit is shown in Fig. 28.6. The left block is the AES circuit, which can be seen as the base, and the right block is the additional circuit for completing a Glitch PUF. Three selectors are inserted in data paths of the AES, thereby enabling to switch paths on demand, and another one is inserted inside each of the SubBytes circuit to select intermediate outputs. In between each pair of adjacent SubBytes', one AND and one XOR gates are placed to enable feedback chaining for further increasing the number of logic stages as a glitch generator.

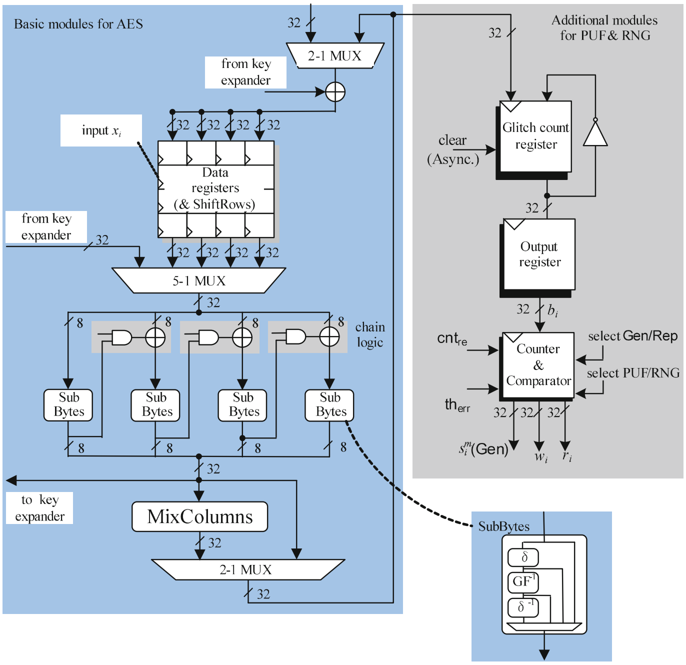


Fig. 28.6 AES and Glitch PUF circuits

28.4.3 Basic PUF Operation

In a Glitch PUF, change of the input signals generates glitches, which are eventually transformed to a PUF output. A challenge for a Glitch PUF is therefore defined to be a pair of input values.

In the left block of Fig. 28.6, the data registers and the 5-1 MUX after them are used to make a challenge. A pair of register values is selected by switching the MUX and supplied as a challenge to the right block.

In the right block, the flip-flops (FFs) denoted as “Glitch count register” are supplied with the glitch as the driving clock, thereby determining whether the number of glitches is even or odd. The FFs are asyncronously reset before a new challenge is applied. The output is once latched by “Output register”, and next the repetition function of a Glitch PUF is performed on it by “Counter and Comparator”.

Figure 28.7 shows an example structure of “Counter and Comparator” in the case of $\mathsf{cnt}_{\mathsf{re}} = 127$ and $\mathsf{th}_{\mathsf{err}} = 0$. For each bit $b_{i,j}(j = 1, \ldots, 32)$ coming from “Output register”, one 7-bit register and one addition circuit are used to count the number of times that $b_{i,j}$ takes the value 1 out of 127 repetitions. The size of the register and addition circuit depends on the choice of $\mathsf{cnt}_{\mathsf{re}}$. After finishing counting the number of 1’s in 127 repetitions, the most significant bit (MSB) of the register represents a resultant response bit determined by the majority rule. In fact, the MSB of the 7-bit

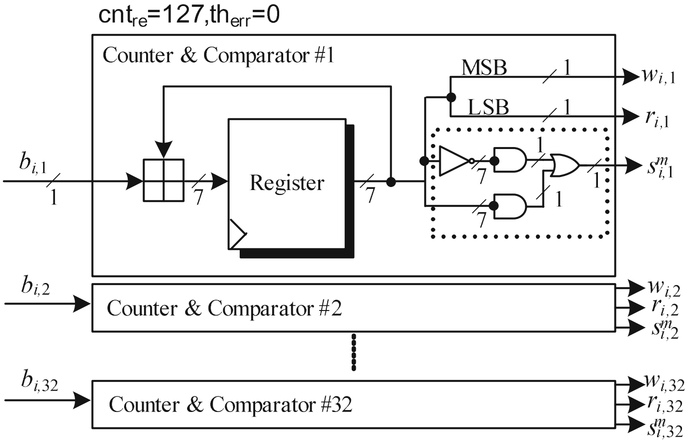


Fig. 28.7 Counter and Comparator

register becomes 1 if and only if $b_{i,j}$ takes the value 1 no less than 64 times. The final response bit is output as $w_{i,j}$.

At the same time, the simple logic enclosed in a dotted square calculates a mask bit that represents the stability of the value of $b_{i,j}$. How the logic can generate a mask bit is described as follows. First, the lower 7-bit AND gate has the value 1 only when every bit of its input has the value 1, meaning that the 7-bit register has the value 127. This is only the case when $b_{i,j}$ takes the value 1 in all 127 repetitions, which corresponds to one of the two most stable case of bit generation. Conversely, due to the 7-bit NOT gate before it, the upper 7-bit AND gate has the value 1 only when $b_{i,j}$ takes the value 0 in all 127 repetitions, which is the other most stable cases. As a result, only when $b_{i,j}$ takes the same value in all 127 repetitions, at least one input of the OR gate has the value 1, and thus the output of the OR gate has the value 1. The mask bit thus generated is finally output as $s^m_{i,j}$.

28.4.4 Operation for Random Number Generation

The challenge to the Glitch PUF is fixed when performing random number generation. Because it can be chosen arbitrarily as long as the input signal changes well enough, the challenge is chosen to be the one in which the input changes from all 0's to all 1's.

In addition to selecting a complex glitch generator by controlling the selectors and chain logic in the AES circuit, error accumulation is performed to make the error rate close to 50%. It can be performed by the same "Counter and Comparator" in Fig. 28.7, which is originally for lowering the error rate. Because its value flips when $b_{i,j} = 1$ and does not otherwise, the behavior of the least significant bit (LSB) of the register corresponds to the error accumulation in Fig. 28.3. Random bits are finally output as $r_{i,j}$.

28.4.5 Secure Key Storage and Challenge-Response Authentication

All the components put together, secure key storage and challenge-response authentication are realized. Figure 28.8 presents an example of a simple authentication protocol based on ISO/IEC 9798-2, where Bob tries to authenticate Alice.

The secret key pre-shared by Alice and Bob, denoted as *PSK*, is securely stored in each side as follows. It is encrypted with the key K_X generated by the proposed key generator and stored somewhere in unprotected nonvolatile memory, as $E_{K_X}(PSK)$. Here, X is either A or B, representing Alice and Bob, respectively. Because K_X is generated by a PUF-based key generator, $E_{K_X}(PSK)$ can only be decrypted by the person who has the identical PUF circuit that generates K_X. In addition, because K_X and *PSK* exists only when used, there are very few chances for attackers to access them.

The authentication proceeds as follows. Bob first generates a random number r_B and sends it to Alice. Random numbers here can be generated by the proposed random number generator. Then, Alice encrypts (r_B, B^*) with the pre-shared key *PSK* and sends it back to Bob. Here, B^* is an optional data concatenated to r_B to prevent reflection attacks. Finally, Bob decrypts the received data with *PSK* and verifies that the decrypted data matches r_B.

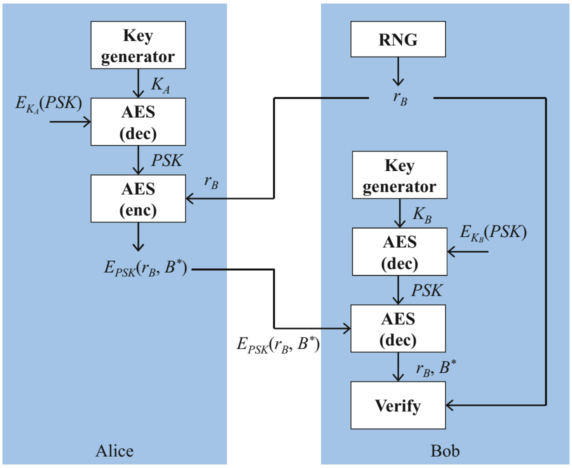


Fig. 28.8 Flow of challenge-response authentication

28.4.6 Discussion on Security of Chips

In order to evaluate the effectiveness of using PUFs, this subsection discusses security of chips that handle security functions, such as the authentication in the previous subsection. Figure 28.9 shows two possible cases for storage of secret information in a typical system consisting of a general-purpose IC and external flash memory. Table 28.1 summarizes the levels of attacks to the system in ascending order of difficulty.

From an attacker's perspective, the case 1 apparently allows an easier access to the secret information than the case 2: the secret key is vulnerable to tapping both in an ASIC and an FPGA, and the configuration of an FPGA is vulnerable as well.

Therefore, it is desirable that secret information such as cryptographic keys is stored inside a chip as the case 2, but it is not always the case that chips have nonvolatile memory inside them. One of the advantages of PUFs lies in that they provide a function for generating device unique keys on demand to chips without nonvolatile memory. With use of a PUF, the following attacks can be prevented: numbers 1 and 2 can easily be solved because it is no longer necessary to store a key in external

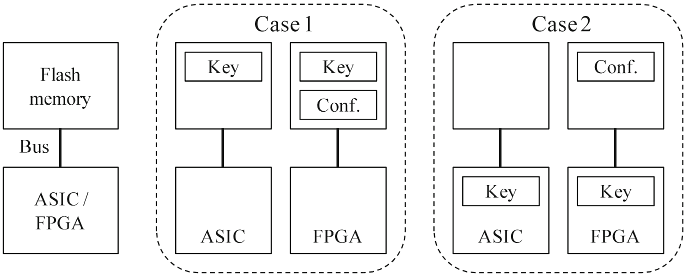


Fig. 28.9 Storage of secret information

Table 28.1 Levels of attacks

No.	Applicable	Device	Description
1	Case 1	A/F	Copy of flash memory
2	Case 1	A/F	Analysis of flash memory
3	Case 1	F	Copy of the configuration
4	Case 1	F	Analysis of the configuration
5	Case 1, 2	F	Manipulation of the configuration
6	Case 1, 2	A	Manipulation of the circuit

A ASIC, *F* FPGA

flash memory. Numbers 3 and 4 can also be solved in that even if a PUF circuit in a certain chip is copied or analyzed, and the same circuit or function is implemented in another chip, the second chip will not produce the same key as the first chip.

Note that numbers 5 and 6 are not prevented by a PUF, and another countermeasure must be employed to prevent them. Note also that it is much more difficult to manipulate the circuit of an ASIC than the configuration of an FPGA.

28.5 Performance Evaluation

This section provides the evaluation results for the proposed circuit from viewpoints of PUFs for key generation and of physical random number generators, thus proving the feasibility of the proposed architecture.

Table 28.2 summarizes the parameters that the proposed circuit can choose. In what follows, $\mathsf{cnt}_{\mathsf{re}} = 255$ and $\mathsf{th}_{\mathsf{err}} = 0$ are used. To examine the environmental effects to the Glitch PUF, ambient temperature is controlled by a thermostatic chamber, and supply voltage is configured with a potentiometer implemented on FPGA boards. Table 28.3 shows the combinations of temperature and voltage to be evaluated, where the combination of 27 °C and 1.20 V corresponds to the normal operation environment, and the other four correspond to the corner cases. The target devices for evaluation are Spartan-3A (XC3S1400A) and Spartan-6 (XC6SLX16) by Xilinx. Six chips each are used. Note that the FPGAs are employed here for prototyping, and use of ASICs are desirable in practical applications according to the discussion on the security of chips conducted in Sect. 4.6.

Table 28.2 Parameters of the proposed circuit

Parameter	Description
$\mathsf{cnt}_{\mathsf{re}} = 1, 3, \ldots, 255$	No. of repetitions
$\mathsf{th}_{\mathsf{err}} = 0, 1, \ldots, \lfloor \mathsf{cnt}_{\mathsf{re}}/2 \rfloor$	Stability threshold
$\mathsf{sel} = 0, 1, \ldots, 63$	Glitch generator no.
$N = 16384$ (const.)	No. of bits generated

Table 28.3 Temperature and voltage to be evaluated

(°C)	(V)		
	1.14	1.20	1.26
0	✓		✓
27		✓	
85	✓		✓

Table 28.4 Circuit performance

Circuit	Spartan-3A		Spartan-6	
	FFs	LUTs	FFs	LUTs
AES (original)	160	919	174	874
AES (modified)	160	1048	188	1071
Key scheduler	256	465	256	374
Glitch PUF (additional)	386	799	391	764
Control	95	193	83	134
Critical path (ns)	21.8		19.0	

28.5.1 Circuit Performance

The performance of the proposed circuit is summarized in Table 28.4. Synopsis Synplify Pro is used for logic synthesis, and Xilinx ISE is used for place and route. In Table 28.4, the AES labeled "modified" is the one that has been modified from the original AES labeled "original" in order to be shared by the Glitch PUF. The values for the Glitch PUF are for additional modules to the AES, namely a Glitch PUF without a glitch generator. It is the essential part of a Glitch PUF for data processing and thus cannot be omitted. The others are for the key scheduler and the control circuit. The result indicates that aside from the essential part, the Glitch PUF is able to be implemented with the increase of LUTs of the AES circuit by about 14%, instead of implementing a dedicated circuit for the glitch generator.

Note that the critical path does not include the chain logic in Fig. 28.6. Therefore, the signal path from the "Data registers" in the left block to the "Output register" in the right block is designed to be a multi-cycle one.

28.5.2 Basic Performance as a PUF

The Glitch PUF with respect to each glitch generator is evaluated in order to find the best point for different uses. While the proposed circuit allows the glitch generator to be changed to 64 different patterns, 17 of them are evaluated here as representatives. Table 28.5 shows them. In Table 28.5, s1, s2, and s3 are component blocks of the SubBytes in [22] represented by composite field arithmetic, where, for example, s1 + s2 + s3 means the whole SubBytes.

Robustness and uniqueness, two of the most basic performance measures for PUFs, are employed to evaluate the Glitch PUF in this chapter. Because Glitch PUFs filter out unstable bits by masking operation, generation efficiency must also be evaluated by measuring how many bits remain after the masking operation.

Table 28.5 Evaluated glitch generators

Number	Description
0	(MC, 0)
1	(MC, 1)
2	(MC, 2)
3	(MC, 3)
4	(s1 + MC, 0)
5	(s1 + MC, 1)
6	(s1 + MC, 2)
7	(s1 + MC, 3)
8	(s1 + s2 + MC, 0)
9	(s1 + s2 + MC, 1)
10	(s1 + s2 + MC, 2)
11	(s1 + s2 + MC, 3)
12	(SB + MC, 0)
13	(SB + MC, 1)
14	(SB + MC, 2)
15	(SB + MC, 3)
16	(SB, 0)

0, …, 3 No. of feedbacks, *MC* MixColumns, *SB* SubBytes, *s1, s2, s3* Components of SB

For example, higher generation efficiency contributes to quicker key generation with a Fuzzy Extractor.

The notations used here are as follows: $\mathsf{HD}(A, B)$ denotes the Hamming distance between the two bit sequences A and B, and $A \cap B$ denotes the bitwise AND of A and B. $\mathsf{HW}(A)$ denotes the Hamming weight of A. The i-th response and mask of the Glitch PUF for the chip labeled k are denoted as W_i^k and S_i^k. Specifically, W_0^k and S_0^k represent the response and mask measured under the normal temperature and voltage, (27 °C, 1.20 V). They are obtained only once per chip and used as reference values for each chip. For $i > 0$, the operation environment is not necessarily the same as that for $i = 0$. Note that S_i^k $(i > 0)$ is practically no use.

Robustness

Robustness represents the extent to which a PUF can reproduce responses that are almost the same as the initial response. It is thus quantified by the Hamming distance between the initial response and each response afterwards. This chapter employs an equivalent notion of the bit error rate (BER), the Hamming distance divided by the number of bits in responses. For Glitch PUFs, BER must be defined for effective bits that remain after the masking operation. Therefore, the BER of the chip k for i-th response is defined as follows:

$$\mathrm{BER}_i^k := \mathsf{HD}(W_0^k \cap S_0^k, W_i^k \cap S_0^k)/\mathsf{HW}(S_0^k).$$

Finally, the BER of the chip k is calculated as the average of BER_i^k with respect to i:

$$\mathrm{BER}^k := \frac{1}{M}\sum_{i=1}^{M}\mathrm{BER}_i^k,$$

where M denotes the number of measurements, and $M = 100$ in this paper.

Uniqueness
Uniqueness measures the extent to which PUFs across chips can generate different responses given the same challenge. Uniqueness is thus quantified by the Hamming distance between a pair of responses for different chips. In the same way as robustness, the Hamming distance divided by the number of bits in responses is employed to represent uniqueness, and hence the value of uniqueness is denoted as FHD for fractional hamming distance. First, the FHD of the chip k compared with the chip l is defined as follows:

$$\mathrm{FHD}_l^k := \mathsf{HD}(W_0^k \cap S_0^k, W_0^l \cap S_0^k)/\mathsf{HW}(S_0^k).$$

Then, the FHD of the chip k is calculated as the average of FHD_l^k with respect to l:

$$\mathrm{FHD}^k := \frac{1}{K-1}\sum_{l\neq k}\mathrm{FHD}_l^k,$$

where K denotes the number of chips, and $K = 6$ in this chapter.

Generation Efficiency
Generation efficiency of a Glitch PUF represents how many bits remain after the masking operation. Thus, it is quantified by the percentage of bits in a mask that have the value 1. The generation efficiency for the chip k, denoted as GE^k, is defined as follows:

$$\mathrm{GE}^k := \mathsf{HW}(S_0^k)/N.$$

28.5.3 Evaluation Results

The summary of the evaluation results is as follows. In Spartan-3A, the Glitch PUF using the number 6 glitch generator can meet the required performance for key generation with a Fuzzy Extractor. However, in Spartan-6, none of the glitch generator designed in this chapter can meet the requirement. In fact, the existing work [23] shows that the error rate of a Glitch PUF is worse in Spartan-6 than in Spartan-3A. The results of this chapter further suggest that in Spartan-6 the uniqueness is better while the robustness is worse. One possible reason is the difference in manufacturing process: Spartan-3A uses a 90 nm process while Spartan-6 uses a 45 nm process.

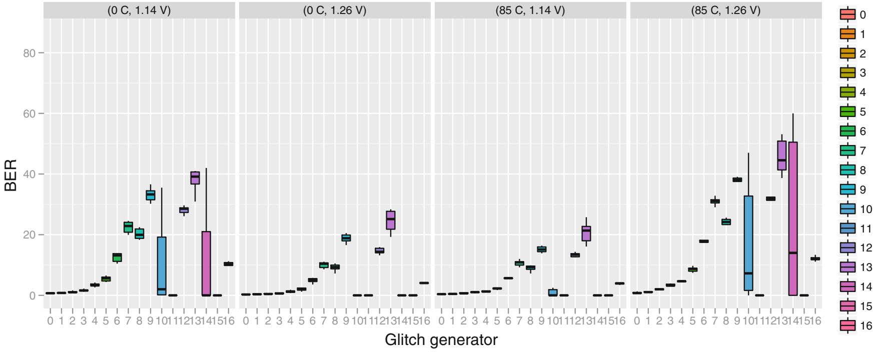


Fig. 28.10 Robustness for Spartan-3A

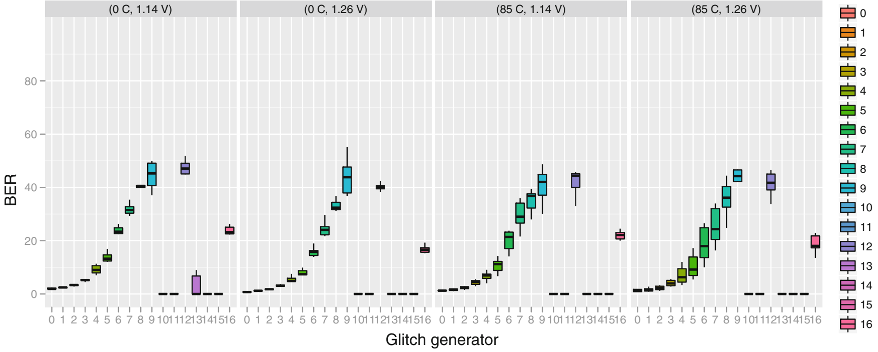


Fig. 28.11 Robustness for Spartan-6

It is possible that a smaller process causes a larger amount of glitches. A further study is needed on the construction of a glitch generator.

Each result is detailed in what follows.

Robustness

The evaluation results of BER^k are shown in Figs. 28.10 and 28.11. The evaluation is done for the four corner cases to find the worst one. In order to implement a key generator combining a PUF and a Fuzzy Extractor in a reasonable circuit size, the error rate must be around 15% at most. Selecting glitch generators by this criterion will get the numbers 1 through 6 and 16 for Spartan-3A, and the numbers 1 through 5 for Spartan-6. Note that although the number 11 for Spartan-3A, for example, has the error rate of nearly 0%, that is merely the result of low generation efficiency. The generation efficiency will be shown later in Fig. 28.14.

Uniqueness

The evaluation results of FHD^k are shown in Figs. 28.12 and 28.13. Among the glitch generators selected by the robustness criterion, the number 6 of Spartan-3A exhibits

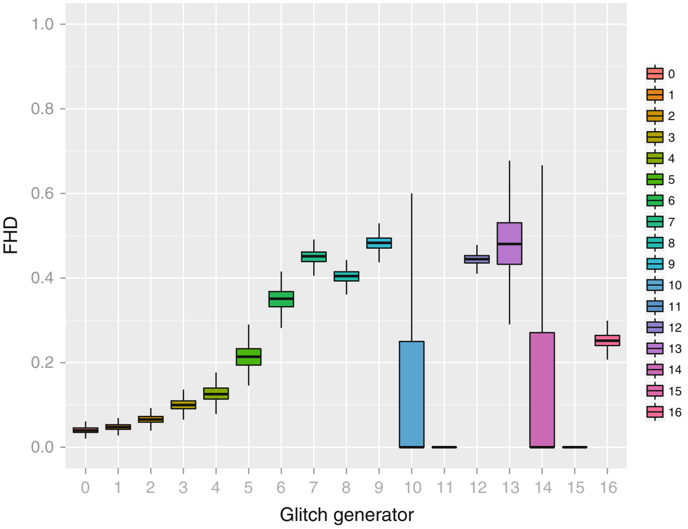


Fig. 28.12 Uniqueness for Spartan-3A

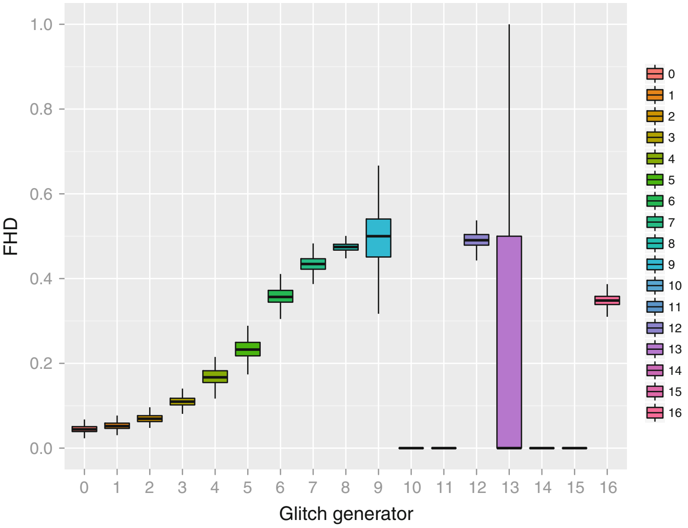


Fig. 28.13 Uniqueness for Spartan-6

the highest uniqueness of about 37%, and the number 5 of Spartan-6, about 23%. The value for Spartan-6 is too low to be used as a PUF.

Generation Efficiency

The evaluation result for generation efficiency is shown in Fig. 28.14. For each glitch generator, the value is the average over all $K = 6$ chips. The number 6 glitch

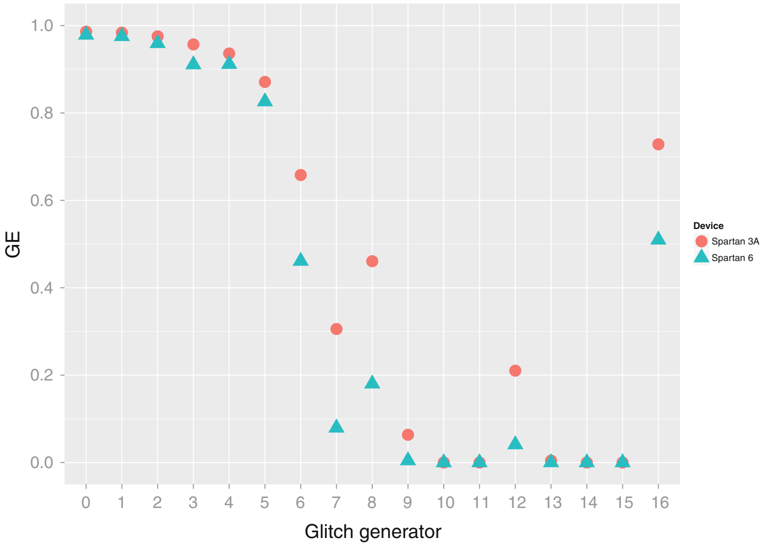


Fig. 28.14 Generation efficiency of the Glitch PUF

generator of Spartan-3A has the generation efficiency of 66%, which is considered sufficient for the purpose of key generation.

28.5.4 Performance of the Random Number Generator

Last, the evaluation results for the proposed physical random number generator are shown. The throughput is calculated to be 1.51 Mbps as the following. The proposed circuit generates a 32-bit sequence per two cycles, the number of repetitions $\mathsf{cnt}_{\mathsf{re}}$ is 255, and the FPGA boards for the experiment operate at 24 MHz. Thus, $(32 \times 24)/(2 \times 255) = 1.51$ (Mbps). The glitch generator used here is the number 13 in Table 28.5, in which the signal path includes both SubBytes and MixColumns with one feedback chain. The complexity of the glitch generator is expected to cause high error rate that generates randomness along with the error accumulation with $\mathsf{cnt}_{\mathsf{re}} = 255$. The proposed random number generator passes two major statistical test suites of NIST SP 800-22 and of Diehard for all the cases. Details are as follows.

Statistical test suites of NIST SP 800-22 [24] and of Diehard [25] are generally used to evaluate the randomness of bit sequences. In this chapter, a sequence of 1 G bits for testing in each of five environmental cases is prepared. The sequence in each case is tested both by the NIST and the Diehard test suites. The procedure of the NIST test suite is as specified in [24]: a sequence of 1 G bits is divided into 1000 subsequences of a fixed size of 1 M bits, and each subsequence is tested by each of the statistical tests. Thus, a total of 1000 subsequences are tested, and 1000

Table 28.6 Pass rate (%) for the NIST suite in (27 °C, 1.20 V)

Test	Parameters	FPGA1	FPGA2	FPGA3	FPGA4	FPGA5	FPGA6	Result
Spartan-3A								
Frequency	–	98.6	99.3	99.1	99.1	99.2	99.1	Pass
Block Frequency	$M = 128$	99.4	99.1	99.1	99.2	98.6	99.1	Pass
Runs	–	99.4	99.1	98.3	98.8	98.6	99.0	Pass
Longest run	$M = 10{,}000$	98.9	98.8	99.4	99.1	98.8	99.0	Pass
Rank	–	99.1	98.8	99.1	99.0	99.1	98.8	Pass
Nonoverlapping templates	$m = 9$	98.3–99.7	97.7–99.7	97.9–99.7	98.3–99.8	98.1–99.7	98.0–99.7	Pass
Overlapping templates	$m = 9$	99.0	98.9	99.3	98.8	98.9	99.1	Pass
Universal	$L = 7$, $Q = 1280$	98.6	98.7	99.0	99.2	99.0	99.2	Pass
Linear complexity	$M = 500$	98.6	98.8	98.7	99.0	98.5	99.4	Pass
Serial	$m = 16$	98.9–99.2	99.0–99.1	98.9–99.3	98.8–99.2	99.2–99.4	98.7–99.4	Pass
Approximate entropy	$m = 10$	98.8	99.4	99.1	98.8	99.0	99.2	Pass
Cumulative sums	–	98.6–98.8	99.2–99.6	99.0–99.1	98.9–99.0	99.0–99.4	98.8–99.3	Pass
Random excursions	–	98.1–99.3	98.7–99.7	98.2–99.5	98.0–99.4	98.7–99.4	98.6–99.8	Pass
Random excursions variant	–	98.5–99.7	98.5–99.7	98.3–99.3	98.4–99.7	97.9–99.7	98.1–99.5	Pass
Spartan-6								
Frequency	–	99.4	98.5	99.3	98.9	99.0	99.3	Pass
Block Frequency	$M = 128$	98.5	98.7	99.3	99.1	98.8	98.6	Pass
Runs	–	99.1	98.8	98.8	98.9	98.6	99.0	Pass
Longest run	$M = 10{,}000$	98.7	99.2	98.8	98.1	98.7	99.2	Pass
Rank	–	98.5	99.3	99.2	99.1	99.0	98.8	Pass
Nonoverlapping templates	$m = 9$	98.2–99.7	98.1–99.8	98.3–99.8	98.3–99.7	98.1–99.9	97.2–99.6	Pass
Overlapping templates	$m = 9$	98.9	99.0	99.1	98.6	98.6	98.8	Pass
Universal	$L = 7$, $Q = 1280$	98.9	99.2	98.2	99.1	99.2	98.5	Pass
Linear complexity	$M = 500$	98.6	99.4	99.0	99.2	99.0	98.9	Pass

(continued)

Table 28.6 (continued)

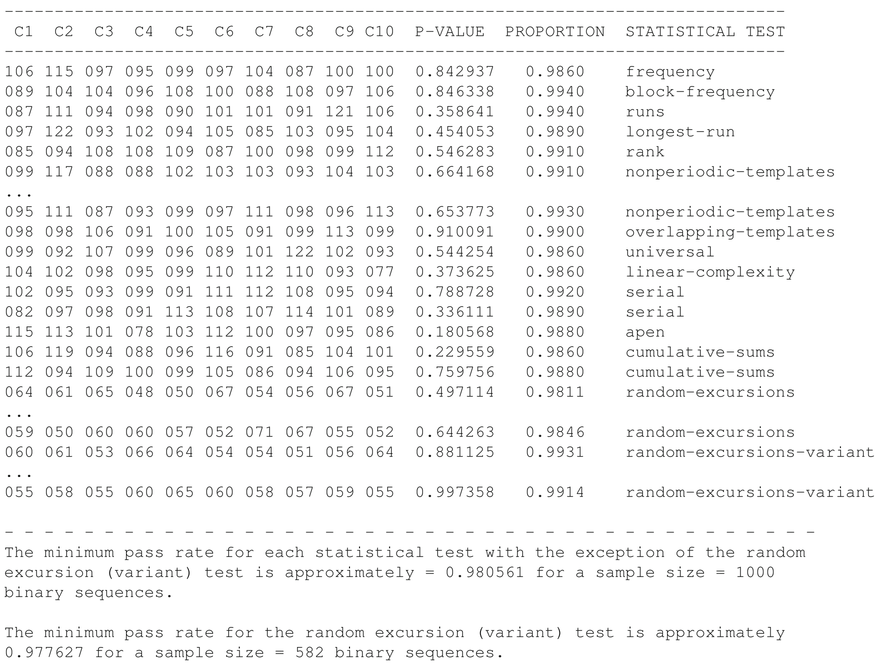
Test	Parameters	FPGA1	FPGA2	FPGA3	FPGA4	FPGA5	FPGA6	Result
Serial	$m = 16$	98.6–98.6	98.4–98.5	98.5–98.5	98.5–98.8	99.2–99.2	99.1–99.2	Pass
Approximate entropy	$m = 10$	99.5	98.7	98.7	98.5	99.2	98.3	Pass
Cumulative sums	–	99.1–99.3	98.4–98.5	99.1–99.3	99.0–99.2	98.9–99.1	99.1–99.4	Pass
Random excursions	–	98.7–99.7	98.4–99.8	98.6–99.4	97.8–99.5	98.0–99.3	98.3–99.2	Pass
Random excursions variant	–	99.0–99.5	98.4–99.5	98.4–99.5	98.3–99.5	98.5–99.3	98.3–99.5	Pass

Table 28.7 Pass rate (%) for diehard

(°C, V)	FPGA1	FPGA2	FPGA3	FPGA4	FPGA5	FPGA6	Result
Spartan-3A							
(0, 1.14)	98.7	99.1	99.1	99.1	99.1	99.1	Pass
(0, 1.26)	99.2	99.1	99.2	99.1	99.0	99.0	Pass
(27, 1.20)	98.8	99.4	99.2	99.1	98.9	98.8	Pass
(85, 1.14)	98.9	98.9	99.1	99.3	99.1	98.6	Pass
(85, 1.26)	98.8	99.2	99.3	98.9	99.4	99.3	Pass
Spartan-6							
(0, 1.14)	98.8	98.8	99.2	99.1	99.0	98.8	Pass
(0, 1.26)	99.1	99.2	99.0	99.1	98.6	99.0	Pass
(27, 1.20)	99.1	99.0	99.1	99.1	99.4	99.1	Pass
(85, 1.14)	99.0	99.2	99.1	99.3	99.0	99.1	Pass
(85, 1.26)	99.2	99.1	99.0	98.9	99.2	98.8	Pass

p-values are obtained for each test. A p-value is the probability of a tested subsequence coinciding with the statistical property that the test assumes. Not only high p-values but uniformly distributed p-values are desirable from viewpoints of randomness. As to the Diehard test suite, about 80 M bits is required for a single test run. Therefore, a sequence of 1 G bits is divided into 12 subsequences of a fixed size of 80 M bits, and each subsequence is tested by the test suite. Because 220 p-values are returned by one test run, a total of 2640 p-values are obtained by 12 test runs.

The evaluation results are supplied in Tables 28.6 and 28.7. To show p-values, a sample output of the NIST test suite is also presented in Fig. 28.15. The p-values correspond to the result for FPGA1 of Spartan-3A in Table 28.6. Note that those are only part of all results due to space limitations.



```
------------------------------------------------------------------------------
 C1  C2  C3  C4  C5  C6  C7  C8  C9 C10  P-VALUE  PROPORTION  STATISTICAL TEST
------------------------------------------------------------------------------
106 115 097 095 099 097 104 087 100 100  0.842937   0.9860    frequency
089 104 104 096 108 100 088 108 097 106  0.846338   0.9940    block-frequency
087 111 094 098 090 101 101 091 121 106  0.358641   0.9940    runs
097 122 093 102 094 105 085 103 095 104  0.454053   0.9890    longest-run
085 094 108 108 109 087 100 098 099 112  0.546283   0.9910    rank
099 117 088 088 102 103 103 093 104 103  0.664168   0.9910    nonperiodic-templates
...
095 111 087 093 099 097 111 098 096 113  0.653773   0.9930    nonperiodic-templates
098 098 106 091 100 105 091 099 113 099  0.910091   0.9900    overlapping-templates
099 092 107 099 096 089 101 122 102 093  0.544254   0.9860    universal
104 102 098 095 099 110 112 110 093 077  0.373625   0.9860    linear-complexity
102 095 093 099 091 111 112 108 095 094  0.788728   0.9920    serial
082 097 098 091 113 108 107 114 101 089  0.336111   0.9890    serial
115 113 101 078 103 112 100 097 095 086  0.180568   0.9880    apen
106 119 094 088 096 116 091 085 104 101  0.229559   0.9860    cumulative-sums
112 094 109 100 099 105 086 094 106 095  0.759756   0.9880    cumulative-sums
064 061 065 048 050 067 054 056 067 051  0.497114   0.9811    random-excursions
...
059 050 060 060 057 052 071 067 055 052  0.644263   0.9846    random-excursions
060 061 053 066 064 054 054 051 056 064  0.881125   0.9931    random-excursions-variant
...
055 058 055 060 065 060 058 057 059 055  0.997358   0.9914    random-excursions-variant

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
The minimum pass rate for each statistical test with the exception of the random
excursion (variant) test is approximately = 0.980561 for a sample size = 1000
binary sequences.

The minimum pass rate for the random excursion (variant) test is approximately
0.977627 for a sample size = 582 binary sequences.
```

Fig. 28.15 Sample output of the NIST SP 800-22 test suite

28.6 Conclusions

This chapter proposes a unified coprocessor for secure key storage and challenge-response authentication that efficiently combines an Fuzzy Extractor, a Glitch PUF, and an AES circuits. The architecture is designed around an AES circuit to be used for multiple purposes: key generation and random number generation by a Glitch PUF in addition to the normal encryption and decryption. The sharing structure contributes to compactness of the whole circuit. The use of a PUF adds tamper resistance to key storage. A coprocessor for secure key storage and challenge-response authentication is thus realized. Alongside, the physical random number generator is realized using the same circuit as the key generator. Evaluations of the PUF and the random number generator are performed for the FPGAs, Spartan-3A, and Spartan-6 by Xilinx. As a result, the Glitch PUF in Spartan-3A is proven to meet the required performance for key generation. In Spartan-6, however, none of the glitch generators designed in this chapter can meet the balance of robustness and uniqueness. It is, therefore, necessary to study glitch generators in greater detail. On the other hand, the physical random number generator is proven to pass the two major statistical test suites for randomness, NIST SP 800-22 and Diehard both in Spartan-3A and Spartan-6, even when the operation environment changes.

The unified security coprocessor is applicable to a wide range of LSIs thanks to downsizing and no need of special-purpose manufacturing process. Three functions, generation of a unique key, encryption, and authentication can be implemented in a small circuit area by letting them share part of their components. The required area is thus one-third compared to the case where each function is separately implemented. We believe that the technology can be modularized and thereby easily applied in a general LSI design flow. The technology contributes to reducing security risks involved in networked devices, for example, by protecting embedded programs and preventing spoofing of devices.

References

1. K. Shimizu, D. Suzuki, T. Tsurumaru, T. Sugawara, M. Shiozaki, T. Fujino, Unified coprocessor architecture for secure key storage and challenge-response authentication. IEICE Trans. **E97-A**(1), 264–274 (2014)
2. R.S. Pappu, Physical one-way functions. Ph.D. Thesis, M.I.T., http://pubs.media.mit.edu/pubs/papers/01.03.pappuphd.powf.pdf (2001)
3. B. Gassend, D. Clarke, M. van Dijk, S. Devadas, Silicon physical random functions, in *Proceedings of the 9th ACM Conference on Computer and Communications Security (CCS 2002)* (2002), pp. 148–160
4. Y. Dodis, M. Reyzin, A. Smith, Fuzzy extractors: how to generate strong keys from biometrics and other noisy data, in *Eurocrypt 2004*. LNCS 3027 (Springer, 2004), pp. 523–540
5. P. Tuyls, L. Batina, RFID-tags for anti-counterfeiting, in *CT-RSA 2006*. LNCS 3860 (Springer, 2006), pp. 115–131
6. R. Maes, Physically unclonable functions: constructions, properties and applications. Ph.D. Thesis, KU Leuven, http://www.cosic.esat.kuleuven.be/publications/thesis-211.pdf (2012)
7. J. Guajardo, S.S. Kumar, G.J. S̃chrijen, P. Tuyls, FPGA intrinsic PUFs and their use for IP protection, in *CHES 2007*. LNCS 4727 (Springer, 2007), pp. 63–80
8. J.W. Lee, D. Lim, B. Gassend, G.E. Suh, M. van Dijk, S. Devadas, A technique to build a secret key in integrated circuits for identification and authentication applications, in *Proceedings of the IEEE VLSI Circuits Symposium* (2004), pp. 176–179
9. G.E. Suh, S. Devadas, Physical unclonable functions for device authentication and secret key generation, in *Proceedings of the 44th Annual Design Automation Conference (DAC 2007)* (2007), pp. 9–14
10. S.S. Kumar, J. Guajardo, R. Maes, G.J. S̃chrijen, P. Tuyls, Extended abstract: the butterfly PUF: protecting IP on every FPGA, in *Proceedings of the IEEE International Workshop on Hardware-Oriented Security and Trust 2008 (HOST 2008)* (2008), pp. 67–70
11. M. Majzoobi, F. Koushanfar, M. Potkonjak, Lightweight secure PUFs, in *Proceedings of the IEEE/ACM International Conference on Computer-Aided Design (ICCAD 2008)* (2008), pp. 670–673
12. C. B̈osch, J. Guajardo, A.-R. Sadeghi, J. Shokrollahi, P. Tuyls, Efficient helper data key extractor on FPGAs, in *CHES 2008*. LNCS 5154 (Springer, 2007), pp. 181–197
13. R. Maes, P. Tuyls, I. Verbauwhede, Low-overhead implementation of a soft decision helper data algorithm for SRAM PUFs, in *Proceedings of the 2009 IEEE International Symposium on Information Theory (ISIT 2009)* (2009), pp. 2101–2105
14. D. Suzuki, K. Shimizu, The Glitch PUF: A new delay-PUF architecture exploiting glitch shapes, in CHES 2010. LNCS **6225**, 366–384 (2010)
15. K. Shimizu, D. Suzuki, Glitch PUF: extracting information from usually unwanted glitches. IEICE Trans. Fundam. Electron. Commun. Comput. Sci. **E95-A**(1) (2012)

16. D. Suzuki, K. Shimizu. T. Tsurumaru, T. Sugawara, M. Shiozaki, T. Fujino, Device key generator using glitch PUFs, in *SCIS 2012* (2012) [in Japanese]
17. B. Sunar, W. Martin, D. Stinson, A provabley secure true random number generator with built-in tolerance to active attacks. IEEE Trans. Comput. **56**(1), 109–119 (2007)
18. M. Dichtl, J. Dj, Golic: High-speed true random number generation with logic gates only, in CHES 2007. LNCS **4727**, 45–62 (2007)
19. K. Wold, C.H. Tan, Analysis and enhancement of random number generator in FPGA based on oscillator rings, in *Proceedings of the International Conference on Reconfigurable Computing and FPGAs* (2008), pp. 385–390
20. C.W. O'Donnell, G.E. Suh, S. Devadas, PUF-based random number generation. Technical Report 481, (MIT CSAIL, 2004), http://csg.csail.mit.edu/pubs/memos/Memo-481/Memo-481.pdf
21. A. Maiti, R. Nagesh, A. Reddy, P. Schaumont, Physical unclonable function and true random number generator: a compact and scalable implementation, in *GLSVLSI 2009, Proceedings of the 19th ACM Great Lakes symposium on VLSI* (ACM, 2009), pp. 425–428
22. A. Satoh, S. Morioka, K. Takano, S. Munetoh, A compact rijndael hardware architecture with S-box optimization, in *ASIACRYPT 2001*. LNCS 2248 (Springer, 2001), pp. 239–254
23. D. Yamamoto, G. Hospodar, R. Maes, I. Verbauwhede, Performance and security evaluation of AES S-box-based glitch PUFs on FPGAs, in *SPACE 2012*. LNCS 7644 (Springer, 2012), pp. 45–62
24. NIST Special Publication 800-22: *A Statistical Test Suite for Random and Pseudorandom Numbers* (2000)
25. G. Marsaglia, Diehard battery of tests of randomness, http://stat.fsu.edu/pub/diehard/

Chapter 29
SRAM-Based Physical Unclonable Functions (PUFs) to Generate Signature Out of Silicon for Authentication and Encryption

Koji Nii

Abstract In this Chapter, we demonstrate chip-ID generation schemes using SRAM-based physical unclonable functions (PUFs) for secure system LSIs. An SRAM-based PUF using failure bit addresses is presented first and discussed on how to improve the uniqueness and reliability of generated IDs. A test chip for chip-ID generation system with memory built-in-self-test (BIST) is implemented using 90-nm CMOS technology. The measured data shows that over 99.9% stable chip-IDs are given by using multiple test scheme with ideal uniqueness, which is obtained by Hamming distance evaluation. Next, we compare three types of SRAM-based PUFs, which are (1) initial data with single power-on, (2) initial data with divided-power-on, and (3) conflicted data after low/low (L/L) writing, in the point of views of uniqueness and reliability. Based on the measurement results obtained with test chips fabricated using 45-nm CMOS bulk technology, theoretical values of uniqueness are obtained in these three schemes. In contrast, results show that higher reliability against variations of temperature and voltage conditions is achieved using the divided-power-on scheme compared to those of single power-on scheme and L/L writing scheme.

Keywords Physical unclonable function • PUF • SRAM • Intrinsic identification (ID) • Uniqueness • Reliability

29.1 Introduction

An intrinsic unique identification number for each chip (chip-ID) is strongly demanded for secure system LSIs to achieve high dependability against tampering and high traceability in production control systems. Conventionally, the assigned

K. Nii (✉)
Renesas Electronics Corporation, Tokyo, Japan
e-mail: koji.nii.uj@renesas.com

S. Asai (ed.), *VLSI Design and Test for Systems Dependability*,
https://doi.org/10.1007/978-4-431-56594-9_29

chip-IDs for authentications and/or encryptions are written into an electrical fuse or into a programmable ROM embedded into a die. These schemes are extremely simple methods that require no additional special IPs. However, there are high risks of thefts for cloning artificially by attackers with physical analysis or signal/power noise analysis. To prevent tampering, physical unclonable functions (PUFs), which will be used for security applications in authentications, cryptographic key generation, and prevention of unauthorized copies, is proposed as the most secure means to generate dependable chip-IDs [1–13].

There are several types of PUFs. Delay-based PUFs (arbiter and ring oscillator) and Bi-stable-based PUFs using sense amplifier have been reported. These schemes entail area penalties and additional hardware IPs that increases design costs. Meanwhile, nonvolatile memory (NVM)-based PUFs have also reported. Those are feasible if the embedded NVM process is applied, otherwise additional manufacturing process steps are needed. SRAM-based PUFs are major candidates for implementation to embed into a chip because of the ease of using existing embedded SRAM IPs, which usually work as on-die buffers or cache memories. The SRAM-based PUFs generate chip-ID using initial data after power-on, written data with any conflicting, or extracting the failure bit addresses for reading operation under unstable bias condition. These PUFs are using device variations or fluctuations for ID generation.

Key challenges of PUFs are mainly uniqueness and reliability. Uniqueness is a requirement for generating exactly different ID for each different chip. It is often evaluated by using Hamming distance. The reliability is a requirement for generating same ID in the same chip at any time against any change of voltage and temperature, and against aging of devices. It is quantified as a stability, which shows the percentages of the numbers of correct ID generation per whole numbers of generating. For example, 100% stability means that there is no error for chip-ID generations in repetitions, exactly same ID is generated every time.

In the next section, we describe an ID generation scheme which, without additional hardware IP, extracts a unique fingerprint from each chip using random bit failures caused by less static-noise-margins (SNM) under the ID generation mode with on-chip memory BIST (MBIST). The test chip measurement results are also shown. In the following Sect. 29.3, we compare three SRAM-based PUFs: (1) single power-on scheme, (2) divided-power-on scheme, and (3) conflict L/L writing scheme from the viewpoints of uniqueness and reliability. Then, the measurement results of uniqueness and reliability for varied voltage and temperature conditions are discussed herein. Identification failure rates and the fingerprint generating time are also reported in this section. The final Sect. 29.4 summarizes SRAM-based PUFs.

29.2 A Unique Chip-ID Generation Scheme Using SRAM-Based PUF with Random Fail-Bit Addresses

Figure 29.1 represents a concept of our proposal. The SRAM operating margins are susceptible to the random variation of threshold voltage (V_t) in the six-transistor–memory cells [14]. If the supply voltage of wordline (WL) driver (V_{WL}) is raised from the ratings to a certain degree, bit failures appear randomly over the chip due to the degradation of SNM, generating a signature in terms of physical locations of failed bits that is unique to each individual chip. Therefore, a unique ID can be generated from the fail-bits under the operating conditions chosen for the purpose. Note that only the SNM failures are used for ID generation and solid failures are eliminated by redundant circuit before shipping. Figure 29.2a portrays the bias condition used to obtain the fail-bit information during the ID generation. In order to not reduce the test speed during the ID generation, only V_{WL} is raised in the memory test with decreased SNM. As shown in Fig. 29.2b, a Monte Carlo simulation demonstrates that a few fail-bits (FBs) appear in the ID generation mode, while all bits are passed in the normal memory operation.

Figure 29.3a depicts the block diagram of proposed SRAM-based chip-ID generation system. The chip fabricated for the proof of concept consists of an

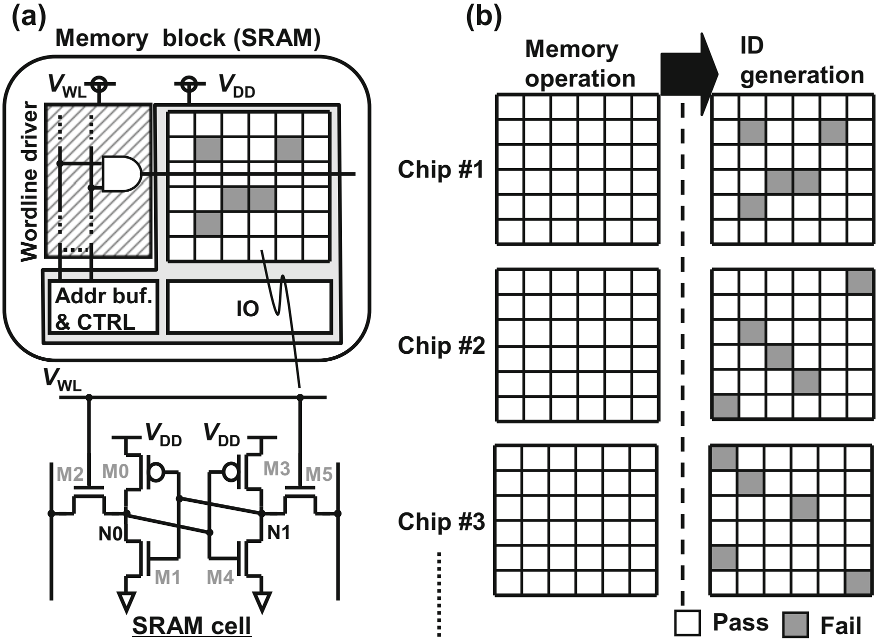


Fig. 29.1 Concept of the SRAM-based chip-ID generating scheme: **a** block diagram of SRAM IP, and **b** fail-bit maps for normal memory operation and ID generation modes

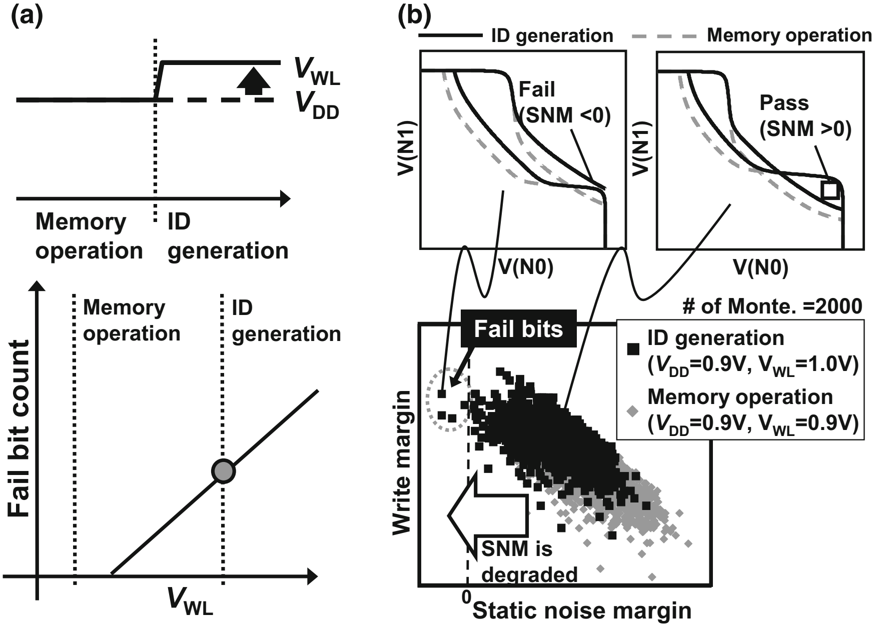


Fig. 29.2 Voltage control scheme in the proposed scheme: **a** only V_{WL} is raised to maintain test speed, and **b** some bits fail in the ID generation mode

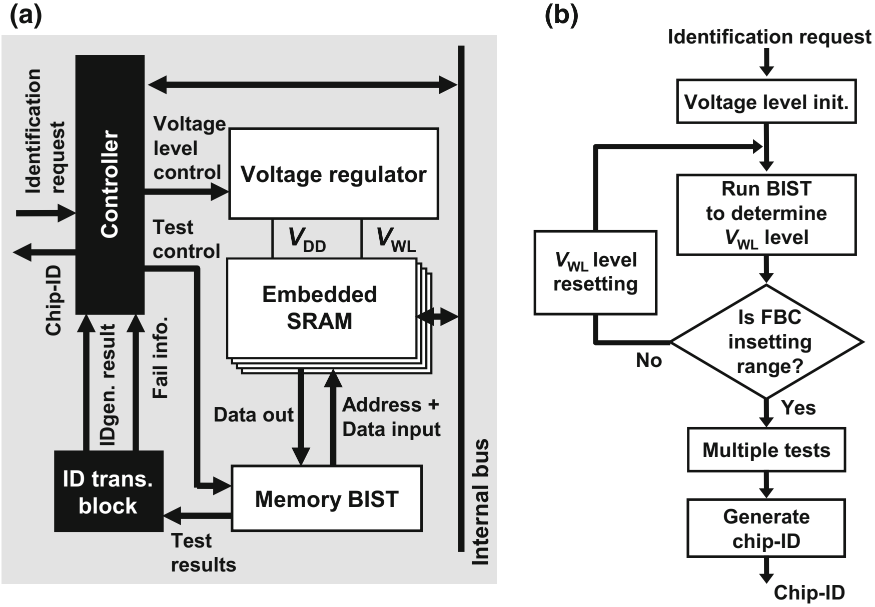
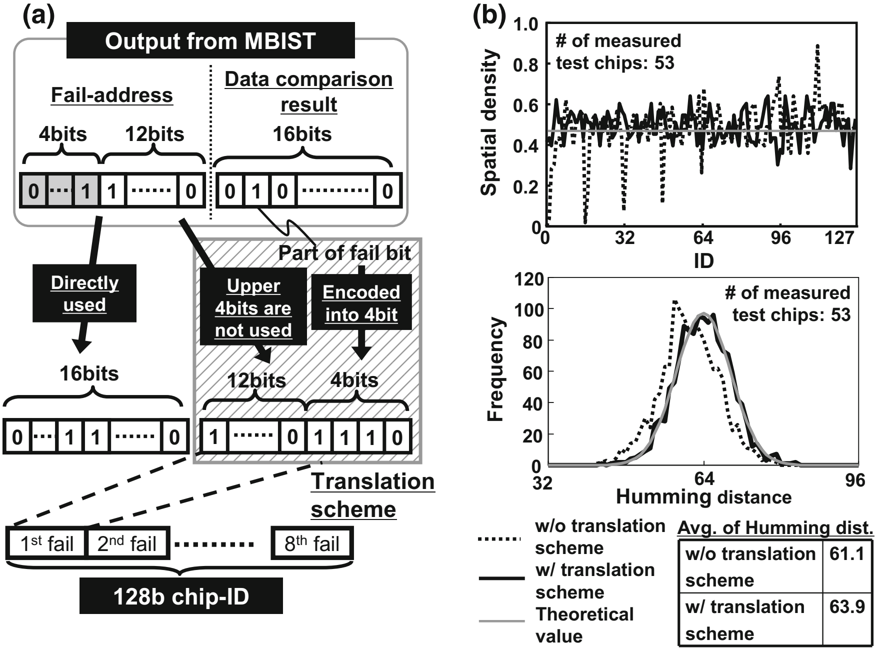


Fig. 29.3 An SRAM-based chip-ID generation system: **a** block diagram, and **b** generation flowchart

SRAM, an MBIST, a voltage regulator, an ID translation block, and a controller. The ID translation block translates the information of the first eight fail-bits to the 128-bit ID. Most SoCs have voltage regulator and SRAM IPs with the MBIST so that only area penalties of proposed scheme are the controller and the ID translation block. The flow of proposed ID generation method is as follows (see also Fig. 29.3b):

1. The voltage regulator initializes the test voltage.
2. The MBIST is run. The FB addresses are detected and the number of FBs (FBC) is counted.
3. At the end of testing, if this FBC is out of the setting range (16–32), then the test voltage level is changed. Due to this mechanism, it is guaranteed that the FB pattern or the signature generated is always identical, even if the temperature during the test may vary from occasion to occasion. Consequently, the temperature tolerance can be achieved by monitoring those FBs without an on-chip temperature sensor.
4. The multiple test schemes in the MBIST is executed at the same voltage condition to increase the ID stability.
5. The ID translation block translates the FB information from the MBIST to the 128-bit ID.

Figure 29.4a depicts the method of translation from the FB information to the chip-ID. SRAMs embedded in recent SoCs have wide data I/O bits and capacities over 1-Mbit. If the width of data I/O is 16, the word depth is 64-k for a 1-Mbit SRAM, which has 16 addresses. A simple approach for generating the ID is to use some FB addresses directly, each having the length of 16-bit lengths. Then, the 128-bit ID will be made up of eight failure addresses by arranging the detected failure addresses in the order of appearance. This ID has uniqueness because of the random locations of fail cells with smaller SNMs. However, the order of appearance of the eight failure addresses may not actually be as reproducible, and thus as unique as can be used as the ID information. To improve the uniqueness of the ID, therefore, we propose a modification to the above-mentioned ID generation by combining both the failure addresses and the failure data I/O bit location. Practically, the modified ID is generated by the lower 12 digits of the failure addresses and four digits encoded from the failure data I/O location of 16 bits. The significant four digits of the FB addresses are not used, eliminating the influence of the order of appearance. Using this scheme, the distribution of "0" and "1" in the ID becomes quite randomized, as it should be. Theoretically, the average Hamming distance of the 128-bit ID becomes 64. The measurement results of 53 test chips are shown in Fig. 29.4b. We confirmed that the proposed translation scheme results in an average Hamming distance by 63.9, which is almost identical to the theoretical value. The output from the MBIST could differ due to the presence of unstable fail-bits. For this reason, the multiple test scheme (Fig. 29.5a) is implemented in the proposed circuit. Multiple tests are executed at the optimal voltage condition determined initially for the ID generation test to come up with the eight FBs. If a FB address is



Avg. of Humming dist.	
w/o translation scheme	61.1
w/ translation scheme	63.9

Fig. 29.4 ID translation scheme of FB information to chip-ID: **a** lower 12 digits of the FB addresses and failure data I/O bit location are translated to 16 bits of the chip-ID, and **b** measurement results of Hamming distances

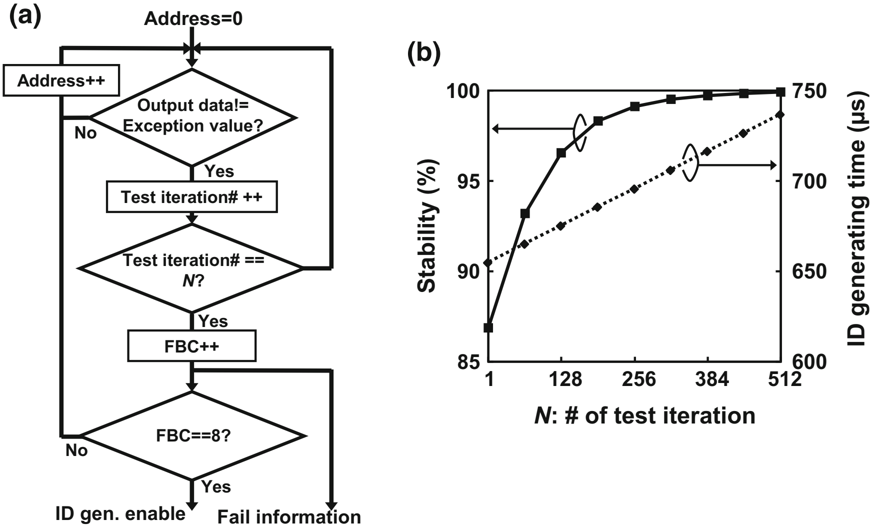


Fig. 29.5 Multiple tests scheme: **a** flowchart, and **b** measured stabilities of chip-ID

passed even once in N iteration tests, this address is excluded from the member of FB addresses used for ID generation. If otherwise, an address has always failed in N tests, this address and data comparison results are translated to 16 bits in the ID. The multiple tests continue until the FBC becomes eight. The multiple tests are not applied to the bits that are always passed, resulting in a shorter test time. The measurement results (Fig. 29.5b) indicate that the stability of ID becomes 99.9% when the number of test iterations is 512. In this case, the test time is 737 μs, which is sufficiently short for practical use. The stability and test time have a trade-off. If longer test time (1.064 ms) is acceptable, higher stability (99.9999999%) can be realized. This value is better than that of authentication (99.99%) using the vein pattern for authentication [15].

Figure 29.6 is the micrograph of test chip fabricated in a 90-nm CMOS technology. Table 29.1 summarizes test chip features. The area overhead is 7200 μm^2, which is smaller than reported elsewhere for a different PUF technology [2]. In future work, by monitoring voltage levels in a chip, side-channel attacks from the external voltage controls will be blocked by detecting the unexpected voltage change, or alternatively generating a mock ID to evade a doubtful identification challenge.

In this section, a chip-ID generation scheme that can be conveniently ported as an SRAM IP has been presented [6]. This enables to extract a unique fingerprint from each chip by using random failure bits in an SRAM under the ID generation mode, and on-chip MBIST. The stability and average of Hamming distance of generated 128-bit IDs using 90-nm technology become 99.9999999% and 63.9, respectively. The proposed scheme does not require any additional hardware IPs.

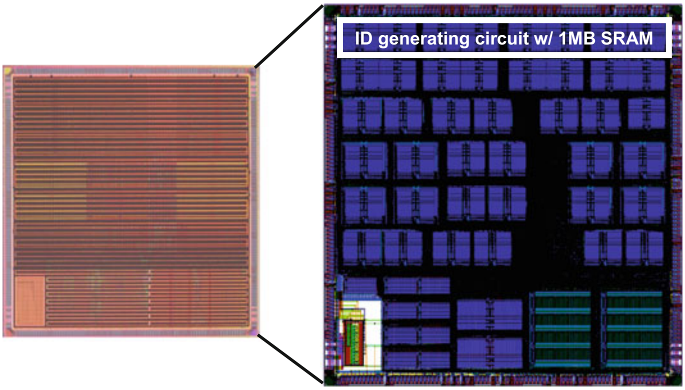


Fig. 29.6 Micrograph and layout plot of the test chip

Table 29.1 Features of the test chip

Process	90-nm CMOS technology	
Area (controller, ID trans. block)	7200 μm^2	
Identity (Humming dist.)	63.9	
Test time	737 μs	1.064 ms
Stability	99.9%	99.9999999%

29.3 Assessing Uniqueness and Reliability of SRAM-Based PUFs from Silicon Measurements

Assessments of the uniqueness and reliability for SRAM-based PUFs embedded in dies were conducted using silicon measurements. To generate unique chip-ID for each die, three types of SRAM-based PUFs were implemented using 45-nm bulk CMOS technology: (1) single power-on scheme, (2) divided-power-on scheme, and (3) L/L writing scheme. Measured Hamming distances of IDs between 64 dies showed no significant advantage or disadvantage in three SRAM-based PUFs in terms of uniqueness, being acceptable for practical use. The measured error rates of IDs in iteration, supply voltage variation, and temperature variation show that the divided-power-on scheme has better reliability than the other schemes.

29.3.1 Power-on Schemes (Initial Values at Power-on)

The simplest means of initializing storage values in an SRAM is power-on [4]. Figure 29.7 presents the concepts of the power-on scheme. The initial storage value is determined by the random V_t variation of the four transistors (M0–M3) in each SRAM memory cell. The butterfly curves at data retention are presented in Fig. 29.7b. For example, the datum in cell 0 is “0” because the left eye is larger than right one. In contrast, the datum in cell 1 becomes “1”. After the voltage is applied, the data read operations are iterated. The readout values out of a chip differ from those out of the others. Therefore, these data can be translated into the unique chip-ID.

In these power-on schemes, the power-on sequence of the SRAM-based PUFs should be designed carefully to ensure correct authentication with high-reliability IDs. For example, if simply using power gating for existing SRAM IPs to enable power-on initializing (presented in Fig. 29.8), then the reliability of the generated IDs might be degraded because of unstable factors. The peripheral circuits in an SRAM IP are unstable at the power-on transition. As presented in Fig. 29.8, it is possible that glitches are generated on wordlines (WLs). Therefore, the initial storage values in memory cells can be affected by some noise from peripheral circuits through access transistors (M4 and M5). Therefore, the initial storage values tend to vary according to environmental conditions.

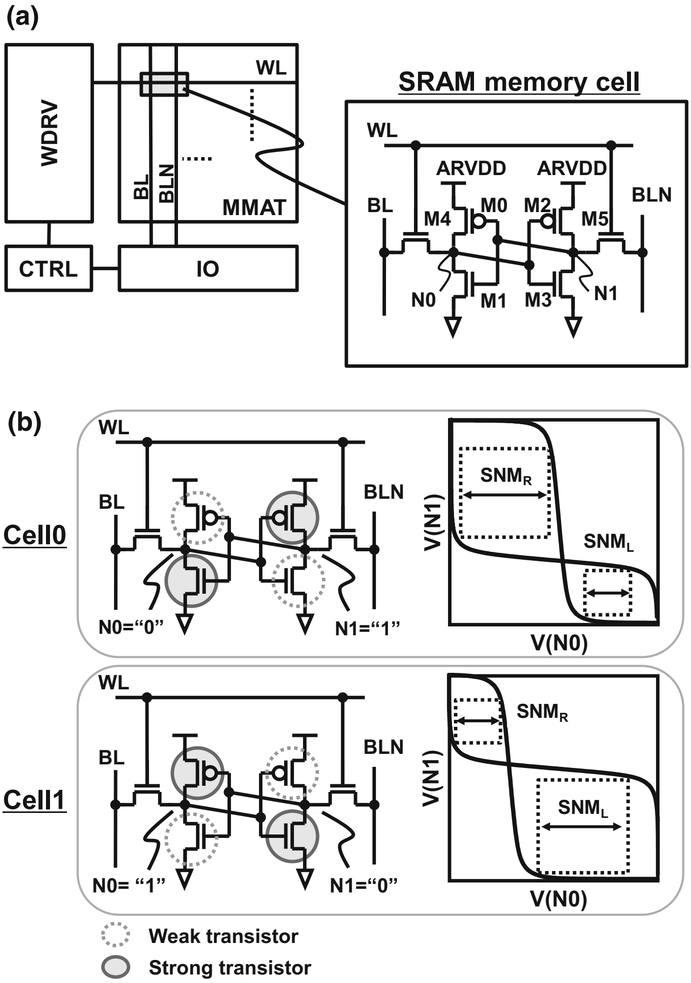


Fig. 29.7 A typical SRAM macro (**a**) and the initial storage values after power-on (**b**)

Application only for power-on the SRAM cell arrays using internal power switch improves the stability of initial values in an SRAM. As depicted in Fig. 29.9, the voltage domain is divided into peripheral circuits and cell array regions by two power supply drivers. The power control flow is the following: (1) First, PW1N is activated and the peripheral circuits are powered on. The noise in peripheral circuits occurs as described in an earlier section. However, PW2N, which drives cell array regions, is not activated. Therefore, noise is not transmitted to memory cells. (2) After states of peripheral circuits are decided, PW2N is asserted. The storage values in memory cells are determined by the transistor variation of

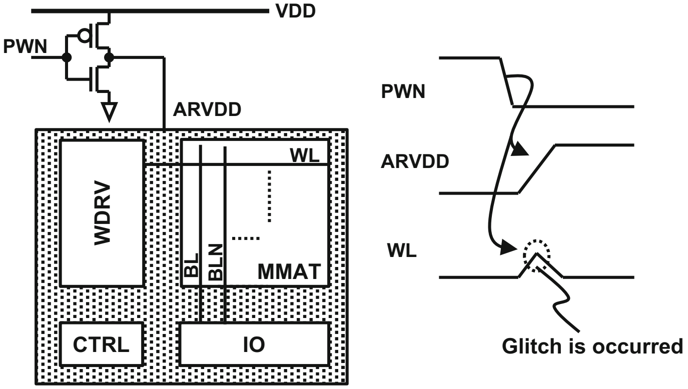


Fig. 29.8 Noise in peripheral circuits in an SRAM at the transition of power-on

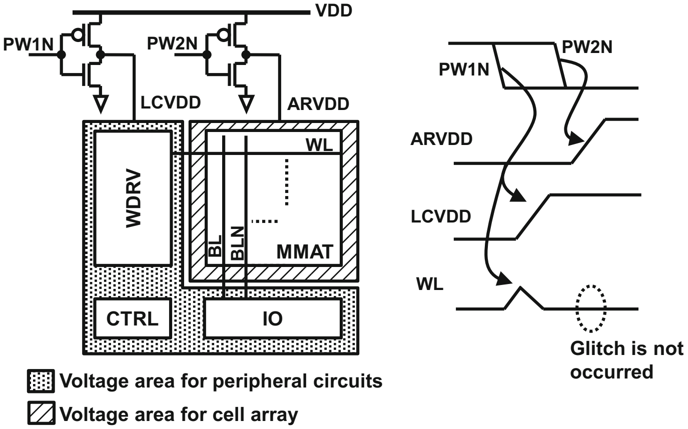


Fig. 29.9 Divided power control scheme that removes noise influences in peripheral circuits

M0–M3 without noise through access transistors. Applying this scheme reduces noise from the peripheral circuits so that the stability of initial values in an SRAM is improved.

29.3.2 Low/Low (L/L) Writing Scheme

The SRAM-based PUF with L/L writing scheme has been proposed in the literature [10]. The concept of chip-ID generation is shown in Fig. 29.10. The generation flow is following: (1) First, both bitlines (BL and BLN) are forced to ground level by a write driver. (2) Then, a WL is activated. Next, both data storage nodes

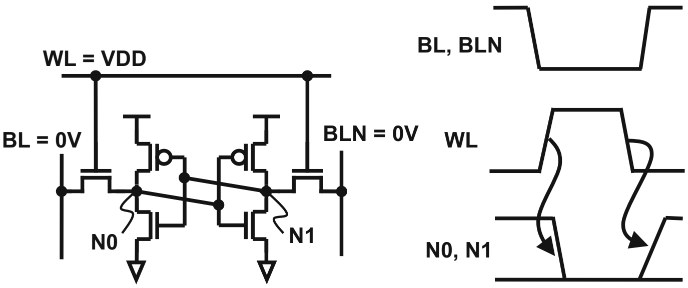


Fig. 29.10 Concept of the L/L write scheme

(N0 and N1) approach the ground levels through the access transistor, but small voltage difference between N0 and N1 would happen because of random V_t fluctuations of M0–M5. (3) After the WL is negated, stored data are determined by extraction along with the small voltage difference.

For the case in which conductance of access transistor is weak, voltages of N0 and N1 do not become ground level perfectly. Figure 29.11 depicts operating waveforms of Monte Carlo simulation at 25 °C, 1.1 V supply voltage (VDD), and process TT (indicates typical PMOS/typical NMOS) corner. Both BL and BLN are set to ground level (VSS). Voltages of storage nodes are varied and are not ground level. This scheme is necessary to modify the write circuitry of the SRAM IP to drive both the BL and BLN to ground level. It takes an area overhead, but it is less than 2%.

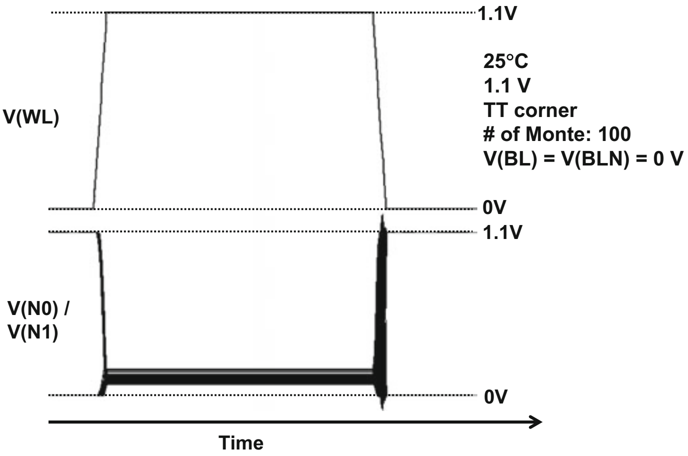
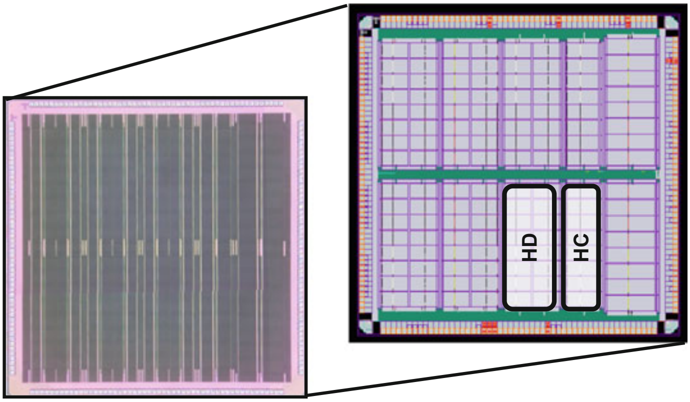


Fig. 29.11 Simulated waveforms derived from Monte Carlo simulation

29.3.3 Measurement Results in a 45-nm Technology

Comparison results by chip measurements are discussed in this section. Figure 29.12 is a micrograph of the test chip fabricated using 45-nm bulk CMOS technology. Two types of 256-kbit SRAM IPs, of which the bitcells were designed as high-density (HD) with small cell size (0.299 μm^2), and high-current (HC) with large cell size (0.374 μm^2). Each SRAM IP has on-chip external power gating, an internal power switch within the cell array, and L/L writing circuitry, as discussed in Sect. 29.3.2. Therefore, we can measure each chip-ID from the same SRAM IP by choosing different ID generating schemes. This generation eliminates other factors, which are within-die variations in physical locations, impedances of power line structures, and so on, to validate the uniqueness and reliability of the generated ID. In the silicon evaluation, we measured each uniqueness and reliability data on the different environment with 64 chips. Here, we consider the 256-bit length ID, generated from the cell array regions of 32 rows × 8 columns of the 256-kbit SRAM IPs partially.

Figure 29.13 depicts the measured Hamming distances for all combinations on 256-bit among different 64 chips at 1.1 V typical supply voltage and 25 °C. Almost identical distributions were obtainable for all schemes for both HD cell and HC cell types. Each mean value (μ) and standard deviation (σ) of the measured Hamming distance is close to the theoretical value: μ = 128.0 and σ = 8.0. Measurement results show all schemes have almost identical uniqueness.



Process	45-nm CMOS technology	
Cell size	HD type	0.299 μm^2
	HC type	0.374 μm^2

Fig. 29.12 Micrograph and layout plot of a test chip including HD and HC types of SRAM memory cells fabricated using 45-nm bulk CMOS technology

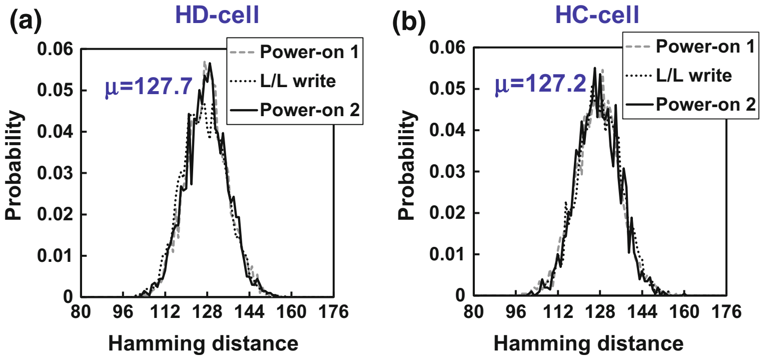


Fig. 29.13 Measured Hamming distance on each 256-bit length ID obtained from 64 measured chips: **a** HD cell at 1.1 V, 25 °C and **b** HC cell at 1.1 V, 25 °C

Even for the same voltage and temperature conditions, the initial values in an SRAM are varied because of noise such as random telegraph noise (RTS). Figure 29.14 presents the Hamming distances on 256-bit in the same chip at 25 °C and 1.1 V. The number of test chips and test iterations are, respectively, 32 and 100. Note that the obtained Hamming distances correspond to the number of error bits in the iterative ID generation in this case.

Applying the divided power control to the power-on scheme, the average of the Hamming distance becomes smaller than those in the others, which means that the divided power control scheme reduces noise from the peripheral circuits.

The measured temperature dependencies of Hamming distances (=no. of error bits) on 256-bit in a chip are shown in Fig. 29.15. Temperature conditions vary from 25 to 125°C. The power-on scheme with divided power control scheme is the most stable against temperature variation.

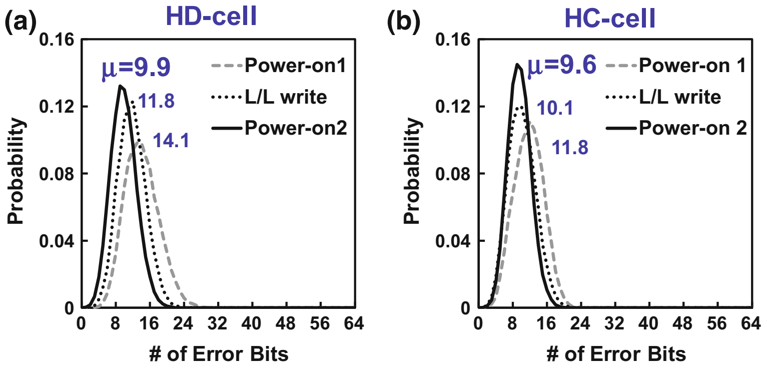


Fig. 29.14 Measured Hamming distance (corresponding to the number of error bits) of 256-bit length ID obtained iteratively at the same condition in a chip: **a** HD cell type at 1.1 V, 25 °C and **b** HC cell type at 1.1 V, 25 °C

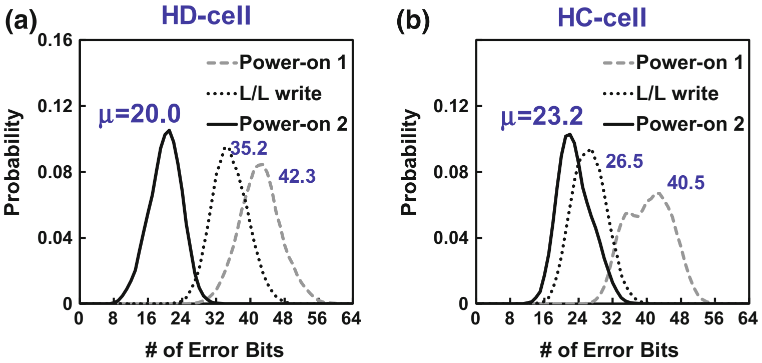


Fig. 29.15 Measured Hamming distance (corresponding to the number of error bits) of 256-bit length ID obtained under different temperature conditions: **a** HD cell type at 1.1 V, 25 and 125 °C, and **b** HC cell type at 1.1 V, 25 and 125 °C

Figure 29.16 presents the measured voltage dependencies of Hamming distances (=no. of error bits) on 256-bit in a chip at 25 °C. The voltage conditions are set as 1.3 V maximum voltage, 1.1 V typical voltage, and 0.9 V minimum voltage. Measurement results at 1.3 V versus 1.1 V are almost identical to those in cases where voltage is not changed so that no voltage dependencies appear if the voltage becomes high. However, when the supply voltage is lowered, L/L writing scheme becomes fragile because performances of the access transistors are degraded.

Figure 29.17 presents measured Hamming distances (=no. of error bits) when both the temperature and voltage conditions are varied. As discussed above, the power-on scheme with divided power control scheme is suitable for SRAM-based PUF, which demands high reliability.

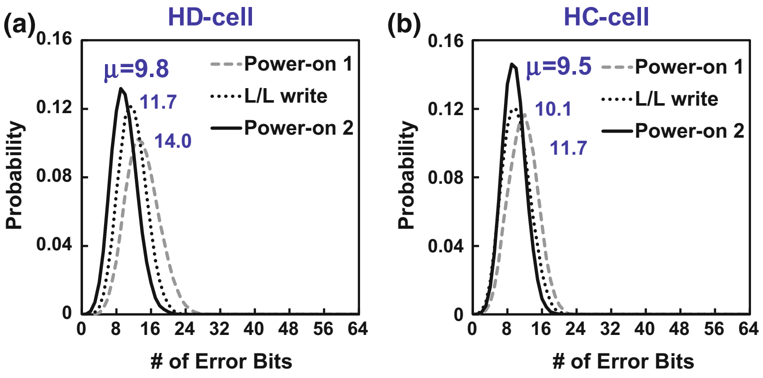


Fig. 29.16 Measured Hamming distance (corresponding to the number of error bits) of 256-bit length ID obtained different voltage conditions: **a** HD cell type (1.1 V vs. 0.9 V), and **b** HC cell type (1.1 V vs. 0.9 V)

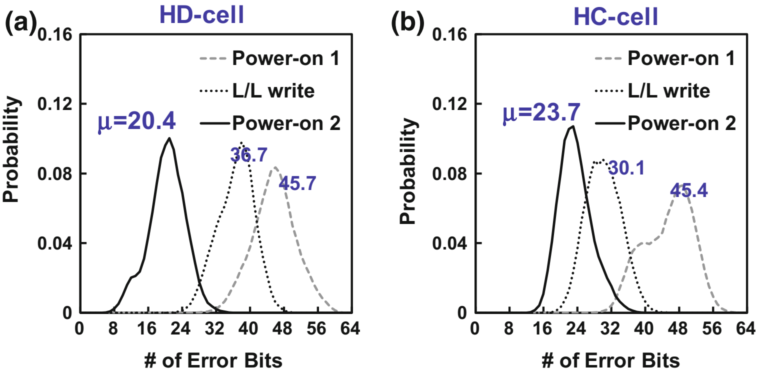


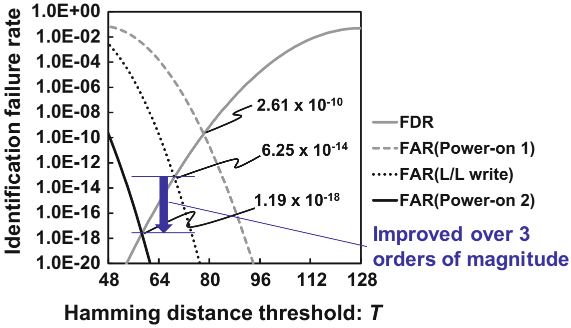
Fig. 29.17 Measured Hamming distances when both voltage and temperature conditions are changed: **a** HD cell type (1.1 V, 25 °C vs. 0.9 V, 125 °C) and **b** HC cell type (1.1 V, 25 °C vs. 0.9 V, 125 °C)

29.3.4 Estimation of Failure Rate and Generation Time

The failure rates of identification in three schemes were assessed. Assuming that a generated fingerprint is identifiable where the Hamming distance is zero or less than a threshold *T*, then the identification failure rate differs according to *T*. For chip identification, two kinds of error probability exist: the false alarm rate (FAR), which corresponds to the authentication failure of registered devices; and the false detection rate (FDR), which corresponds to authentication of a latent (and/or fake) device as a registered device [2].

Here, we assume a normal distribution for the Hamming distance. For simplicity, μ and σ of the FDRs are 128 and 8, respectively. In contrast, the values in Fig. 29.17 are used as those of the FARs. Figure 29.18 shows the approximate FARs and FDRs. The identification failure rates change when *T* is varied and the cross points of FAR and FDR curves become their minimum values. The minimum identification failure rates become 1.19 × 10^{-18} in the HD cell and 1.99 × 10^{-18}

Fig. 29.18 Estimated FDR and FAR (1.1 V, 25 °C vs. 0.9 V, 125 °C) curve for HD cell type



in the HC cell applying divided voltage control to a single power-on scheme. These values are 0.002% and 0.38% compared to those of the L/L writing scheme.

The generation time is also estimated. Formulae of generating time in power-on 1, L/L writing, and power-on 2 are the following.

- $T_{\mathrm{power\_on1\_total}} = T_{\mathrm{pon1}} + T_{\mathrm{cycle}} \times N_{\mathrm{ID}} / N_{\mathrm{IO}}$
- $T_{\mathrm{LL\_write\_total}} = T_{\mathrm{pon1}} + T_{\mathrm{cycle}} \times N_{\mathrm{ID}} / N_{\mathrm{IO}} \times 2$
- $T_{\mathrm{power\_on2\_total}} = T_{\mathrm{pon2}} + T_{\mathrm{cycle}} \times N_{\mathrm{ID}} / N_{\mathrm{IO}}$

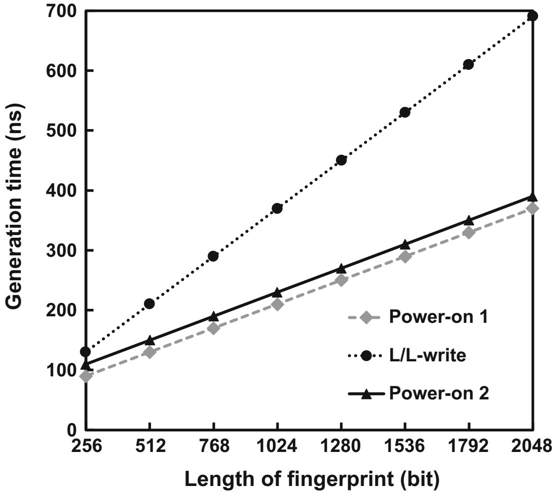
Here, variables of $T_{\mathrm{power\_on1\_total}}$, $T_{\mathrm{LL\_write\_total}}$, $T_{\mathrm{power\_on2\_total}}$, T_{pon1} T_{pon2} T_{cycle} N_{ID}, N_{IO} indicate total time of fingerprint generation in power-on 1, total time of fingerprint generation in L/L writing, total time of fingerprint generation in power-on 2, period after PWN is asserted until circuits in an SRAM are stabilized in power-on 1, period after PWN1 is asserted until values of memory cells are stabilized in power-on 2, cycle time of read and write operation, number of fingerprint lengths, number of I/O bit widths, respectively.

From the measured data, we set variables as $T_{\mathrm{pon1}} = 50$ ns, $T_{\mathrm{pon2}} = 70$ ns, $T_{\mathrm{cycle}} = 5$ ns, and $N_{\mathrm{IO}} = 32$ bits. In the power-on schemes, data readout cycles are necessary in addition to initialization of the storage values in an SRAM. In contrast, extra data write cycles are required for the L/L writing scheme.

Figure 29.19 shows the generation time when the number of fingerprint lengths is changed. The L/L writing scheme requires the longest generation time. Generation time of 256-bit length fingerprints in power-on 1, L/L writing, and power-on 2 respectively become 90 ns, 130 ns, and 110 ns. Furthermore, if the larger number of bits in fingerprint is necessary to increase uniqueness and reliability, then the L/L writing scheme requires a longer period because of the extra data writing cycles.

In this section, we compared three SRAM-based PUFs, power-on with and without divided power control and L/L writing schemes, using measurement results

Fig. 29.19 Estimated generation time depending on the bit length of the chip-ID (finger print)



obtained with test chips fabricated using 45-nm CMOS bulk technology. Theoretical values of uniqueness are obtainable in these three schemes. In contrast, results show that higher reliability against variation of temperature and voltage conditions are achieved using the power-on scheme by which the divided power control realizes higher tolerance against variation of the temperature and voltage conditions.

29.4 Summary

Chip-ID generation schemes using an SRAM-based PUF for secure system LSIs are demonstrated. An SRAM-based PUF using the extracted failure bit addresses are presented first. The stability of chip-ID was improved by multiple ID generation scheme with memory BIST. Then, three types of SRAM-based PUFs were assessed from the viewpoints of uniqueness and reliability. From the measurement results obtained with test chips fabricated using 45-nm CMOS bulk technology, theoretical values of uniqueness were obtained in these schemes. In contrast, we found that the SRAM-based PUF using the divided-power-on scheme achieved highest reliability against variation of temperature and voltage conditions. It is feasible for practical use of chip-ID generation in secure system LSI, achieving high dependability against tampering and high traceability in production control systems.

References

1. K. Lostrom, W.R. Daasch, D. Taylor, IC identification circuit using device mismatch, in *IEEE ISSCC Digest of Technical Papers*, 372–373, Feb 2000
2. Y. Su, J. Holleman, B. Otis, A 1.6 pJ/bit 96% stable chip-ID generating circuit using process variations, in *IEEE ISSCC Digest of Technical Papers*, 406–407, Feb 2007
3. N. Liu, S. Hanson, D. Sylvester, D. Blaauw, OxID: on-chip one-time random ID generation using oxide breakdown, in *Symposium on VLSI Circuits*, 231–232, Jun 2010
4. J. Guajardo, S.S. Kumar, G.J. Schrijen, P. Tuyls, FPGA intrinsic PUFs and their user for IP protection, in *Digest of Technical Papers CHES 2007*. LNCS, vol. 4727/2007 (Springer, Heidelberg, 2007), pp. 63–80
5. H. Fujiwara, M. Yabuuchi, H. Nakano, H. Kawai, K. Nii, K. Arimoto, A chip-ID generating circuit for dependable LSI using random address errors on embedded SRAM and on-chip memory BIST, in *Digest of Technical Papers Symposium on VLSI Circuits,* 76–77, June 2011
6. D. Lim, J.W. Lee, B. Gassend, G.E. Suh, M. van Dijk, S. Devadas, Extracting secret keys from integrated circuits. IEEE Trans. VLSI **13**(10), 1200–1205 (2005)
7. D.E. Holcomb, W.P. Burleson, K. Fu, Power-up SRAM state as an identifying fingerprint and source of true random numbers, IEEE Trans. Comput. **58**(9), 1198–1210 (2009)
8. R. Meas, P. Tuyls, I. Verbauwhede, A soft decision helper data algorithm for SRAM PUFs, in *IEEE International Symposium Information Theory,* 2101–2105, July 2009
9. M. Bhargava, C. Cakir, K. Mai, Reliability enhancement of Bi-stable PUFs in 65nm Bulk CMOS, in *Proceedings of HOST,* 25–30, June 2012
10. S. Okumura, S. Yoshimoto, H. Kawaguchi, M. Yoshimoto, A 128-bit chip identification generating scheme exploiting SRAM bitcells with failure rate of 4.45×10^{-19}, in *Proceedings of European Solid-State Circuits Conference (ESSCIRC),* 527–530, Sep 2011

11. S. Chellappa, A. Day, L.T. Clark, Improved circuits for microchip identification using SRAM mismatch, in *Proceedings of IEEE CICC,* 1–4, Sep 2011
12. H. Fujiwara, M. Yabuuchi, Y. Tsukamoto, H. Nakano, T. Owada, H. Kawai, K. Nii, A stable chip-ID generating physical unclonable function using random address errors in SRAM, in *Proceedings of IEEE SoC Conference,* 143–147, Sep 2012
13. M. Bhargava, C. Cakir, K. Mai, Comparison of Bi-stable and delay-based physical unclonable functions from measurements in 65 nm bulk CMOS, in *Proceedings of IEEE CICC,* 1–4, Sep 2012
14. M. Yabuuchi, K. Nii, Y. Tsukamoto, S. Ohbayashi, S. Imaoka, H. Makino, Y. Yamagami, S. lshikura, T. Terano, T. Oashi, K. Hashimoto, A. Sebe, G. Okazaki, K. Satomi, H. Akamatsu, H. Shinohara, A 45nm low-standby-power embedded SRAM with improved immunity against process and temperature variations, in *IEEE ISSCC Digest of Technical Papers*, 326–327, 606, Feb 2007
15. J. Hashimoto, Finger vein authentication technology and its future, in *Symposium on VLSI Circuits Digest of Technical Papers,* 5–8, June 2006

Index

S. Asai (ed.), *VLSI Design and Test for Systems Dependability*,
https://doi.org/10.1007/978-4-431-56594-9