Lecture Notes in Electrical Engineering 455

Yang Xu
Feng Gao
Weihua Chen
Zheming Liu
Pengfei Gu *Editors*

Nuclear Power Plants: Innovative Technologies for Instrumentation and Control Systems

The Second International Symposium on Software Reliability, Industrial Safety, Cyber Security and Physical Protection of Nuclear Power Plant

Springer

Lecture Notes in Electrical Engineering

Volume 455

About this Series

"Lecture Notes in Electrical Engineering (LNEE)" is a book series which reports the latest research and developments in Electrical Engineering, namely:

- Communication, Networks, and Information Theory
- Computer Engineering
- Signal, Image, Speech and Information Processing
- Circuits and Systems
- Bioengineering

LNEE publishes authored monographs and contributed volumes which present cutting edge research information as well as new perspectives on classical fields, while maintaining Springer's high standards of academic excellence. Also considered for publication are lecture materials, proceedings, and other related materials of exceptionally high quality and interest. The subject matter should be original and timely, reporting the latest research and developments in all areas of electrical engineering.

The audience for the books in LNEE consists of advanced level students, researchers, and industry professionals working at the forefront of their fields. Much like Springer's other Lecture Notes series, LNEE will be distributed through Springer's print and electronic publishing channels.

More information about this series at http://www.springer.com/series/7818

Yang Xu · Feng Gao · Weihua Chen
Zheming Liu · Pengfei Gu
Editors

Nuclear Power Plants: Innovative Technologies for Instrumentation and Control Systems

The Second International Symposium on Software Reliability, Industrial Safety, Cyber Security and Physical Protection of Nuclear Power Plant

Springer

Editors

Yang Xu
Department of Engineering Physics
Tsinghua University
Beijing
China

Zheming Liu
Product Information Committee
of China Instrument and Control Society
Beijing
China

Feng Gao
China Nuclear Power Design Co., Ltd.
Shenzhen, Guangdong
China

Pengfei Gu
China Nuclear Power Design Co., Ltd.
Shenzhen, Guangdong
China

Weihua Chen
China Nuclear Power Design Co., Ltd.
Shenzhen, Guangdong
China

ISSN 1876-1100 ISSN 1876-1119 (electronic)
Lecture Notes in Electrical Engineering
ISBN 978-981-10-7415-8 ISBN 978-981-10-7416-5 (eBook)
https://doi.org/10.1007/978-981-10-7416-5

Library of Congress Control Number: 2017959626

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer Nature Singapore Pte Ltd.
The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

Preface

The Second International Symposium on Software Reliability, Industrial Safety, Cyber Security and Physical Protection of Nuclear Power Plant (ISNPP) was successfully held in Chengdu, China, from August 23 to 25, 2017.

We are very pleased to see that since last year's symposium, the academic exchange has been promoted among the participants on every aspects of nuclear power plants' instrumentation and control system. This symposium has become an effective platform for nuclear power builders, regulators, research institutions, and manufacturers. At the same time, a number of outstanding independent research results and products were implemented, such as the speed monitoring device for 1E-class main pump, the verification and validation for security level and the commercial grade software. In fact, many issues discussed in the symposium provide a lot of important reference and strong support for the related work of nuclear power plant.

120 researchers, experts, and students from 29 units attended this symposium, including Tsinghua University, the Ministry of Environmental Protection, China Nuclear Society, and the China General Nuclear Power Group. We received a total of 76 papers; after anonymous peer review and expert selection, 30 outstanding papers were finally recommended to LNEE published, including 9 remarked excellent papers. We hope these papers could also provide beneficial help for the entire instrumentation and control system industry.

On the occasion of the publication of these papers, we would like to thank the organizers of the symposium for providing a good platform for the majority of nuclear power practitioners, also very grateful thanks to the experts and scholars who provide review and guidance for the paper. Finally, we extend appreciation to the authors of the relevant papers, and it is their constant study and efforts to the sophisticated technology that makes it possible to publish this volume of papers successfully.

Organization

Editor and Organizing Committee

Xu Yang	Department of Engineering Physics, Tsinghua University Beijing, China
Gao Feng	China Nuclear Power Design Co., Ltd., China
Chen Weihua	China Nuclear Power Design Co., Ltd., China
Liu Zheming	Product Information Committee of China Instrument and Control Society, China
Gu Pengfei	China Nuclear Power Design Co., Ltd., China

Executive Committee

Chen Yanfeng	Product Information Committee of China Instrument and Control Society, China
Yu Yuzhou	Product Information Committee of China Instrument and Control Society, China

Contents

A Design of High Efficient Multipoint Communication Systems in Nuclear Safety Digital Control Systems

Guo-Jin Jiang, Le Li(✉), Gui-Lian Shi, and Yong Zhao

China Techenergy Co., Ltd., 5 Yongfeng Road, Haidian District, Beijing 100094, China
lile3@cgnpc.com.cn

Abstract. As a part of a communication system in a safety Digital Control System (DCS) applied in a nuclear power plant, multipoint communication network mostly influences the information obtained by operator and inter-stations correctly. Traditional communication systems where some special features, such as reliability, safety, real-time, certainty, independent etc. are not strictly required are various illustrated, However, how to implement a communication system in a safety DCS is rarely stated in current research. In this paper, safety multipoint communication systems are discussed, which also analyses requirement of a safety network. Furthermore, a method is proposed where FPGAs are employed to implement nuclear safety multipoint networks with high efficiency in this paper. Finally, a positive conclusion is also delivered after experimental results being given.

Keywords: DCS · Multipoint network · Safety · FPGA

1 Introduction

Since the first civil Nuclear Power Plant (NPP) in the world was built in 1950 s, the Instrument and Control (I&C) technology applied in NPPs has been developed though three generations. Digital I&C systems, also known as Digital Control Systems (DCS), have been increasingly utilized in NPPs to replace the system implemented by analogue circuits, after the second-generation technology was applied (Chen 2013). As monitoring and controlling the whole operation status of devices in NPPs, a DCS plays a more and more important role in ensuring the safe, reliable, stable and economical operation of nuclear power plant.

As an important component, a communication system is used to exchange data and transmit parameter in a safety DCS, which contributes to operators achieving to perform a variety of control operations and monitoring the real-time status of a power plant system. In other words, communication systems in a safety DCS take responsibility for reporting status and parameter of system operation and releasing control instructions, which requires great quality of reliability, safety, real-time and certainty. Traditional communication systems where some special features, such as reliability, safety, real-time, certainty, impendency etc. are not strictly required are various illustrated. In this case, a new solution to improve efficiency for communication network is proposed, which achieves the attribute of a safety multipoint communication network applied in

Y. Xu et al. (eds.), *Nuclear Power Plants: Innovative Technologies for Instrumentation and Control Systems*, Lecture Notes in Electrical Engineering 455,
https://doi.org/10.1007/978-981-10-7416-5_1

NPPs. Furthermore, the new system is based on FPGA technologies where complex logics are executed in parallel to promote higher processing speed contributing to high efficiency. The new designed system is currently verified in FirmSys, the first DCS with safety class 1E produced by China with proprietary intellectual property.

In this paper, the architecture of a safety communication system is firstly introduced and the requirement of a safety multipoint communication system is discussed in Sect. 2. Furthermore, it illustrates how to implement a safety multipoint communication system and it also shows the FPGA-based system in Sect. 3, followed by the verification of the FPGA-based system described in Sect. 4. Finally, a conclusion is given in the Sect. 5.

2 Requirement of a Safety Multipoint Communication System

2.1 Architecture of a Safety Communication System

A typical communication system of a nuclear safety DCS called the FirmSys is shown in Fig. 1 where point to point and multipoint network are both illustrated. As shown, the point to point network is used to transfer system operation parameters for reactor trip

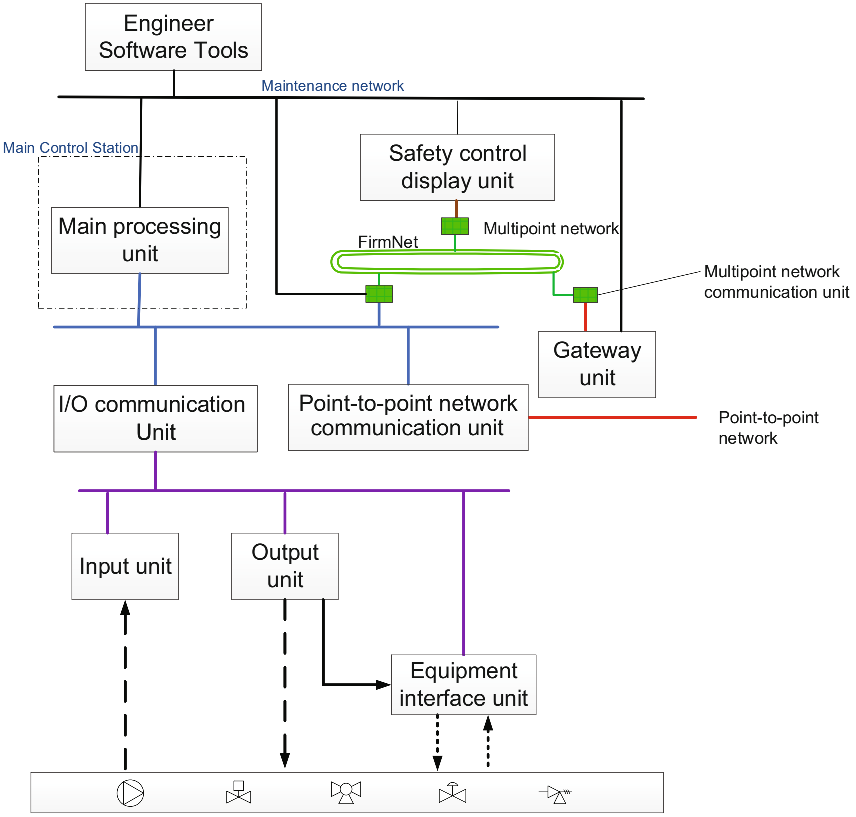


Fig. 1. Architecture of a safety communication system

systems between different main processing units. Differed from the point to point network, the multipoint network in a safety DCS system is employed to transfer a large amount of data among different main control stations and maintenance networks. In addition, devices with specific functions, such as safety control display units and gateway units, are also connected using multipoint networks. In this case, the multipoint network is also an important component of a safety communication system. In the next few sections, the requirement of the multipoint network and how to implement a safety multipoint network will be discussed.

2.2 Requirement of Safety Multipoint Communication

Design of a safety system applied in NPPs should meet the related standards and regulations, such as IEC 61513, IEEE 7-4.3.2, NRC ISG-04, and etc. From the relevant standards and regulations, the requirement how to design a safety multipoint communication system should be considered, which are listed as below.

2.2.1 Reliability

According to IEEE 7-4.3.2, the reliability is defined as the ability to achieve the communication function without failure in normal and abnormal conditions in a certain period of time (IEEE 2010). In addition, the protocol of the nuclear safety communication system should keep simple without useless protocol level and useless service. This is due to the simple protocol contributes to decreasing probability of failure. Furthermore, the function of data integrity check and redundancy should be provided to enhance the reliability of the network.

2.2.2 Safety

Safety refers to the ability of a communication system to prevent a reactor from being in a potentially dangerous or unstable state (Ma et al. 2003). In other words, the communication system shall not endanger the safety function of the reactor control and protection system in any conditions. In this case, the function of self-check and self-monitoring should be employed by safety communication systems. The system should be alarmed in time when the event of equipment failure, communication function loss or communication performance attenuation happens. Furthermore, tit should take isolation, bypass and other measures for the communication equipment, when serious failure occurs.

2.2.3 Real-Time

Real-time means the ability of a communication system to transmit the process data or operational instructions to the destination for a limited amount of time (IAEA 2011). The nuclear safety communication system should provide sufficient performance to ensure that any data sent from any communication node can be received within a certain time limit by the intended target node.

2.2.4 Certainty

Certainty indicates that the speed, delay, throughput, load, and period of data updating should be calculated accurately when the communication being designed or application being configured. The nuclear safety communication system should be state-based communication, which means fixed data sets should be sent in fixed time intervals, regardless of whether the data has been changed. In addition, the length of messages should be fixed and the composition of the message should be unchanged.

2.2.5 Independency

It is required by IEEE Std 603-1998 that equipment of nuclear safety communication systems should meet the requirements of physical separation, electrical isolation, communication isolation and functional independence (IEEE 1998). Furthermore, when transferring data between communication systems with different safety level, the data from the system with high safety level could be sent to the system with low safety level. However, it is not allowed transferring data from the system with low safety level to the system with high safety level, which means that the data from non-safety system should not be sent to safety system.

3 Design of a High Efficient Safety Multipoint Network

3.1 Design of a Safety Multipoint Network

A safety multipoint network could be designed following the requirement discussed in the last section. According to the requirement, how to achieve a safety multipoint network will be presented in this section.

3.1.1 The Topology of the Safety Multipoint Network

A safety multipoint network should transmit data using broadcasting mode due to certainty mentioned in Sect. 2.2.4. It also achieves the property of real-time stated in Sect. 2.2.3 because the transmitted data only depends on the send node. In this case, the topology of the safety multipoint network should be a ring network, which could be implemented by FPGA technologies efficiently. In addition, the network should achieve the function of redundancy for achieving reliability. Thus, all communication equipment should be connected with two reverse and redundant communication link to constitute a double ring topology where the same data will be transmitted to both clockwise and counter-clockwise direction. The topology of the safety multipoint network is shown in Fig. 2.

In this topology, the ring where data is transmitted clockwise is defined as Ring 0, and the other ring is defined as Ring 1. Each communication node sends its data to other nodes through both Ring 0 and Ring 1. Furthermore, each node could receive two sets of the same data from any other node through both clockwise and counter-clockwise ring. In this case, the ring network could work correctly even if one of two rings is failure.

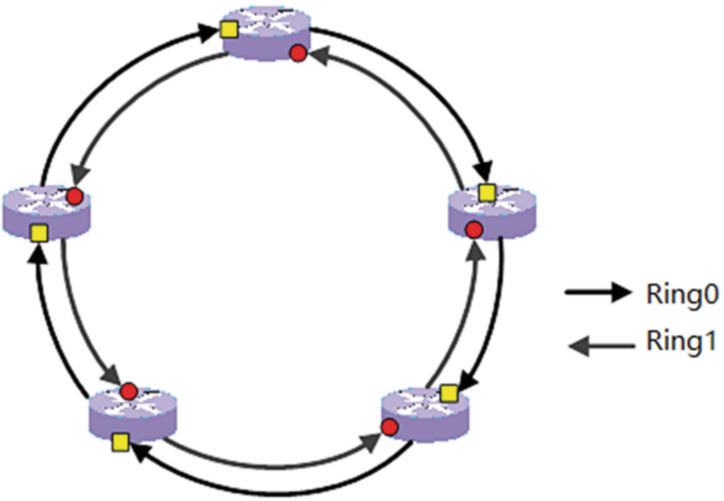


Fig. 2. The topology of the safety multipoint network

3.1.2 The Simple Protocol

As discussed in Sect. 2.2.1, the protocol of the safety multipoint network should be designed simply, which contributes to the reliability of the system. Based on the feature of safety communication that the data transmission is completely controlled by the sender without any handshake mechanism, the protocol of the safety multipoint network could be simplified from Open System Interconnect (OSI) model and employs physical Layer, data-link layer and application layer only, which is shown in Fig. 3.

As shown in Fig. 3, the physical layer provides an electrical, mechanical, and procedural interface to the transmission medium transmitting raw bits, which is as same as the one defined in IEEE 802.3. The data-link layer contains three sub-layers that are Media Address Control (MAC) data channel, MAC control layer and data mapping layer. The MAC data channel provides the function of data sending and receiving. The MAC control sublayer is responsible for connecting data mapping area and MAC data channel. The main functions include data processing, data analysis, ring selection, data mapping area access control, data frame scheduling management and fault handling. The data mapping sub-layer manages and maintains data in the data map area, handles access conflicts and ensures data integrity. The application layer provides services for the application to access the network.

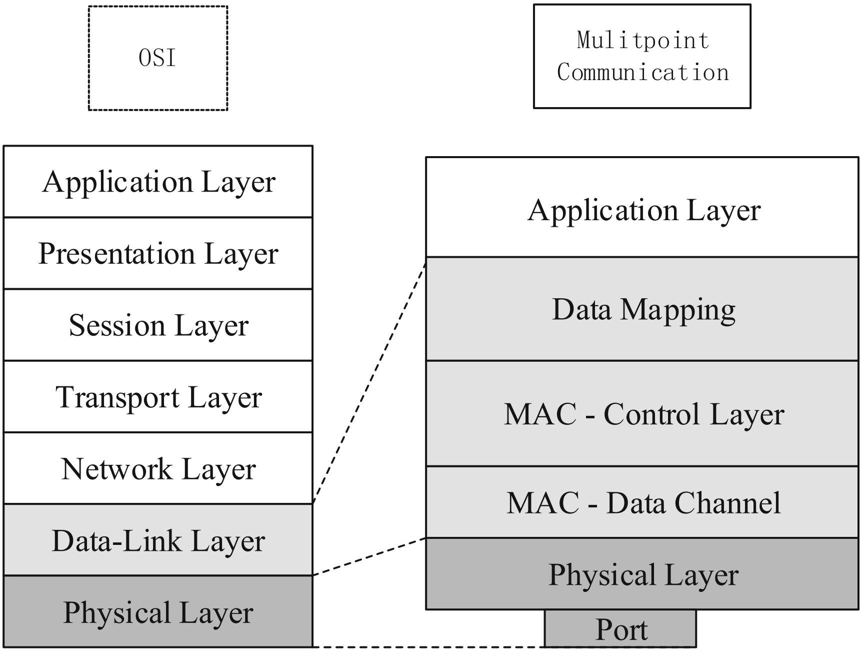


Fig. 3. The protocol of the safety multipoint network

3.1.3 Model of Data Transmission

Due to the topology of the ring network and the simply protocol mentioned above, the model of data transmission could be defined, which is illustrated in Fig. 4. The local data produced by the application layer is stored in a memory in data mapping sublayer, followed by data process in MAC control sublayer. After framing in MAC data channel sublayer, the data is sent to other nodes though the physical layer by two directions. Other stations stored the data to local memory for application invoking after received

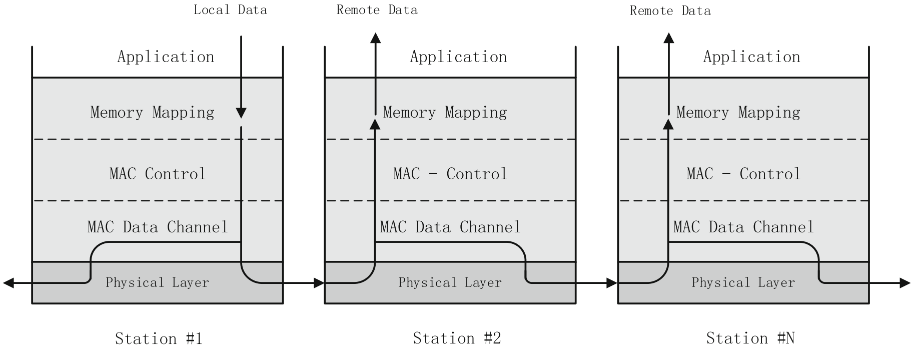


Fig. 4. Path of data transmission

though physical layer and checked by MAC-related sublayer. The received data is also transferred to other stations though MAC data channel processing.

3.2 Implementation of a Safety Multipoint Network on FPGAs

Since invented in 1985, Field Programmable Gate Arrays (FPGAs) have been utilized in applications to replace computer-based system depending on its high processing speed and ability of parallel processing (York 1993). In the past few decades, FPGAs are increasingly employed to achieve some specific functions in various field of industries where high safety and reliability are required, such as automobiles, aircraft control systems, aerospace mission-critical applications, and etc. In recent years, FPGA-based I&Cs were growingly applied for safety systems in NPPs for obtaining a high efficient system. For instance, a trip channel logic implemented by FPGAs was applied to Shutdown System No.1 in CANDU NPP in Canada (She and Jiang 2011). In addition, Radiy implements more than 50 systems based on FPGA technologies in four NPPs in Canada and one NPP in Bulgaria, which are reactor trip systems, engineering safety features actuation systems, reactor power control and limitation system and rod control systems (Bakhmach et al. 2009; Karchenko 2010).

It is proved that FPGA-based communication systems could promote to throughput and efficiency in some researches (Vanderbauwhede et al. 2012). In this case, FPGA technologies are employed when a safety multipoint network was achieved on FirmSys.

3.2.1 Implementation of the Safety Multipoint Network on FPGAs

The simple block diagram of the FPGA-based safety multipoint network is shown in Fig. 5 where two FPGA-based communication boards are connected and transfer data with each other. As shown in the figure, a Radom Access Memory (RAM) is employed to store the data produced by application module or received from other communication nodes. In this case, it is said that the RAM is the core component of each the multipoint network node due to all information of every node stored in it. The network communication process is actually the updating process of each station memory map area. In this process, each communication node updates the data received from other nodes in the corresponding data mapping area. Owning to FPGA technologies applied, the progress of sending and receiving data with ports and the process of writing and reading data with RAMs could be proceeded at the same time, which contributes to achieving a high throughput and efficiency network (Zhang et al. 2010).

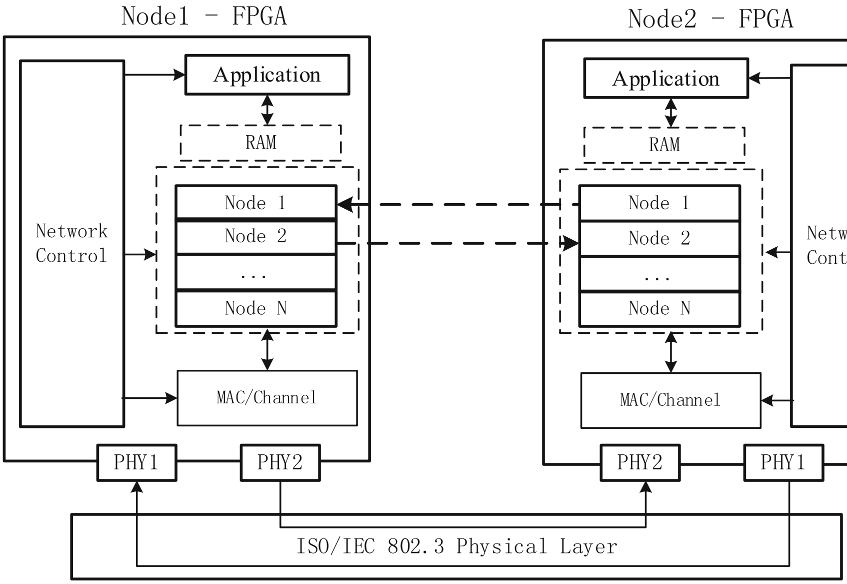


Fig. 5. Block diagram of FPGA-based system

3.2.2 Data Frame Designed for FPGA

A new type of safe and reliable communication frame is designed for the safety ring network which is extremely suitable for being implemented in FPGA contributing to data integrity check. In common communication protocol, the protocol only provides only one method of data checked, Cyclic Redundancy Check (CRC) or checksum (Jiang and Kan 2013). For FPGA-based systems where all logic elements and registers are parallel processing, the Error Correction Check (ECC) and CRC could be jointly applied. ECC is used to check the head of frame where the amount of data is not large and error correction could be applied. In addition, CRC is used to check a large amount of data followed the head. The structure of the frame is shown in Fig. 6.

Frame Head	ECC	Data	CRC

Fig. 6. Structure of the design frame

An ECC is a process of adding redundant data, or parity data, to a message, such that it can be recovered by a receiver even when a number of errors were introduced, either during the process of transmission, or on storage (Layton 2014). Since the receiver does not have to ask the sender for retransmission of the data, an ECC promotes the efficiency of communications.

3.2.3 Isolation

For the independent required by design standards, isolation should be applied in the safety ring network. A method for achieving isolation is shown in Fig. 7. In isolation system, three types of isolation are introduced in Sect. 2.2.5. The sending and receiving side are connected by optical fibber which enhances physical separation and electrical isolation. In addition, a dual-port RAM is implemented in the receiving side for data exchange between the receiving port and the FPGA contributing to communication isolation.

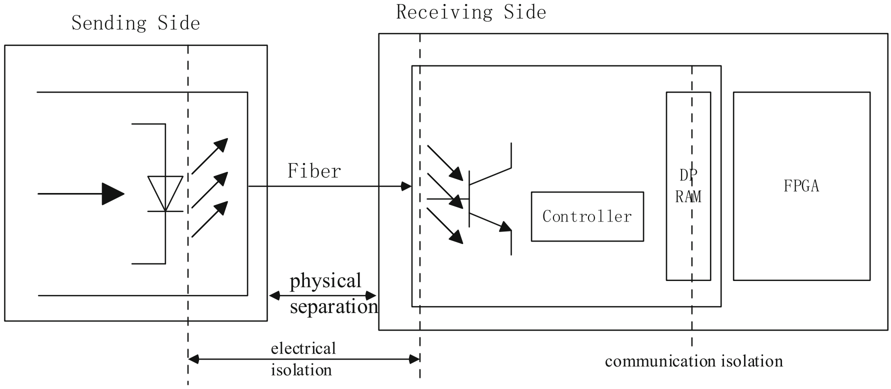


Fig. 7. Isolation system

4 Verification and Analysis

4.1 Simulation

Following the design regulation of FPGAs and NUREG-CR-7006 (U.S NRC 2009), behavioral simulation should be taken after a FPGA design. The block diagram of functional simulation is shown in Fig. 8. There are a signal generator and a signal generator implemented in the testbench. A group of data generated from signal generator is sent

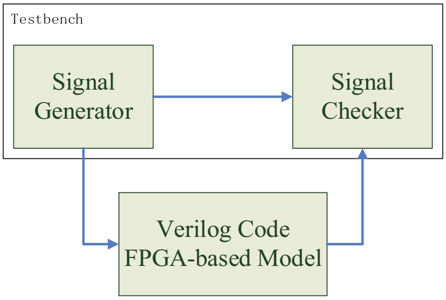


Fig. 8. Simulation model

to FPGA-base module and the signal checker. The output data is verified by the original data in the signal checker to judge whether the output is correct.

4.2 Verification Model

A verification model establishes based on a PC monitor, which is shown in Fig. 9. The interface of the model provides a sender to the node 1 and a receiver to the node 2, which allows the designed product to be validated in a PC-based monitor. The operational condition of FPGAs and data in FPGA could be monitored by logic analyser.

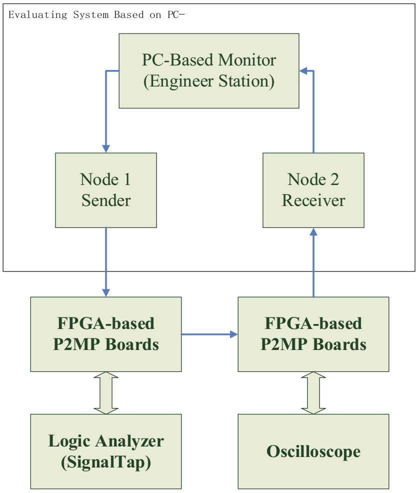

Evaluating System Based on PC-
PC-Based Monitor (Engineer Station)
Node 1 Sender
Node 2 Receiver
FPGA-based P2MP Boards
FPGA-based P2MP Boards
Logic Analyzer (SignalTap)
Oscilloscope

Fig. 9. Verification model

4.3 Analysis of Result

To obtain the signal of data in the sending and receiving ports, test points are applied in the cache of sending and receiving side, which could be monitored by SignalTap, an on-chip logic analyser produced by Altera. A group of register value monitored by SignalTap is shown in Figs. 10 and 11. As shown in the figure, the received data is as same as the sent data, which means the transferred data between two nodes are correct.

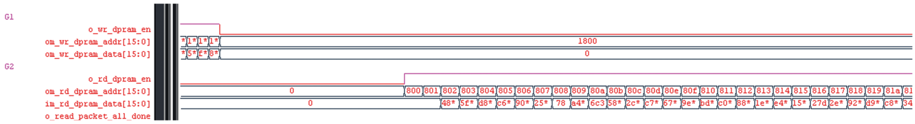

G1
o_wr_dpram_en
om_wr_dpram_addr[15:0]
om_wr_dpram_data[15:0]
G2
o_rd_dpram_en
om_rd_dpram_addr[15:0]
im_rd_dpram_data[15:0]
o_read_packet_all_done
1800
0
0
800 801 802 803 804 805 806 807 808 809 80a 80b 80c 80d 80e 80f 810 811 812 813 814 815 816 817 818 819 81a 81
0
48* 5f* d8* c6* 90* 25* 78 a4* 6c3 58* 2c* c7* 67* 9e* bd* c0* 88* 1e* e4* 15* 27d 2e* 92* d9* c8* 34

Fig. 10. The sent data

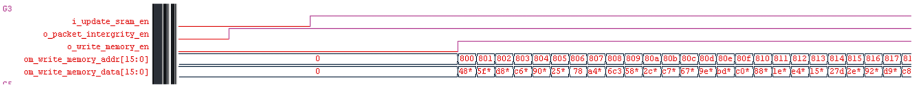

G3
i_update_sram_en
o_packet_intergrity_en
o_write_memory_en
om_write_memory_addr[15:0]
om_write_memory_data[15:0]
0
0
800 801 802 803 804 805 806 807 808 809 80a 80b 80c 80d 80e 80f 810 811 812 813 814 815 816 817 81
48* 5f* d8* c6* 90* 25* 78 a4* 6c3 58* 2c* c7* 67* 9e* bd* c0* 88* 1e* e4* 15* 27d 2e* 92* d9* c8

Fig. 11. The received data

The data transmission period for 48 communication nodes is tested, where the length of every data pocket is 2096 bytes. The result shown in Fig. 12 illustrates that the data transmission period for 48 nodes is around 5.5 ms. The new designed system is faster than the former CPU-based system where the data transmission period for 48 nodes is around 41.5 ms by eight times. In this case, the FPGA-based system contributes to high efficiency in multipoint communication systems in a DCS.

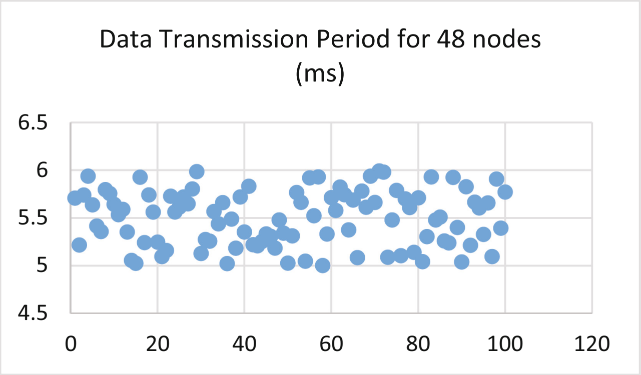


Fig. 12. Experimental result of data transmission period

5 Conclusion

In this paper, the architecture of a nuclear safety communication system is presented and the requirement of a safety multipoint communication network is also discussed. In addition, the method of implementing a FPGA-based multipoint network has been described and the verification is also delivered. In conclusion, it is provided that a new designed redundant ring network is proposed in nuclear safety communication systems where FPGA-based technologies achieve high efficiency.

The FPGA-based multipoint communication network is proved to be applied in a safety DCS in NPPs. Further research will focus on the advantage of FPGA technologies applied in multipoint communication systems and whether the safety multipoint communication could be implemented on other platforms, instead of FPGAs, to achieve higher efficiency.

References

Bakhmach, E., Siora, O., Tokarev, V., et al.: FPGA - based technology and systems for I&C of existing and advanced reactors. IAEA, Vienna, Austria (2009)

Chen, L.: Basic design criteria of safety DCS system network in nuclear power plant. Autom. Panorama **1**, 78–81 (2013)

IAEA: Implementing Digital Instrumentation and Control Systems in the Modernization of Nuclear Power Plants (IAEA NP-T-1.4). IAEA Nuclear Energy Series (2011)

IEEE: IEEE Std 603-1998, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations (1998)

IEEE: IEEE std 7-4.3.2, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations (2010)

Jiang, X., Kan, R.: Research on nuclear safety-level communication technology based on FPGA technology. Ind. Control Comput. **26**(10), 84–85 (2013)

Karchenko, V.S.: Diversity-oriented FPGA-based NPP I&C systems: Safety assessment, development, implementation. In: 18th International Conference on Nuclear Engineering, vol. 1, pp. 755–764 (2010)

Layton, J.: Error detection and correction. Linux Mag. **128**, 4 (2014)

Ma, G.Q., Du, Q.R., Shi, G.L., et al.: Research on communication protocol technology of advanced nuclear safety instrumentation and control systems. Instumentation User **20**(5), 28–31 (2003)

She, J., Jiang, J.: On the speed of response of an FPGA-based shutdown system in CANDU nuclear. Nucl. Eng. Des. **241**(6), 2280–2287 (2011)

US (2009): NRC Review Guidelines for Field-Programmable Gate Arrays in Nuclear Power Plant Safety Systems. Washington, DC, USA (2009)

Vanderbauwhede, W., Chalamalasetti, S., Margala, M.: Throughput analysis for a high-performance FPGA-accelerated real-time search application. Int. J. Reconfigurable Comput. **1**, 1–16 (2012). Special issue on High-Performance Reconfigurable Computing

York, T.A.: Survey of field programmable logic devices. Microprocess. Microsyst. **17**(93), 371–381 (1993)

Zhang, A., Wang, W., Hu, X., et al.: Design and implementation of FPGA based communication architecture for control system. J. Zhejiang Univ. (Eng. Sci. Ed.) **44**(4), 659–664 (2010)

A Study and Application About Software V&V Requirement Management Scheme in Digital RPS

Wang Xi[(✉)], Peng-Fei Gu, Wei Liu, and Wei-Hua Chen

State Key Laboratory of Nuclear Power Safety Monitoring Technology and Equipment,
Laboratory of I&C Equipment Qualification and Software V&V,
China Nuclear Power Design Co., Ltd., Shenzhen, China
wang.xi2@cgnpc.com.cn

Abstract. V&V (Verification and Validation) is an important way to assure the safety and reliability of software. Requirement management plays a critical role through the whole process of V&V. Based on the practice on Generation II + pressurized water reactor named CPR1000, this paper establishes requirement management scheme for digital RPS (Reactor Protection System) software V&V, the scheme is applied in typical DCS (Digital Control System) V&V project of nuclear power plant, and enhances the trace efficiency. The successful engineering practice provides efficient requirement management reference for succeed nuclear DCS devices development and test projects.

Keywords: NPP · DCS · RPS · V&V · Requirement management

1 Introduction

The Reactor Protection System (RPS) is an important part of the instrument control system [1], including the Reactor Trip (RT) and Engineering Safety Feature (ESF) actuation protection devices, which is the core system to ensure the safe and reliable operation of the Nuclear Power Plant (NPP). Compared with the analog instrument control system, the digital instrumentation control system (DCS) introduce the software in nuclear safety level. The DCS obtained higher control precision, integration, easy expansion and data transmission reliability. Software and system defects may cause system failure, furthermore, resulting in serious consequences. In accordance with the requirement of the nuclear safety regulations HAF102 [3], V&V [1, 2] is a necessary step to ensure the quality of the software. The safety and reliability of the software, which is applied in nuclear power station safety functions, should be demonstrated and confirmed by V&V process [4].

Requirement management is a systematic approach to acquiring, organizing and documenting system requirement, as well as a process that enables customers and project teams to reach and align with changing system requirement. Requirement management is also an important part for QC (quality control [5]) in development of the entire nuclear power project and V&V. Requirement management includes requirement change management,

Y. Xu et al. (eds.), *Nuclear Power Plants: Innovative Technologies for Instrumentation and Control Systems*, Lecture Notes in Electrical Engineering 455,
https://doi.org/10.1007/978-981-10-7416-5_2

requirement version management and requirement tracing management, all of them providing a reusable and traceable evidence for software reliability verification [6].

Based on the practice of CPR1000 project, this paper constructs requirement management model and file tracking network for digital reactor protection system software V&V, the model applies on typical products of localization nuclear power instrumentation control equipment.

2 V&V Model for RPS

According to IEC 60880 Standard for software used in nuclear power plant safety systems [7] and IEEE Std. 1012 Standard for Software Verification and Validation [8], this paper construct the V&V model relies on the V&V project combined with the actual situation of RPS software requirements and designs process in NPP.

As shown in Fig. 1, according to the design and implementation of system requirement and software requirement in reactor protection system, the V&V model divides the V&V process into 5 stages, including Concept V&V, Requirement V&V, Design V&V, Implementation V&V, and Test V&V. Each stage verifies its input and output files. The Test V&V including integration test, which validate the software requirement, and acceptance test, which validate the system requirements.

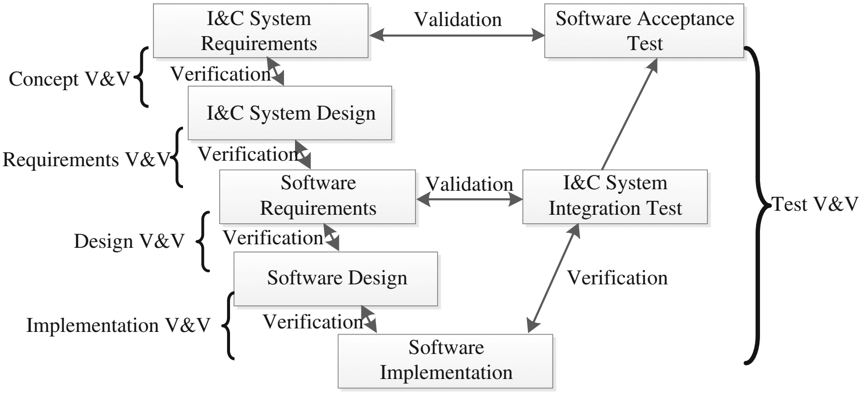


Fig. 1. V&V model for digital RPS

3 V&V Requirement Management Scheme for RPS

3.1 Files Architecture

The basic files architecture of RPS system design and development process is shown in Fig. 2.

- In the concept stage, the “RPS system requirement specification” and “logic diagram and analog diagram” are proposed by the designer. The developer will refine the system requirement into the “functional design specification” according to the design document.

- In the requirement stage, the software-related part of the functional design specification can be extracted as “software requirement specification”, the “functional diagram” is established in according to the software function requirement and “logic/analog diagram”.
- In the design stage, the developer makes the function diagram into software configuration diagram by special software tool;
- In the implementation stage, the configuration diagram of the specific algorithm block is achieved by the code, and get executable function block;
- In the integration test stage, the integrated system should be tested.

Therefore, the RPS files architecture has the dependencies among various stages, as well as the characteristics of the design documents and diagrams, on which need to be focused in the requirement management.

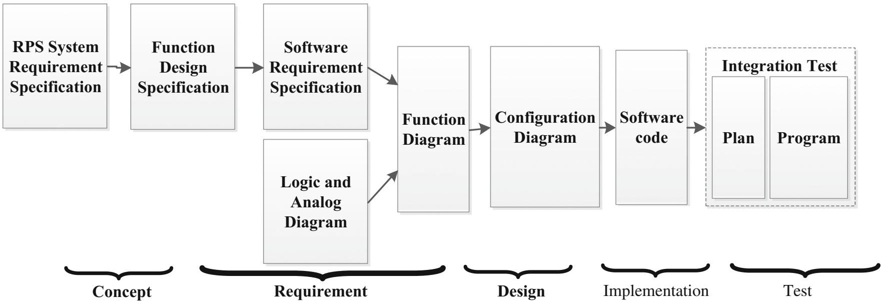


Fig. 2. RPS files architecture

3.2 Requirement Management Model

In according to the relationships of RPS files, this paper constructs the requirement management model from three aspects: requirement version management, requirement change management and requirement tracking management. Requirement tracking is the main content of requirement management. As shown in Fig. 3, the model establishes a baseline for each file to control the version, performs requirement tracking at each stage. When the requirement change, the baseline should be updated, the requirement management process for the update should be repeated, and ensure that the requirement change in upstream file has been re-implemented in downstream file with continued consistency and traceability.

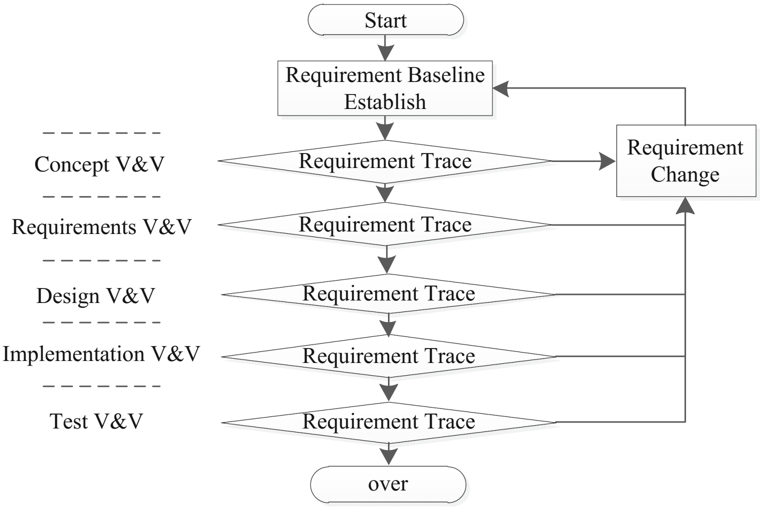


Fig. 3. V&V model for digital RPS

3.3 Requirement Management

In according to RPS system document system characteristics and requirement management model, this paper constructs the requirement management scheme for RPS system software V&V. As shown in Fig. 4, this scheme combines the actual situation of CPR1000 project to build the most complete requirement management.

- The concept stage is the source of requirement tracking, the correctness of requirement analysis is related to the whole project design. In the actual project, the contract annex is the supplement for RPS requirement specification. In this scheme, both the contract annex and the RPS requirement specification are made an upstream document in concept stage, to improve the quality of project requirement entry from the source.
- The file of the downstream stage of the concept stage includes the "Overall Design Specification" and its "Subsystem Design file" and "Special Function Design Specification". This scheme adds the forward and backward tracking from "Overall Design Specification" to "Subsystem Design Manual" and "special function design specifications" for their internal file relationship, to further ensure that the functional design specifications to meet the upstream file needs.
- The "Basic I/O List", "Set point Manual" and "Safety Control Display Device (SCID) Database" are also generated at the same time as the "Software Requirement Specification", "Logic/Analog diagram", these three documents describe the details of signal point name, value assignment and equipment relationships in functional diagram. In requirement stage, the internal relationship between the functional diagram and the above three documents is tracked to further ensure the functional design satisfice the requirement.

- In the design stage, this scheme makes "detailed I/O list" and "configuration diagram" together as a management object to ensure the configuration diagram interface to meet the needs.
- In the implementation stage, this paper makes "software code" and "function block user manual" as a management object, on the one hand to verify the configuration diagram function module to meet the requirement, and the other hand to verify the functional unit code design to meet the needs.
- In the testing stage, this scheme use "integration test program", " integration test program", and " integration test results" together as a management object, on the one hand to confirm whether the developer integrated test design can effectively meet the test requirement, on the other hand to verify the integration whether the test results meet the functional requirement.

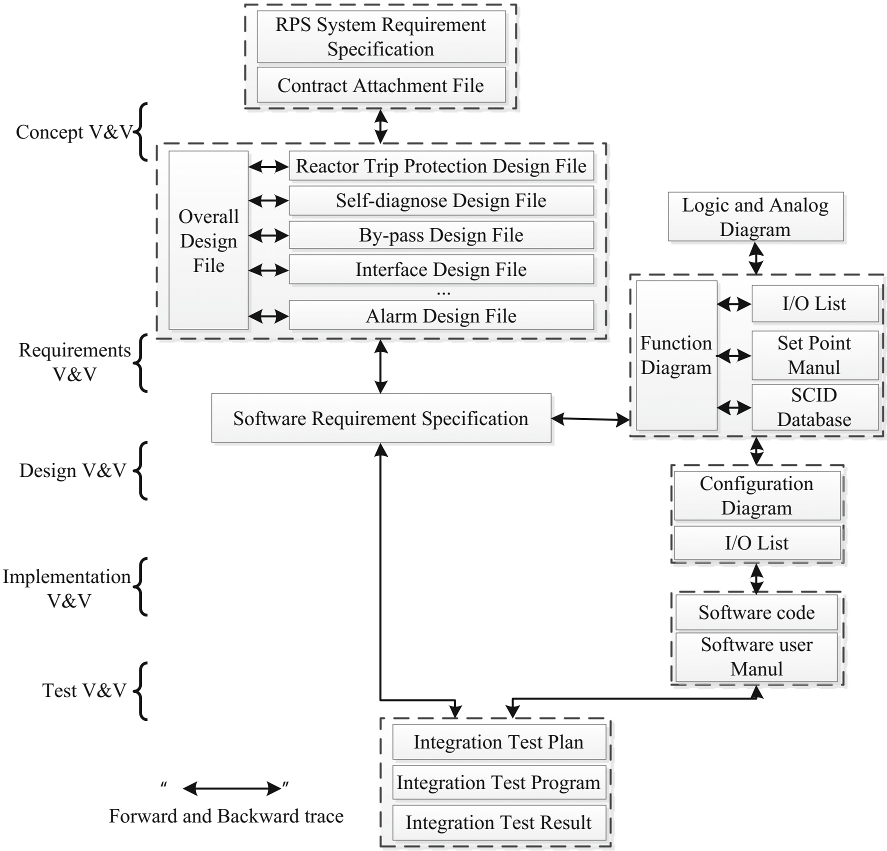


Fig. 4. Digital RPS software V&V requirement management scheme

4 Application Base on DOORS

4.1 Requirement Traceability Link

Requirement tracking is the main content of requirement management, relying on the tracking link, through the tracking chain can be forward or backward tracking to the upstream requirement and downstream implementation [9, 10]. By using the DOORS, which is a requirement management tool to capture, link, track, analyze and manage user requirement information, the partitioning units in upstream and downstream file will be managed first [11], each unit can be used as a "tracking point". As the "tracking point" of the downstream file as the "line element", the "tracking point" of the upstream file "Column element", if there is a traceable relationship between the tracking points of the two files, the link is connected. Link diagram shown in Fig. 5, through the tracking link, you can visually draw the Traceability link point between the two files, what's more, the requirement partitioning units has been managed.

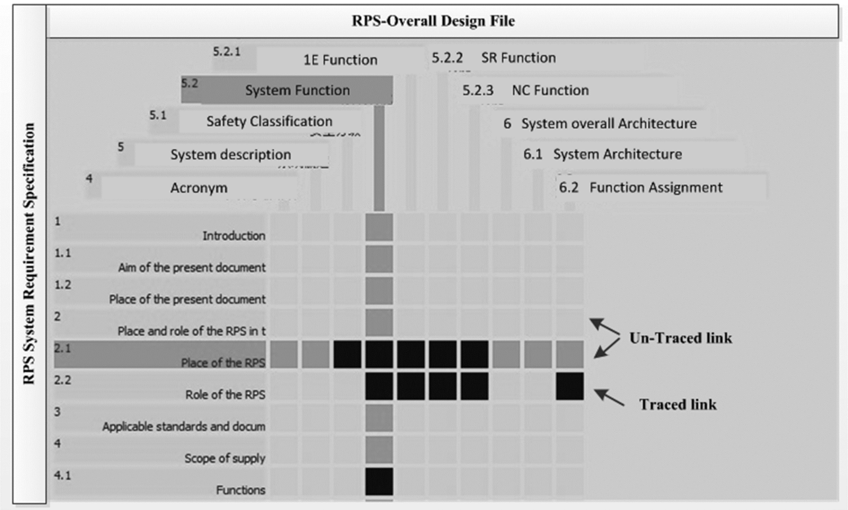
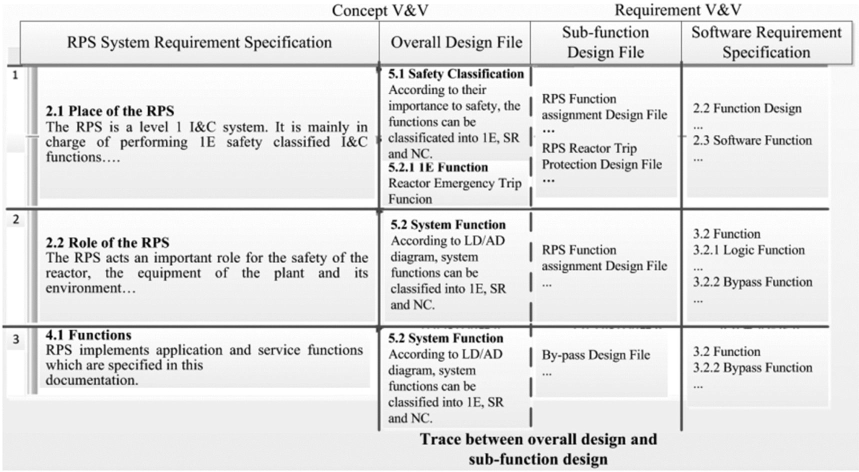


Fig. 5. Requirement Traceability link

4.2 Requirement Traceability Matrix

For the files that have been linked, the Requirement Traceability Matrix (RTM) can be generated from the relationships between "row elements" and "column elements" of the file in each stage. The RTM is shown in Fig. 6, the association between the different files in each stage is presented. The tracking matrix can be used to track the implementation of the upstream requirement at each stage, and the requirement tracking and consistency analysis are carried out quickly.



	Concept V&V		Requirement V&V	
	RPS System Requirement Specification	Overall Design File	Sub-function Design File	Software Requirement Specification
1	**2.1 Place of the RPS** The RPS is a level 1 I&C system. It is mainly in charge of performing 1E safety classified I&C functions….	**5.1 Safety Classification** According to their importance to safety, the functions can be classificated into 1E, SR and NC. **5.2.1 1E Function** Reactor Emergency Trip Funcion	RPS Function assignment Design File … RPS Reactor Trip Protection Design File …	2.2 Function Design … 2.3 Software Function …
2	**2.2 Role of the RPS** The RPS acts an important role for the safety of the reactor, the equipment of the plant and its environment…	**5.2 System Function** According to LD/AD diagram, system functions can be classified into 1E, SR and NC.	RPS Function assignment Design File …	3.2 Function 3.2.1 Logic Function … 3.2.2 Bypass Function …
3	**4.1 Functions** RPS implements application and service functions which are specified in this documentation.	**5.2 System Function** According to LD/AD diagram, system functions can be classified into 1E, SR and NC.	By-pass Design File …	3.2 Function 3.2.2 Bypass Function …

Trace between overall design and sub-function design

Fig. 6. Requirement Traceability Matrix

4.3 Achievement

Based on the DOORS tool, the application of the requirement tracking model, which is proposed in this paper, has been successfully applied in the software V&V of the digital RPS of CPR1000 project, and has achieved good results. During the V&V process, a certain number of important issues have been detected, and contributed to improving the quality of the project.

To evaluate the trace efficiency by using requirement management by DOORS, this paper makes an experiment. The same files are traced by two methods, one searches the target tracking point by people, and the other one by DOORS. We use searching time, which means the time we use to find the tacking point or the track link among several stages, to evaluate the trace efficiency.

As show in Table 1, compared to the manual method, the mean searching time that tracing by DOORS has been reduced by 40%–72.7%, as the stages added, the efficiency that improved more obvious.

Table 1. Trace efficiency experiment result

Searching time	Manual	DOORS
1 stage	≈10 s	≈6 s
2 stages	≈24 s	≈9 s
3 stages	≈37 s	≈12 s
4 stages	≈55 s	≈15 s

5 Conclusions

In this paper, by researching on the files architecture of digital reactor protection system and combining with the engineering practice, a reasonable and feasible requirement management scheme is established. With the application based on DOORS, this scheme effectively improves the tracking efficient, enhance the quality of digital instrument control system software development, provides a useful reference for the requirement management program in nuclear power safety digital instrumentation and control system development and testing.

References

1. Gu, P.F., Xi, W., Chen, W.H., et al.: Evaluation system of software concept V&V about the safety digital I&C system in nuclear power plant. In: International Symposium on Software Reliability, Industrial Safety, Cyber Security and Physical Protection for Nuclear Power Plant, vol. 400, pp. 125–132. Springer, Singapore (2016)
2. Ye, W.P., Tang, J.Z., Chen, W.H.: Software V&V methods for safety digital I&C system of nuclear power plant. At. Energy Sci. Technol. **49**, 378–381 (2015)
3. HAF 102: Safety of Nuclear Power Plant Design Regulations. Doctoral dissertation (2012)
4. Gu, P., Wang, S., Chen, W., et al.: A study about safety I&C system software V&V in nuclear power plant. In: The 24th International Conference on Nuclear Engineering. American Society of Mechanical Engineers, vol. (1), 005 (2016)
5. Chen, W.H., Xi, W., Gu, P.F., et al.: A study about software development QC and QA of the digital RPS in nuclear power plant. In: International Symposium on Software Reliability, Industrial Safety, Cyber Security and Physical Protection for Nuclear Power Plant, vol. 400, pp. 105–112. Springer, Singapore (2016)
6. Ding, Y.X., Gu, P.F., et al.: Study on standard about safety digital I&C system in NPP. Process Autom. Instrum. **36**(11), 61–64 (2015)
7. International Electro Technical Commission: IEC 60880 nuclear power plants-instrumentation and control systems important to safety-software aspects for computer-based systems performing category A functions. International Electro Technical Commission, Switzerland (2006)
8. Software Engineering Standards Committee of the IEEE Computer Society: IEEE 1012 IEEE Standard for Software Verification and Validation. Institute of Electrical and Electronics Engineer, New York (2004)
9. Xiao, W.: An optimized method for software requirement development process using doors. Comput. Appl. Softw. **29**(9), 175–177 (2012)
10. Xia, D.Y., Liu, W.P.: Requirement management on nuclear power plant DCS for development. Instrumentation **22**(2), 63–66 (2015)
11. Lin, S.Q., Guo, X.X., et al.: Software requirement management on human-machine interface (HMI) software for nuclear power plant. Comput. Knowl. Technol. **8**(21), 5097–5099 (2012)

The Software Security Analysis for Digital Instrumentation and Control Systems of NPPs

Hui-Hui Liang(✉), Peng-Fei Gu, Jian-Zhong Tang, and Wei-Hua Chen

State Key Laboratory of Nuclear Power Safety Monitoring Technology and Equipment,
Laboratory of I &C Equipment Qualification and Software V&V,
China Nuclear Power Engineering Co., Ltd., Shenzhen, China
lianghuihui@cgnpc.com.cn

Abstract. Software security relates to the economy and safety of nuclear power plants (NPPs). Cyber security is a hot research topic for NPPs. The standards and regulations have been established for cyber security in NPPs, such as regulatory guide 5.71. Cyber-attack is a threaten that may be happened at any point during the life cycle of the digital instrumentation and control systems. The vulnerabilities of information security can be reduced by physical protection, independent strategies and administrative measures. The security measures only concern with the cyber security for NPPs in commonly. The essence of digital instrumentation and control systems has not been paid enough attention. Software security is the last line of against the attacker. In this paper, the risk of software security has been analysed for the digital instrumentation and control systems in NPPs. The identification and detection measures have been proposed in the paper.

Keywords: Software security · Security analysis · I&C · NPPs

1 Introduction

Software security of digital instrumentation and control (I&C) system relates with the economy and safety for the nuclear power plants (NPPs). The standards and regulations have been built by the plants and regulator. IEC 62654 [1] has provided the activities what the security programme should be contained in the instrumentation and control systems. From IEEE 7.4.3.2-2010 [2], during the NPEC preview of this revision of the standard, the security of safety system software is discussed. Recommendations have been made that a future revision of the standard will address software risks associated with attacks by inside and outside. IEC 60880 [3] is the software standard for systems performing category A functions of instrumentation and control system important to safety in NPPs. Security analysis of designing and security of user access of during development need to be concerned. Software security is also required in the HAD102/16-2004 [4]. The requirements have been described from the following aspect: the safety management, software requirements, and system validation. IEEE 1012-2012 [5], the security analysis is one of the minimum tasks and it should be performed in every verification and validation phase.

Y. Xu et al. (eds.), *Nuclear Power Plants: Innovative Technologies for Instrumentation and Control Systems*, Lecture Notes in Electrical Engineering 455,
https://doi.org/10.1007/978-981-10-7416-5_3

The information security is not only the cyber security. It also includes the software security. The cyber security is a hot research topic for the NPPs. Software security has not been paid enough attention. Cyber-attack is a threat that may be happened at any point during the life cycle of the digital instrumentation and control systems. The security cyber vulnerabilities can be reduced by physical protection, independent strategies and administrative measures. The common security measures only concern with the cyber security for NPPs. Software security is the last line of against the attackers. The software security can enhance the defence capability for the digital instrumentation and control systems. Cyber security can against the external attacks. Software security is that the software can be exactly executed when it is attacked. At the same time, the software should be ensured that it is authorize and lawful used. Software security can be executed in static testing of nuclear safety-critical software [6, 7]. Software security can be tested by the fault injection strategy for digital safety software in Nuclear Power Plant [8]. The security analysis is the basic task for the software V&V in nuclear power plant [9, 10].

This paper is structured as follows. Section 1 is the background. Section 2 describes the risk of software security. Section 3 describes the necessity of software security analysis. The strategies have been proposed in the Sect. 4. Section 5 is conclusions.

2 The Security Risk of Instrumentation and Control Systems

Software security of digital instrumentation and control systems for the NPPs is different from the industrial control systems. They have been shown as Table 1. So the software security of digital instrumentation and control system for the NPPs is not only a special testing. The software security testing should be included in the system functional and safety testing.

Table 1. The differences between safety instrumentation and control systems and the industrial control systems

Differences	Safety instrumentation and control systems for NPPs	Industrial control systems
Operating system	Special or without operating system	Common operating system
Cyber	Special and safety	Ethernet network/Field bus
Operational	Certain	Uncertain
Differences	Safety instrumentation and control systems	Industrial control systems
Code rules	Rigorous	Defined by manufacturers
Control algorithm	Simple	Complex

Software security of digital instrumentation and control systems for the NPPs may provide the following risks,

- Unauthorized access, sensitive information or date disclosure
- Intercept and tamper with information, software, hardware, etc.
- Prevent data transmission and/or shut down the system
- Invasion of data communication systems or computers

Software security of digital instrumentation and control system for the NPPs is mainly about the following factors,

- Platform threats

The threats may come from the design, development, testing, operation and maintenance. They may be the product design flaws. Application software is designed with vulnerabilities and errors. The developers cannot identify the malicious code (viruses, etc.).

- External threats

It includes the hackers, nuclear radicals against molecules, disgruntled employees/ users, criminal organizations, terrorists and so on. The platform can be attacked or illegal accessed through the network or other means.

- Human factors

The staff factors contain the password leaked, unauthorized actions, equipment damage or replacement which leads to isolation failure.

3 Necessity of Software Security Analysis

Software security of digital instrumentation and control systems includes the three layer defense architectures as shown in Fig. 1. First, the firewall, intrusion detection systems, safety router and virtual private network can provide the foundation prevent. The security infrastructure can only defend illegal access from network layer and application layer. The attacker can make a camouflage construct for the specific application. The inner attack and the camouflage construct cannot be prevented. The safety penetration test can be executed as the second prevention measure. Safety penetration testing continues sending the penetration attack script aimed to the detection object. The safety penetration testing can only detect the known vulnerabilities. A large of unknown vulnerabilities exists in the network. They cannot be check by safety penetration testing.

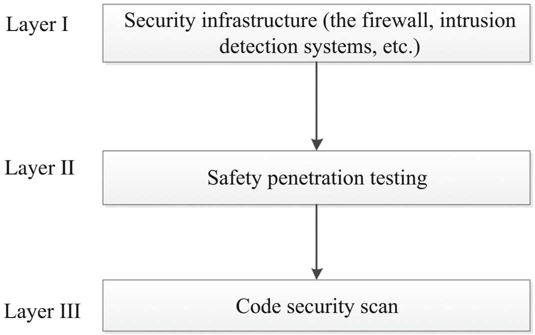

Layer I
Security infrastructure (the firewall, intrusion detection systems, etc.)
Layer II
Safety penetration testing
Layer III
Code security scan

Fig. 1. The defense architecture of the digital instrumentation and control systems

The essence security of software is the last line for the digital instrumentation and control systems to resist the attracters. Commonly, the software developers don't concern whether the code can be used by the attacker. The tester doesn't perform the testing from the attacker perspective. The code security scan is the general measures to ensure the software security. An analysis of potential security threats regarding the software shall be performed. The security vulnerabilities which are depended by the attack can be checked by code security scan. The security scan includes the static and dynamic methods. So the software security of nuclear power plants should include the three level architecture.

4 Software Security

4.1 Software Security Analysis

The risks of software security may come from any moment during the software life cycle. The software security analysis for the safety instrumentation and control system should be performed during the software life cycle.

- Software concept

In the concept, an acceptable level of the security risk needs to be defined. The confidentiality, integrity, availability and accountability security should be identified.

- Software requirements

The security requirements need to satisfy or mitigate the security risks to the acceptable level.

- Software design

The security of architecture and detailed design has been adequately identified. The security threats and vulnerabilities have been controlled or prevented.

- Software Construction

The software implementation needs to accordance with the software design. The new security risks through coding flaws, complier or software update have not been introduced.

The abnormal characteristics (double free, information leak, use of uninitialized variable, array index overflow, etc.) of the code may lead to the software security risks. The inventory of security rules should be built to enhance the software nature security. The inventory needs to be keeping improved by the developers and testers.

The software security testing should to be enhanced during the software development and testing for the safety instrumentation and control systems. The software design flaws which effect the security need to be avoided.

- Software integration

The security strategies have been implemented and the software does increase the system security risk.

4.2 Software Security Strategies

The development should build the acceptable principles of software security. Based on the security risks, the security requirements need to be proposed. The testers make up the security requirements based on the security testing. The defense strategies of security have been constituted and implemented by the development. The testers should execute the testing from the security perspective. Then, the computer security vulnerability database has been built. So the standard security database of safety software needs to be implemented by the developers and tester showing as Fig. 2.

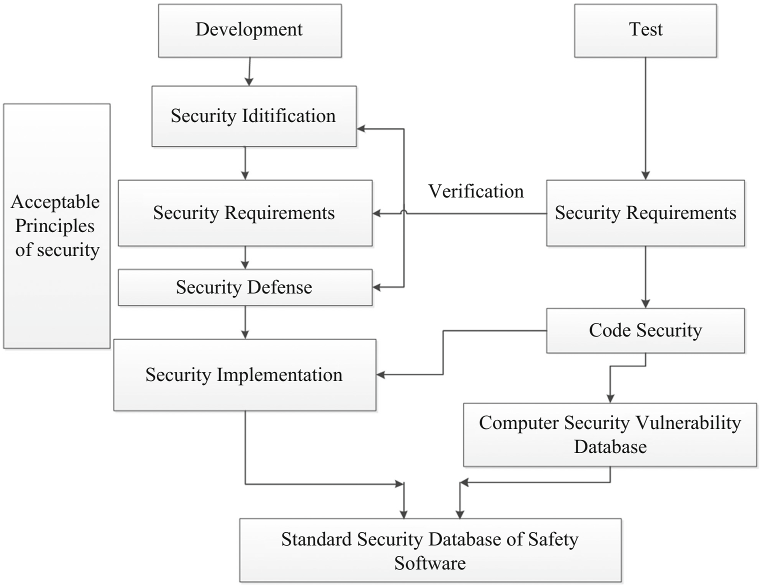


Fig. 2. The security strategies of the digital instrumentation and control systems

5 Conclusions

Software security has been proposed by the article. The digital instrumentation and control system has been compared with the industrial control systems. The security for digital instrumentation and control system of NPPs does not only include the cyber security. Software security needs to be researched during the software life cycle. The nature security of software can enhance the resistance to attack. The three layer defense architecture of the digital instrumentation and control systems has been provided. Finally, the strategies for the software security have been proposed.

Acknowledgements. This project was financially supported with funds which provided by a reliability research of reactor protection system which based on digital microprocessor and electrical equipment (national science and technology major project). The award number is 2014ZX06004002-004.

References

1. IEC 62645: Nuclear power plants – Instrumentation and control system –Requirements for security programmes for computer-based systems. International Electrotechnical Commission (2014)
2. IEEE 7.4.3.2: IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations. The Institute of Electrical and Electronics Engineers (2003)
3. IEC 60880: Nuclear power plants – Instrumentation and control systems Important to safety – Software aspects for computer – based systems performing category A functions. International Electrotechnical Commission (2006)
4. HAD 102/16: Systems Important to Safety Based on Computer of Nuclear Power Plants (2004)
5. IEEE 1012: IEEE Standard for system and software verification and validation. The Institute of Electrical and Electronics Engineers (2012)
6. Chen, W.H., Bai, T., Gu, P.F., et al.: Research on static testing of nuclear safety-critical software. Nucl. Sci. Eng. 36(3) (2016)
7. Ye, W.P., Tang, J.Z., Chen, W.H.: Software V&V methods for safety digital I&C system of nuclear power plant. At. Energy Sci. Technol. 49 (2015)
8. Xi, W., Gu, P.F., Bai, T., Chen, W.H.: A study about software-implemented fault injection strategy for digital RPS in nuclear power plant. In: International Conference on Nuclear, vol. 25 (2017)
9. Gu, P.F., Xi, W., Chen. W.H., et al.: Evaluation system of software concept V&V about the safety digital I&C system in nuclear power plant. LNEE (Lecture Notes in Electrical Engineering), vol. 400 (2016)
10. Gu, P.F., Wang, S.C., Chen, W.H., et al.: A study about safety I&C system software V&V in nuclear power plant. In: 24th International Conference on Nuclear Engineering, vol. 1 (2016)

Application of Variable Frequency Control Technology in Solid Waste Treatment System of Nuclear Power Plant

Jing-Jie Bo(✉), Li Zhou, and Cong Xue

State Key Laboratory of Nuclear Power Safety Monitoring Technology and Equipment,
Shenzhen China Nuclear Power Design Co., Ltd., Shenzhen 518045, Guangdong Province , China
bojingjie@cgnpc.com.cn

Abstract. Based on the brief introduction of the variable frequency control technology, this paper elaborates the design and implementation of the variable frequency control strategy in the transmission line of the cementation facility, and describes the salient features of the control strategy. A frequency converter switches the control of two motors. And the reactor is used to achieve long-distance transmission of the frequency signal. In this project, the frequency regulation mainly affects the operation speed of the roller, and the shift of the roller speed is to take into account both the efficiency of waste treatment and the positioning accuracy of metal drum. The successful implementation of the project provides a good theoretical basis and example for the massive, standardized application of variable frequency control technology in the nuclear power plant.

Keywords: Variable frequency control technology · Solid waste treatment
Cementation facility · Roller transfer

1 Introduction

Cementation facility is a mature and common process dealing with the solid waste in nuclear power plant. Before very long time, it has been monopolized by foreign suppliers. But as the spread of democracy and localization in the nuclear power plant construction in recent years, solid waste treatment system breaks the foreign monopoly, the key equipment and the design of control system adopt customized design. On this basis, through application of variable frequency control technology in the cementation facility, the efficiency of the solid waste processing is improved significantly.

2 An Overview of Variable Frequency Control Technology

The basic principle of variable frequency control technology based on the characteristics of motor speed is proportional to the work input power frequency, to achieve the purpose of changing motor speed by changing the power frequency. The main characteristics of variable frequency control technology include the power saving, power factor improving and the motor soft start-up and so on. The control mode of variable frequency control

Y. Xu et al. (eds.), *Nuclear Power Plants: Innovative Technologies for Instrumentation and Control Systems*, Lecture Notes in Electrical Engineering 455,
https://doi.org/10.1007/978-981-10-7416-5_4

system is including volt & frequency (V/F), vector control (VC) and direct torque control (DTC), etc. V/F control is mainly applied to lower cost and lower performance requirements. Due to the introduction of VC, the variable frequency control system can be applied in high-performance situations. DTC is a kind of inverter to control the torque of a three-phase motor. It can control the speed of the motor after controlling the torque. In recent years, with the development of semiconductor technology and the popularity of digital control, the application of vector control has been extended to general drive and special driving situations from high-performance areas, such as the variable frequency air-conditioning, refrigerator, washing machine and other household appliances [2].

Alternating Current (Ac) drive has been widely used in industrial robots, automation equipment, processing tools, transmission equipment, elevators, compressor, fan pumps, electric cars and other fields. With the rapid development of semiconductor technology, the processing capacity and speed of Microcontroller Unit (MCU) are increasingly improved. Variable frequency control system is fully capable of dealing with complex tasks, complex observation and control algorithm. Therefore the transmission performance can be up to an unprecedented height [3].

3 Introduction of Solid Waste Treatment System (TES)

3.1 The Function of the Process System

Solid waste treatment system in nuclear power plant is mainly used to collect, store and handle the middle and low radioactivity level of solid waste through the operating of the nuclear power units. In domestic nuclear power plant, the cement solidification process is mostly used to deal with the three kinds of solid waste: waste resin, concentrate and filter cell. They are fixed with cement and form stable curing in the metal drum, which can be transported and stored easily.

3.2 Introduction Control System

As a result of the processing object has certain radioactive, in order to reduce the exposure of the operator, all operations can be completed on the digital control platform in the control room when the cementation facility is operating. Control system connects the equipment such as roller transmission system, the dry mixing station, waste filter cartridge etc., which implements the following control functions:

- Under normal operating conditions, the process system can be started and stopped normally, and the waste treatment process can be automated and controlled by the operator.
- In the event of an emergency, the system can be stopped through the emergency shutdown function, ensuring the integrity of the equipment and avoiding damage to the equipment and the leakage of radioactive materials.
- Set the interlock protection and alarm function, in order to avoid the damage of the equipment and the leakage of radioactive material that caused by the operation.

- The system self-check function and equipment initialization settings, to ensure that all equipment is in a safe position before operation and all equipment should be back to the safe position in the event of failure.
- Provide friendly human-computer interface and video monitor interface, and operator can monitor the whole process of waste treatment and key station.

4 The Application of Variable Frequency Control Technique in TES Control Strategy

4.1 The Design of the Roller Transmission System

As one of the most important unit in cementation facility, roller transmission system aims to transmit and locate drums between stations accurately and smoothly. Roller transmission system consists of many rollers that be connected together. Its function includes forward/backward transmitting of drums, elevating/descending of drums and sideway between rollers. In order to improve the reliability of the roller transmission system, two redundant motors are configured for each roller. In order to increase production efficiency, the normal transmission speed of the roller is about 5 m per min. Furthermore, transmitting speed decreases to 1 m per min. in order to ameliorate positioning accuracy. To realize variable speed control, variable frequency servo motors are applied as roller motors whose speed is controlled by inverters. Transmitting speed of each operation mode can be set and be modified on human machine interface (HMI). An overview diagram of roller transmission system is shown with Fig. 1 [4].

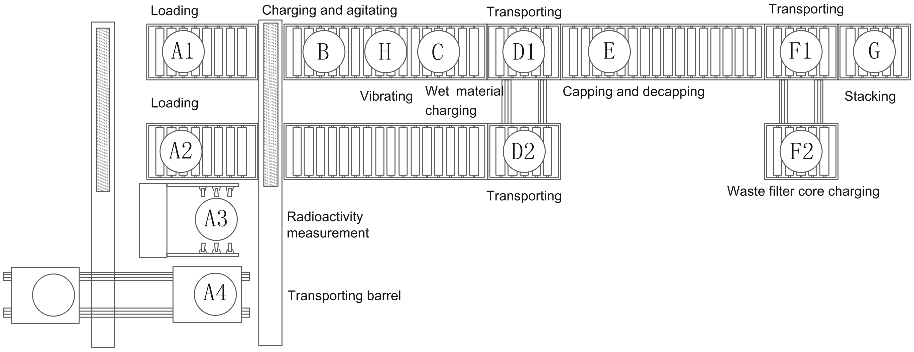


Fig. 1. Roller transmission system

4.2 The Design of the Inverter

According to the power of the roller motors and the requirements of control precision, cementation facility control system uses ABB-ACS series inverter, to provide high performance of speed control, torque control and motor control for the mechanical equipment. Compact hardware design and flexible programming ensures optimal solutions. The new type of storage unit is designed with flexible transmission configuration for mechanical drive.

The ACS series inverter provides superior performance and functional mechanical drive for mechanical applications. It can control induction motor with feedback or no feedback function, synchronous servo motor and asynchronous servo motor. It uses DTC motor control technology to ensure superior performance. The ACS design of structure is very compact and can be mounted side-by-side. In addition to standard features, there are three options slots for control and communication. Drive tools can be used for function of debugging, optimization, and programming. Its design features are as follows:

- Compact design and modular design.
- Global compatibility for the mechanical environment and standards.
- Various standards for control and communication interfaces.

In addition, the roller motor is a drag type motor, so the inverter must have "torque" overloading starting. ACS series inverter is with "torque" and "speed" two kinds of configuration mode.

4.3 Control Strategy of Variable Frequency

According to the arrangement of the roller and the distribution of each key position, the entire transmission system is composed of thirteen rollers. The transmission of each roller is completed by one master variable frequency motor and one backup, with 26 variable frequency motors installed. According to the network architecture of cementation facility control system, operating station is connected to the main controller with process control network, and main controller exchanges signals to the inverter through I/O cards. The inverter transfers the 380 VAC input power in the plant to the variable frequency motor after frequency modulation. According to the number and size of inverter, the overall plan is to install four inverters for one inverter cabinet, and the control system structure chart is illustrated with Fig. 2.

According to the control requirements of process system, the centralized control system sends motor's start and stop command, frequency set, and fault restoration command. And the signals, including inverter ready state, running state, fault state, state of positive & negative, frequency feedback and current feedback signal are sent back from the inverter. At the same time, the overload relay is set up in the inverter outlet to ensure the safety of the motor circuit.

Based on the switching characteristics of the main and backup motor, it uses an optimized control strategy that an inverter hangs a main and a spare of variable frequency motor for one roller. The operator sets the operating motor and switches these two motors on HMI. The scheme is accomplished by remote control of the AC contactor on the motor powered circuit. Two contacts of the main and spare motor carry the interlock on the electrical circuit, and only one motor could be started. The main and spare motor's contacts are controlled separately by the control system to prevent false action [1].

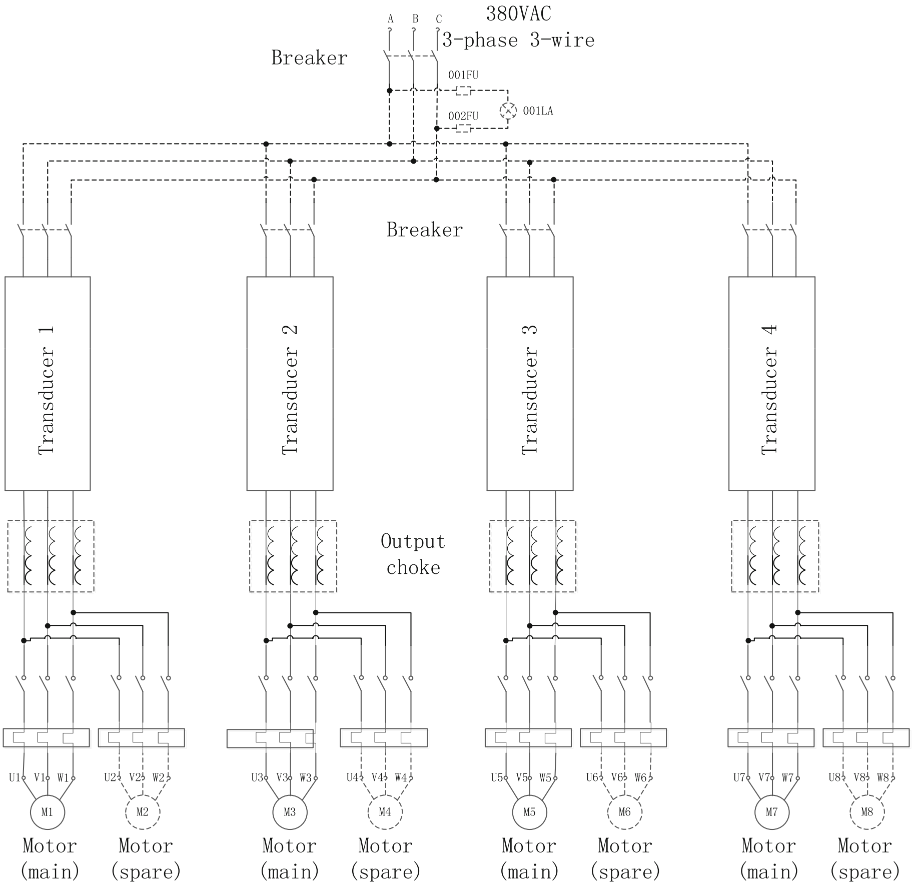


Fig. 2. Inverter control system

In addition, because the distance between the frequency inverter cabinet and inverter motor is longer than 100 m, variable frequency control strategy has been designed from the following three aspects in order to ensure the inverter's output performance:

- Equip the inverter with a motor reactor, and then the motor reactor can reduce the overvoltage of motor terminal and minimize the current waveform, so the motor noise can be reduced.
- Equip the inverter with a brake resistance, and it is used to stop the motor quickly, absorb excess power, and reduce the impact on the frequency inverter.
- The power of inverter is greater than the motor, to ensure that the output power of the inverter is sufficient.

5 Conclusion

In the nuclear power plant, the use of fixed frequency and constant speed motor is relatively common, and mainly applied to the actuator, such as pump and valve on the process pipe. Because of the special control requirements of the roller transmission line in solid waste treatment system, variable frequency control technology has been introduced in order to ensure the production efficiency and positioning accuracy. Meanwhile, through the integration of control system, inverter, variable frequency motor, and electrical equipment, a remarkable characteristic of variable frequency control strategy has been made. After on-site debugging and commissioning, a successful application case of using variable frequency control technology was provided in the follow-up nuclear power plant.

References

1. Chen, L.: Domestic application of the cementation facility control system. Automation Application (7) (2016)
2. Chen, G.C.: PWM variable frequency control and soft switch power technology. Mechanical Industry Press (2002)
3. Wang, Z.A., Yang, J.: Application of variable frequency control technology. China Electric Power Press, vol. (7), pp. 42–46 (2015)
4. Zhu, H., Chan, H., Lv, N.: The design of TES cementation facility in Ning De nuclear power plant unit 3–4. The Annual Report of China Atomic Energy Science Institute (2013)

Application Research of the Computer-Based Post-Accident Monitoring System on the Third Generation Nuclear Power Plant

Xiang-Jie He(✉)

State Key Laboratory of Nuclear Power Safety Monitoring Technology and Equipment,
Design Institute Shenzhen China, Shenzhen China Nuclear Power Engineering Co., LTD.,
Shenzhen, Guangdong Province, China
hexiangjie@cgnpc.com.cn

Abstract. The Post-Accident monitoring system (PAMS) which used in the monitoring system of nuclear power plants for preventive accidents management and mitigative accidents management is a safety important instrument system. This paper introduces the selection of accident monitoring parameters and the general design requirements. Through analysing PAMS about the typical application for structure, acquisition and condition scheme, equipment qualification and the characteristics of the power supply on the third generation of Pressurized Water Reactor (PWR) Nuclear Power Plant (NPP), contrast the technical characteristics and plan of accident monitoring system on the third generation of PWR NPP, explore the technical requirements and the development trend of monitoring technology, provide the reference for PWR NPP accident monitoring system of computer application, research and development.

Keywords: Post-Accident monitoring · Computer-based equipment · The third generation Nuclear Power Plant · Comparison of application · Research

1 Introduction

PAMS is a safety important I&C system including a series of monitoring information. This information can provide judgments for the operator accomplishing and maintaining NPP to safety states. The computer-based equipment has the high reliability, flexibility, and less restriction on scale of panels. The qualification computers have been extensively adopted by NPP,which have the high reliability, better maintainability, and meeting the requirement of information shared and date secondary exploitation. For using computer, the conditioning and selection information according to plant condition is easier. It is more convenient for operator on accident management and monitoring. It should be necessary to enhance the application research of computer-based PAMS.

Y. Xu et al. (eds.), *Nuclear Power Plants: Innovative Technologies for Instrumentation and Control Systems*, Lecture Notes in Electrical Engineering 455,
https://doi.org/10.1007/978-981-10-7416-5_5

2 Selections and General Design Requirement for Accident Monitoring Parameters

2.1 Selection of Plant Parameters for Accident Monitoring

Accident monitoring instrumentation needs to provide the necessary information to support making operational decisions during implementation of emergency operating procedure (EOPs) and severe accident management guideline (SAMGs),need to be selected with the goal of supporting the emergency response plan decision making process [2]. Generally plant parameters for accident monitoring include DBE and DEC parameters to support preventive accident management and mitigating accident management.

Parameters for Design Basis Accident include [3] includes:

- Parameters for providing information essential for the control room operator of taking the specific planned manually-controlled actions for which no automatic control is provided to bring the plant to safety state;
- Parameters for providing the assessment of achievement and maintenance of the plant safety functions to the control room operators;
- Parameters for providing the most direct indication of the integrity of threefold fission product barriers;
- Parameters for providing the performance of safety system, auxiliary supporting features and other systems indirectly indicating the safety shutdown state, and f or confirming safety system status;
- Parameters for providing evaluation of the magnitude of the release of radioactive materials through identified meteorological condition.

The accident monitoring parameters for Design Extension Condition (DEC, including Severe Accidents) needs to provide the safety information required to appropriately respond to plant conditions as the accident progresses. This information enables plant operators to make correct decision.

2.2 General Design Requirement of Instrumentation

Referencing GB/T13627, the types of post-accident monitoring variable include Type A, B, C, D, and E, different variables are not mutually exclusive. When a variable belong to one or more of five types, this variable must comply with the variable type the highest requirements. Accident monitoring instrumentation implement functions over the duration required to enable plant operators to appropriately respond to the accidents according to guidelines and procedures. The safety classification of the specified instrument for accident is to comply with GB/T 15474-2010 [4]. The safety classification of various parameters for the requirements of equipment list in the following Table 1, which only give the basic requirements of accident monitoring parameters corresponding to the different safety function classification equipment, taking D parameters as an example, the signal can be taken from the A/B safety classification of class equipment.

Table 1. Requirements of safety Classification of accident monitoring parameters

Accident monitoring variables	A	B	C	D	E
Categories of safety function (Requirement of equipment)	A/B	B	B	C (shall be seismically qualified and environmentally qualified according at the installed location), DEC will generally be assigned to category C	NC

For Type A, Type B, and Type C variables, instrument has the highest reliability requirements. The instrument shall be seismically qualified and environmentally qualified for that accident's intended environment at the installed location. Accident monitoring instrument shall satisfy the requirement of single failure, common cause failure, independence and separation, isolation. The failures of an accident monitoring instrument don't result in information ambiguity that could lead the operator fail to accomplish a required safety function. The power supply for instrumentation that monitors Type A, Type B, and Type C variables is Class 1E. Control room indication shall be uniquely identified with a characteristic designation so that the operator can easily discern. At least one of the redundant display for Type A and Type B accident monitoring variables shall be a spatially dedicated continuously display. The reliability requirements of class D parameters are not as high as Type A/B/C variables. They are generally implemented with Non-1E equipment to meet the requirements of the environment and seismic, and Non-1E power supply is required. The reliability requirements of Type E variable are the lowest, which are generally realized by NC equipment, without relevant environment and seismic qualification requirements.

3 Characteristic of PAMS on the Third Generation NPP

3.1 The Characteristic in EPR

In EPR, 1E TXS and non-1E TXP DCS platform are adopted. Although no system standard for design criteria of PAMS be used, redundant configuration qualified display system (QDS) are still used as the man-machine interface of TXS, and realize the power plant an important safety parameter monitoring function. Independent severe accident instrumentation should be considered. Two PS QDS and two SA QDS are equipped to display and record the safety important parameter. At the same time, the conventional safety display instrument (ID) is also considered in the safety information and control system (SICS). The safety important parameters are also processed and displayed by the process information and control system (PICS) implemented by the gateway to the non 1E class TXP platform. The structure abbreviated drawing is shown in Fig. 1.

QDS Configuration meets the requirements for independence and isolation between channels. The safety classification signals are acquired and distributed through Protection Instrumentation Pre-processing System (PIPS), afterwards are delivered to the protection system (PS with four channels), which is connected to the QDS via the Message and service interface (MSI). The calculated core thermocouple signal and RPN signal for the core cooling calculation are sent to PS, these signals are sent directly to the 1E ID via MSI, parts of signals from MSI are sent to the QDS by PI. The parameters needn't be calculated and recorded are sent to 1E ID directly through PI, otherwise the

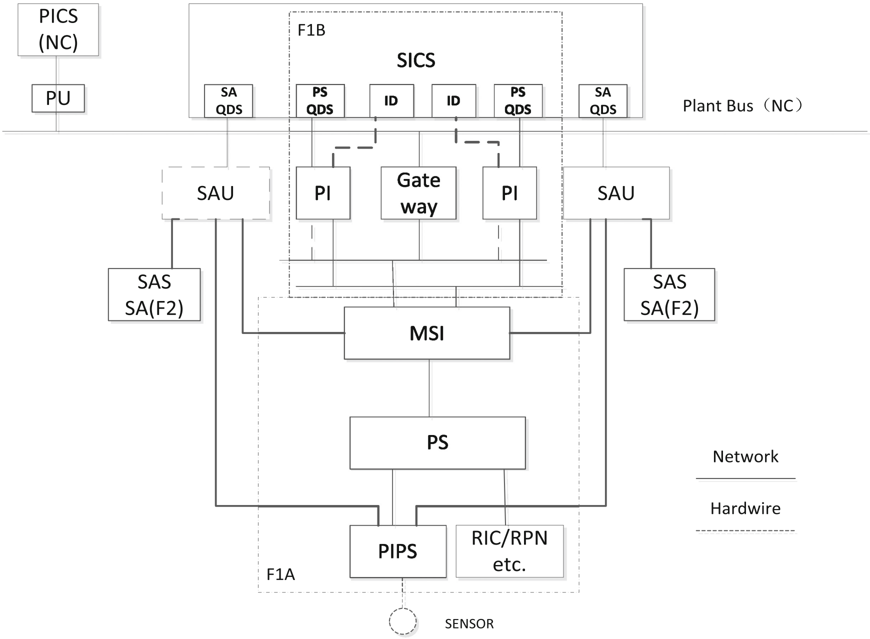


Fig. 1. The structure abbreviated drawing of PAMS for EPR

parameters are delivered to QDS and/or 1E ID. Few signals collected from NC system (such as meteorological and regional radiation monitoring parameters) are displayed in non-safe PICS.

For SA QDS, there are two severe accident units (SAU), the interface with PICS is ensured through the Monitoring and service interfaces units of PS (PS-MSI) and the gateways of PS. Parts signals are acquired from PIPS and SAS [5].

The PS QDS is powered by 1E AC power supply, which is connected with diesel generators and two hours of UPS when normal power is lost, and the SA QDS are powered by SBO diesel and 12 h of UPS [5].

The main characteristics of accident monitoring system in EPR is to adopt the special safety important redundancy QDS based on computer, for data acquisition and processing, indicating the overview of plant sate, showing the sorted according to the safety function, displaying the trend of accident parameters and records as shown in Fig. 2. For some of F1A function continuously display signals, such as valve state etc. if the PICS becomes unavailable SICS design the conventional indication Devices ID, the different color of equipment label can distinguish PAMS parameters. The operator can be identified by the QDS display and the alarm when the data is reliable.

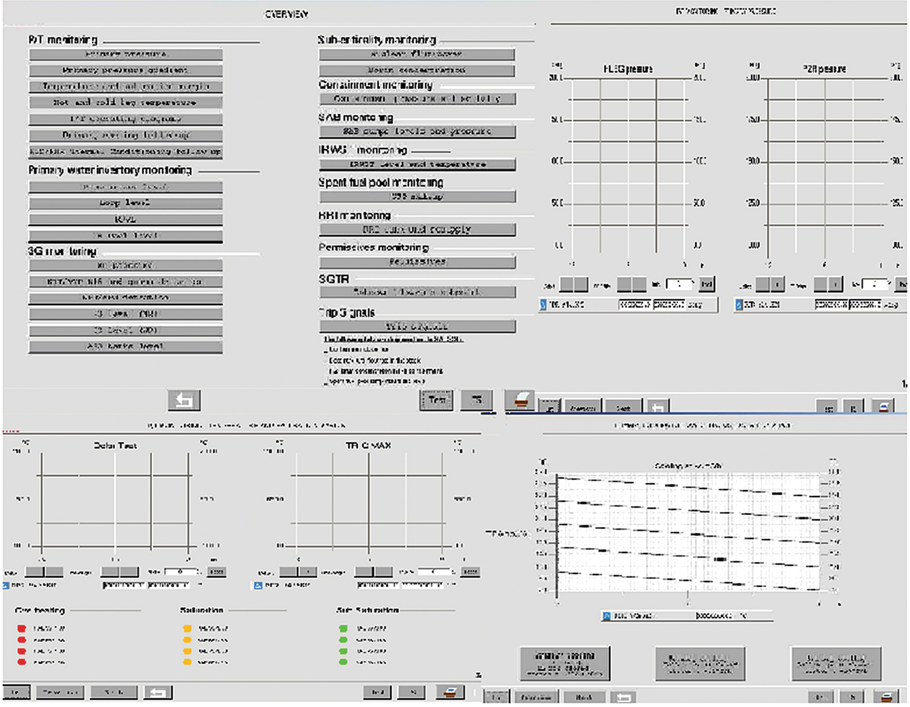


Fig. 2. Illustration of QDS display

3.2 The Characteristic in AP1000

Taking an AP1000 nuclear power plant as an example, the DCS consists of a 1E Common Q platform and a Non-1E Ovation platform. PAMS is performed by part of the reactor protection and safety monitoring system (PMS), power plant control system (PLS) and the data display and processing system (DDS). The PMS provides signal conditioning, communications, and display functions for Category 1 variables and for Category 2 variables that are energized from the Class lE uninterruptible power supply system. The PLS and the DDS provide signal conditioning, communications, and display functions for Category 3 variables and for Category 2 variables that are energized from the non-Class 1E uninterruptible power system. The DDS also provides an alternate display of the variables, which are displayed by the PMS. The structure of PAMS is shown in Fig. 3.

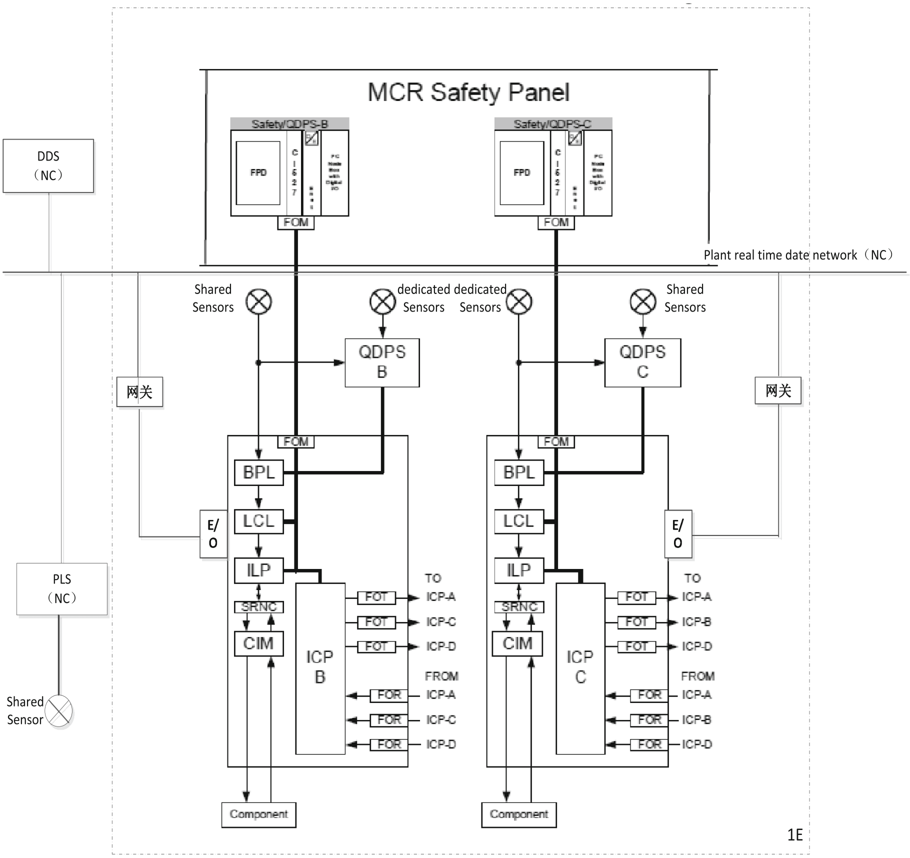


Fig. 3. The structure abbreviated drawing of PAMS

The accident monitoring system is implemented by the PMS with redundant configuration, One QDPS subsystem is located in Division B and the other QDPS subsystem is located in Division C of the four redundant divisions, designated A, B, C, and D of the PMS. The post-accident monitoring system consists of 1E flat-panel displays (FPD), the identification data processing system (QDPS), and the AF100 internal isolation network [1].

The dedicated sensors are directly connected to the QDPS via hardwire. For the shared sensors, part of signals sent to QDPS directly or via Bi-stable Processor Logic (BPL). The signals from division A, D communicate by HSL point-to-point and photoelectric isolation from integration communication processor (ICP) of division A/D to ICP of HSL B/C, then share in AF100 network of division B/C with QDPS.

QDPS processors realize group control of valves, calculation of the sub cooling and the core cooling conditions, and display the accident monitoring the information in FDS for the operator command.

Power of QDPS subsystems are from the Class 1E DC and uninterruptible power supply (UPS) system for 72 h after a loss of all AC power (station blackout). After 72 h, the ancillary diesel generators provide power for the QDPS subsystem.

The Non-1E accident monitoring parameters are sent to DDS from PLS via the NC plant real-time date network, via which PLS is connected to PMS.

4 Comparison and Application Research

4.1 Comparison of Technical Characteristics

On the third generation NPP, PAMS adopt special safety important digital display device, and combine with few conventional safety display instrument structure. Based on the principle of "available with", under normal condition NC system is used to display the state of plant, once in accident condition NC system failure, the safety display device can be used for monitoring the safety status of NPP. Safety processing display device meet the requirement of single failure criterion and the redundant configuration. Except

Table 2. The technical comparison of PAMS on the third generation NPP

Technical requirement	Third generation NPP	
	EPR	AP1000
System structure	Signal decentralized collection and centralized display based on computer	Signal decentralized collection and centralized display based on computer
display (Continuous and on-demand display)	Dedicated F1B PS QDS and F2 SA QDS for on-demand display,With 1E conventional ID. All parameter Display in KIC with NC and anti- seismic.	Dedicated pages in 1E QDPS, including severe accident parameter All parameter Display in DDS with NC
Independence, separation and isolation	Two channels redundant QDS meting the requirement between channels, 1E and NC	Two channels redundant QDPS meting the requirement between channels, 1E and NC
Common cause failure	Alternative parameter, 1E conventional instrumentation spare, and KIC	Alternative parameter and DDS
Information ambiguity	The failure alarm in KIC and BUP by Calculating and processing in QDS.	The failure alarm in KIC and BUP by Calculating and processing in DDS and QDPS
Power supply	PS QDS with 1E AC and 2 h UPS, SA QDS with SBO(part with 24 h UPS)	QDPS with 1E AC, 72 h UPS and SBO
Seismic and environmental qualification	Safety important parameters	Category 1
Trend	On-command displays With QDS	On-command displays With QDPS
Recording	KIC and QDS	DDS and QDPS
Display identification	Without in QDS, available in conventional ID	Without in FDS

for some special monitoring signal, most shared signals are acquired via communication isolation and electrical isolation from safety system. The characteristic of robust technologies is used, through the different structural configuration to meet the requirements of the performance of the existing nuclear power plants.

According to the design and technical requirements of PAMS, the technical requirements comparison of the accident monitoring system on the third generation NPP are analyzed as shown in Table 2.

4.2 Application Research

During the Japan Fukushima Daiichi accident, in 2011, the instrumentation provided for accident monitoring proved to be ineffective for a combination of reasons that appeared to include a loss of power, failure of sensors due to environmental conditions, instrument ranges that were not suitable for monitoring plant condition and a lack of alternative data for use in validating instrument readings [2]. All national authorities have strengthened the review of accident monitoring instrument on high requirements for reliability, design criteria and performance criteria, and application of operator aids equipment. Reference the design requirements of accident monitoring instrument in IAEA NO.NP-T-3.16, the development of the accident monitoring system based on computer equipment is suggested in following,

- Two diversified digital platform of 1E and non-1E may be adopted for different system structure according to the classification and design requirements of the monitoring parameters. In normal condition all parameters including the severe accident are monitored in non-1E digital platform. Type A, B, and C parameters with display identification can be display by one alone digital safety display device of redundant configuration. For the development of qualification large screen equipment for continuous and trend parameters should be considered according to the requirement display.
- Operators need to be provided with information about the reliability, expected limits to operability and survivability of both designated and other available accident monitoring channels, so that they can recognize conditions that may be impairing the reliability of the readings. For each accident monitoring channel, the aid should ideally include information such as,instrument tap, sensor, transmitter, signal processing and readout locations, instrument channel range and any provisions available for extending the measurement range, channel uncertainties when exposed to the environmental conditions and plant power source, which provide support for operator accident handling and evaluation.
- Advantage characteristics of computer equipment on confirming quickly and validity of the digital display signal can be used for such as that the signal can be judge by color logo and alarm in combination with the background of solution, making it easier to identification for operator.
- As a backup of computer equipment, complete and clear information on the instrument of an accident should be maintained in the emergency procedure and severe accident guide.

- The application development of calibration following environment and extended display range can be conducted for the parameter impact of the base accident environment and the severe accident environment.
- Using of severe accident modeling to establish necessary parameter ranges, mission times and environmental conditions which equipment needs to withstand, provide better analysis for the design of the accident monitoring instrument [2].
- Although the safety classification of extend accident condition monitoring instrument (including severe accident) generally is lower, but the instrument may be exposed to severe environments for long-term, unless a single channel can be repaired or replaced at an acceptable exit time within the scope of operation, redundancy need to be considered. Because severe accidents are more likely to be characteristic of trend monitoring, it is considered to set up a redundant digital display device for severe accident monitoring.
- As a backup of computer equipment, complete and clear information on the instrument of an accident should be maintained in the emergency procedure and severe accident guide.

5 Conclusions

With the development of technology, for meeting the higher requirements of PAMS, the safety classification digital equipment will be widely adopted in PAMS. In addition to the permanent monitoring instrument, the safety information can be gained through the offline analysis sampling method, such as portable instrument. The use of robots and unmanned aircraft can be used as a means of support for the harsh environmental conditions, it is developed in further.

References

1. Application of Common Q of 1E digital platform in AP1000, Progress Report on China Nuclear Science & Technology, vol. 1 (2009)
2. Accident Monitoring Systems for Nuclear Power Plants IAEA NO.NP-T-3.16, Vienna (2015)
3. GB/T 13627. Criteria for accident monitoring instrumentation for nuclear power generating stations (2010)
4. GB/T 15474. Classification on instrumentation and control function important to safety for nuclear power plants (2010)
5. Overall I&C Architecture Description TS-X-NIEP-NLEC-F-DC-18 (2008)

Study About UI Design Optimization of TNPS MMI

Jie Xu[✉]

Electrical and I&C Branch, China Zhongyuan Engineering Corporation,
Shanghai Branch, Shanghai, China
xujie@czec.com.cn

Abstract. Tianwan Nuclear Power Station Phase I is the first nuclear power station that adopts full digital instrumentation and control system in China. Due to the fact that there is no reference station in the complete sense for the original design, most of the design is actually new. This leads to plenty of exploration and study in terms of how the Man Machine Interface satisfies most effectively the requirements of human factors engineering. To certain extent, it affirms the utilization of digital I&C system, and proves the effectiveness of MMI, as the two units of Phase I have achieved good operation performance, economic benefits since commercial operation. So Phase II based on the successful construction and good practice of Phase I, implements the strategy of 'Copy plus Improvements'. I&C System still adopts full digital I&C system. MMI is basically the same, and assimilating the experiences in aspects of design, commissioning and operation of Phase I. This essay introduces the general structure of computerized MMI in Phase I, studies and summaries the principles of display design, discourses how to realize these principles during engineering. Through aforementioned studies, this essay analyzes the display design advantages and disadvantages of Phase I, introduces some implemented measures in Phase II.

Keywords: NPP · I&C system · MMI · UI · HFE · V&V

1 Introduction

Tianwan Nuclear Power Station Phase I processes and systems' general designer is institute SPAEP of Russian. Full digital instrumentation and control (I&C will be used in the following contents) is used for the first time. Main I&C system is used during normal operation or events combined with relatively, independent I&C system for the reactor and fire protection and ventilation I&C system. All these I&C systems are used to monitor and control the units in all conditions. Man-machine interface is computerized and achieved by OM690 (Operation and Monitoring System 690) supplied by SIEMENS. Tianwan Nuclear Power Station Phase II Nuclear Island is designed by the institute SPAEP of Russian. Phase II Conventional Island's designer is Chinese institute. Control system is still full digital I&C system. Man-machine interface system is improved OM690 designed and supplied by CASS (Consortium of AREVA, SIMENS

Y. Xu et al. (eds.), *Nuclear Power Plants: Innovative Technologies for Instrumentation and Control Systems*, Lecture Notes in Electrical Engineering 455,
https://doi.org/10.1007/978-981-10-7416-5_6

and SPPA). The following paper illustrates displays design process, combining principles and practices of Phase I. The paper also illustrates design improvements based on analytical results from concept design and displays' detailed designing process.

2 Content

2.1 Overview

In accordance with URD, each MMI system at nuclear power stations is comprised to some degree of the following functions:

- Data gathering equipment which monitors equipment and process variables.
- Data communication equipment which transmits equipment and process variables between data processing equipment and plant equipment.
- Plant information display and control equipment which provides alarm and display media for plant personnel to access plant processes and equipment status, and control to operate plant equipment.
- Output processing equipment which provides the necessary interfaces between plant controls and plant equipment actuators.

The scope and interface for a typical integrated MMI system are shown in Fig. 1.

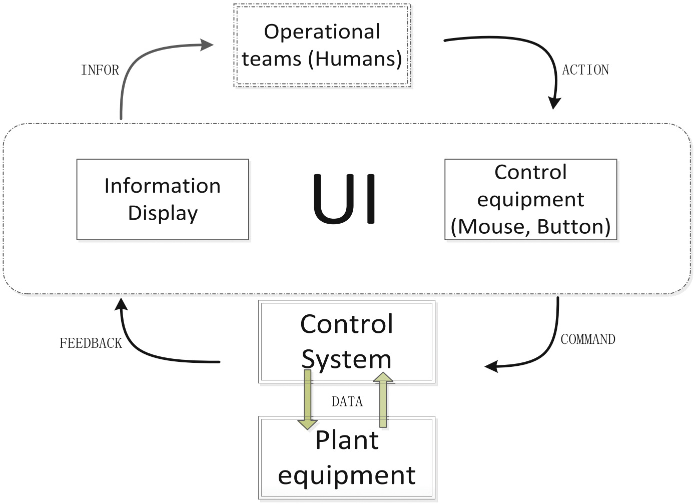


Fig. 1. Structure of man-machine interface system

It shows that UI is the media to transfer and exchange information between human and machine. Plant operators can intervene and check in the plant process system or control system on different levels by means of specially designed interface to enable MMI system to execute its functions.

Displays are one kind of UI. After adopting full-digital I&C system, except a small number of display and control in backup safety control panel/desk, a large amount of information and control is shown in different form of display.

2.2 Phase I's Displays Design

2.2.1 Establishment of Phase I's Displays Structure

The principal users of each group of displays should be identified to convert visual hierarchy concept into actual NPP operation requirements, which will be part of design requirements definitions. There is a need for information and control as well as systems' safety, availability and operability.

Phase I's displays have the structure which includes overview, plant major processes, sub-functions and detailed information. It's organized and distributed based on tasks of reactor operators, turbine operators and auxiliary system operators. The layered structure design of displays is shown in Fig. 2.

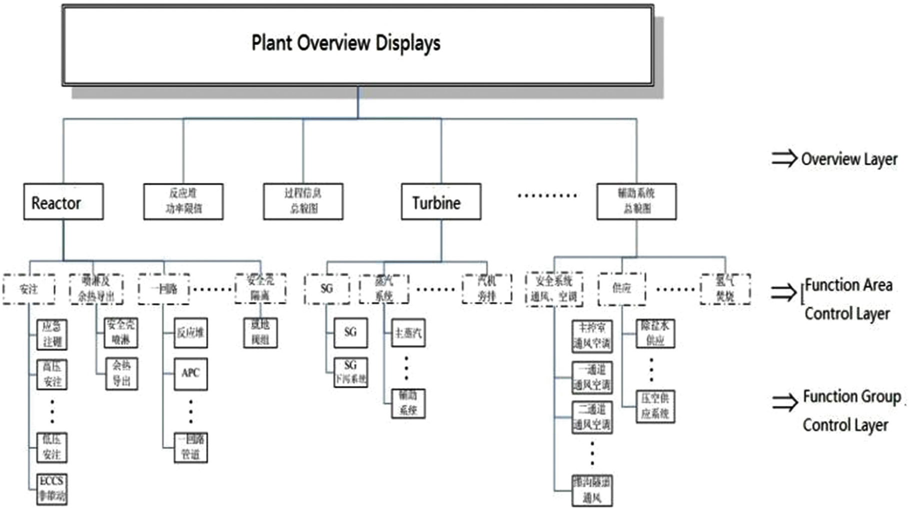


Fig. 2. Display layered structure design

2.2.2 General Design Requirements for Phase I's UI

The design process of the Phase I's UI is according to the requirements of IEC964 in general. The requirements for display design used in Phase I as following:

- Displays should be as simple, clear and comprehensible as possible. Where complex or highly detailed displays are necessary, good organization and structure are used.
- Information shown on display shall be clearly understood in any operation conditions, and the display shall communicate the intended information to the operator without ambiguity or loss of meaning.

- Standardization of displays and symbols shall be used. all items within a suite of displays which represent the same information should be similarly named.
- Related items of the power plant should be organized in such a way that reflects their relationships with an appropriate degree of abstraction to avoid complication of the display.
- Background colors should be neutral. It is essential to use grouping and coding techniques for enhancement of the perceptions of displayed information.

All plant conditions and most of the equipment status information of Phase I can be displayed with UI, which shows simulations, data, states, time charts and alerts of either a power plant or equipment. The displayed information is sufficient and necessary, not only gives the overall operating parameters and operating conditions of the NPP under various operating conditions, but also gives the safety status of NPP, the operating status of major equipment and the operating state of the major safety facilities. The range of the parameter settings takes into account the startup, shutdown and accident conditions. equipment state display can reflect the actual situation, such as liquid to charged state. Standard dynamic symbols are used for the valve state, the pump start or shut down upon the background color with a light gray. Standard layout is used in the measured value of the digital string.

2.2.3 HFE in the Implementation of UI Design in Phase I

It is commonly known that human factors and possible human errors play an important role in the safety and availability of the nuclear power plant which needs to achieve required safety and availability. HFE principle shall be obeyed and run throughout all cycle life of NPP.

We have developed a plan that defines the HFE team configuration and assure that all activities are correctly performed in Phase I. The U.S. NRC NUTEG-0711 has been used as guidance in order to ensure consistency and to address all aspects of HFE design. HFE related engineering documentation have been delivered to NNSA for review to support NPP operation license application.

HFE principle complied in the UI design, such as the set of any group displays or a display of an arbitrary element meets operators' demand. The size of characters and symbols in readability also meets the requirements.

2.3 Improvement of UI for Phase II Project

The UI design is based on users' demands to implement the task correctly and quickly. It's also based on the design instruction of NPP systems and all operation conditions of NPP. Taking into consideration the fact that the strategy of "Copy plus Improvements" is adopted for Phase II project, the collection and analyzing of experience feedback from Phase I project was conducted before the UI design for Phase II project started.

2.3.1 Improvement of Display Structure

Owing to the complexity of operations at nuclear power plants, the designer of UI needs to orient the function of computerized MMI based on the quality and performance of equipment adopted, and determine the concept of how the operators conduct monitoring operation at the power plant by means of man-machine interface after completing control room function analysis and allocation, and task analysis.

Relevant materials about function design of Phase I control room has been analyzed and confirmed together with the institute and operation personnel before the design on the UI for Phase II project starts. In this way the operation configuration of power plant, function of control room, and safety, availability and operability targets of system are not changed. It is determined that no big adjustment is needed for the schematics categorization, function, hierarchical structure and organization mode, but small design improvement is made to consider hierarchical principles and operation experiences when determining display structure.

2.3.2 Improvement on UI Design Input

In Phase I, the process design personnel from SPAEP submits the input data related to the design of Main I&C system and MMI, and the personnel of SIEMENS executes the UI design. The input data of UI design includes display draft, display signal list and necessary signal logic list.

The design input of UI is summarized into the following contents at least through the investigation on the input data of UI design in Phase I for design personnel to create reasonable display:

- Brief description about display purpose submitted in text.
- Proposal about display layout submitted in sketch drawing.
- Necessary signals list submitted in excel form, including signal identification (such as KKS) and signal definition.
- Information such as signal process logic and related time correlation, submitted in the form of function diagram.
- Description about display of refresh time, description about refresh frequency of every signal, description of test etc.

Based on a.m. analytical results, there isn't a very important part in Phase I project, that's the brief description about display purpose submitted in text. Therefore, it's defined in the concept design stage of Phase II that the part of display description will be added into the input data submitted by the process design personnel including the graph, displayed signal list, necessary signal logic list and the display purpose, function and represented information Before subsequent UI design starts, the process design personnel are required to give explanation referring to the control function and corresponding display elements as for important display of control function.

From the viewpoint of implementation result, the information is not only helpful for the UI designer to understand and implement display design, but also essential for the instruction developer to correctly understand the original intention of designed monitoring means and develop various instructions.

2.3.3 Improvement on Verification of UI Design

As for the UI design, the implementation condition of general requirements of design from Phase I has been summarized as follows:

- Layout of information displayed in UI. Confirm that the display layout based on the functions of NPP is reasonable, and it's capable of transmitting the information clearly without missing anything under any condition.
- Source of information displayed in UI. Simultaneous performance of display design and I&C design of corresponding function group obtains balanced design meeting actual condition.
- Display interface and database used 'Master plate'. The actual application in Phase I project has proved that the background color, standard symbol, interface and used schematics database etc. specified for UI design requirements are suitable and applicable.
- HFE V&V have integrated with the design process, the V&V findings presented that the proposed function assignment takes the maximum advantage of the capabilities of human and machine without imposing unfavorable requirements on either of them.

Based on these analyses, the design principle and requirements haven't been changed largely. However, it's found during analysis that the practicality test of UI design have been passed the characteristics evaluation of design itself, but have not performed evaluation by user (as for the NPP, the user of UI is the plant operation personnel) on utilization of this design before factory acceptance.

Therefore, a multi-disciplinary owner team has been set up in the course of UI design to directly participate in the review of display draft, including I&C, commissioning and maintenance personnel, and operation personnel familiar with normal, abnormal and accident operation procedures. This owner's team review the design document (including display) completed for function groups, confirm the main information and related information in one display, and especially test the unacceptable contradiction. As for subsequent factory test, this owner's team is conduct operation verification on actual display, including the correctness of NPP displays navigation and related link, correctness of display data and rationality of information combination, to confirm if the display design conforms to the original design requirement.

For the Phase II the execution of all plant procedures will take place in a dynamic environment (mock-up or simulator) prior to the plant going into service. This effort will be lead and executed by this owner's team.

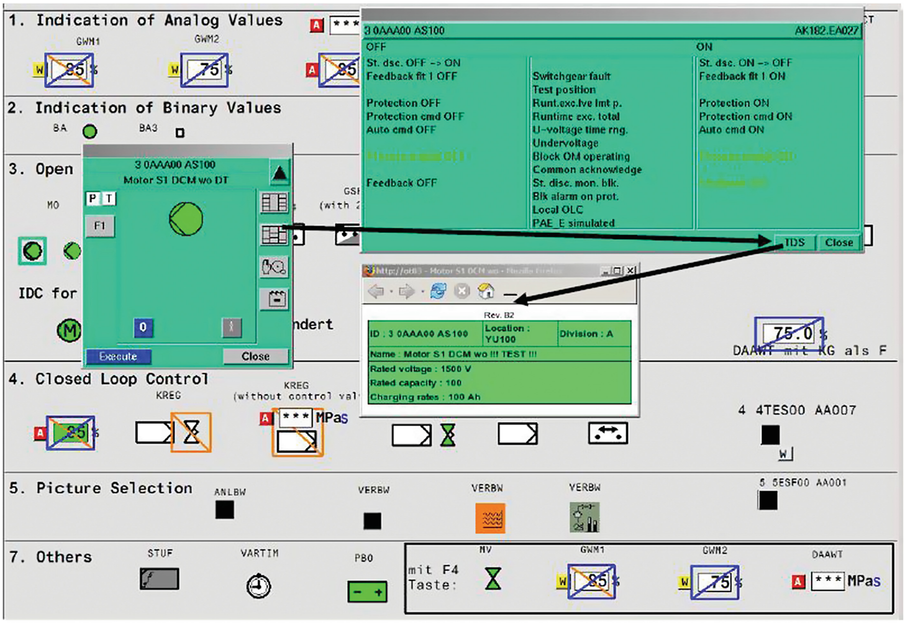
2.3.4 The Implementation and Improvement of HFE in Display Design

The HFE has been blended in each field of design of modern nuclear power plant, so the implementation of HFE principle should be taken as a formal part during display design period and design verification period.

After applicability analysis and discrimination of the HFE principles in Phase1, from meeting the requirements of 'to eliminate possible source of human failure' and 'to minimize possible human failure', the principle of display design adopted in Phase 1 is reasonable and applicable for Phase II. From the strong self-diagnosis function owed by

I&C hardware device, it is able to 'monitor and help correct mistakes before they influence power plant', but some aspects can be improved and implemented.

From the aspect of 'correctly support specified task to reduce the possibility of human failure', the one method is improved to adopt the text and electronic version in Phase II, it lacks normal, abnormal and accident operation procedure of electronic display. The link will be set in UI. after clicking the procedure list will be called and then search quickly to switch digitalized procedure. And the other is provided a function named 'Technical Data Sheet-TDS' (see Fig. 3), which is aimed at specific equipment to provide more detailed information in the form of dynamic window for operators. The information includes equipment operation parameters and technical data like specific location, acceptable scope, setting value and other specifications, due to the limitation of screen layout and MMI system, so some supportive information will be not directly shown on the screen.



3 0AAA00 AS100 AK182.EA027

OFF
St. dsc. OFF -> ON
Feedback flt 1 OFF
Protection OFF
Protection cmd OFF
Auto cmd OFF
Feedback OFF

Switchgear fault
Test position
Runt.exc.lve lmt p.
Runtime exc. total
U-voltage time rng.
Undervoltage
Block OM operating
Common acknowledge
St. disc. mon. blk.
Blk alarm on prot.
Local OLC
PAE_E simulated

ON
St. dsc. ON -> OFF
Feedback flt 1 ON
Protection ON
Protection cmd ON
Auto cmd ON

Rev. B2

ID : 3 0AAA00 AS100	Location : YU100	Division : A
Name : Motor S1 DCM wo !!! TEST !!!		
Rated voltage : 1500 V Rated capacity : 100 Charging rates : 100 Ah		

Fig. 3. TDS

3 Conclusions

In a word, the Phase I MMI design is basically able to provide the relatively fine, integrated, explicit and reader-friendly analysis and judgment information and also to ensure the safe, reliable and high-quality operation since commercial operation. Now with increasing NPP automation level and optimization of MMI of Phase II display, the MMI definitely will be improved better to produce huge potential benefits because it can not only provide operator with more requirement-met and more appropriate information, but also can support the operator with information search, status understanding, correct operation and decision-making to ease the burden on the operation and judgment of the operator and to reduce human failure.

Of course, with the improvement of the computer hardware/software and the accumulation of engineering experience, there will be room for gradual upgrade and improvement.

References

1. Advanced Light Water Reactor Utility Requirements Document (URD), vol. 2, Chap. 10, Revision 7
2. International Electrotechnical Commission. IEC 73: Basic and safety principles for man-machine interface, marking and identification - Coding principles for indication devices and actuators: 10 (1996)
3. International Electrotechnical Commission. IEC 964: Design for control rooms of nuclear power plants: 03 (1989)
4. SIEMENS Work Report. General description for the arrangement of video displays of the OM system for Tianwan NPP (2003)
5. International Electrotechnical Commission. IEC 61772: Nuclear Power Plants - Control Rooms - Application of Visual Display Units (VDUs) (2009)
6. Consortium technical report. HFE program for control room and HMI design (2013)

Study on I&C Safety Classification Method of Nuclear Power Plant

Tao Fu(✉), Xiang-Jie He, and Long-Qiang Zhang

State Key Laboratory of Nuclear Power Safety Monitoring Technology and Equipment,
China Nuclear Power Engineering Co., Ltd, Shenzhen 518172, China
futao@cgnpc.com.cn

Abstract. According to IAEA SSR 2/1, the instrumentation and control (I&C) systems which are important to safety, should be first identified and then classified on the basis of their function and significance with regard to safety in the design process of nuclear power plant. A clear logical safety classification method is very important to complete items classification. At present, there is no uniform requirement for the specific classification method. In this paper, a set of I&C safety classification method for nuclear power plants is studied from the perspective of safety function design, distribution, realization process and accident analysis and safety classification relationship, and the function classification process, the system classification process and the equipment classification process are described.

Keywords: I&C safety classification · Function design · Accident analysis

1 Introduction

There are 7 key phases, including site selection, design, construction, commissioning, operation, decommissioning and waste disposal through the cycle of nuclear power plant. There are numerous complex systems and equipment in the nuclear power plant. In order to realize the nuclear safety target of nuclear power plant, it is necessary to classify the I&C function, system and equipment according to the importance of the nuclear safety function and the different degree of sensitivity to the internal and external events. Reasonable safety classification can effectively ensure the safe and stable operation of nuclear power plants, reduce construction investment and in-service maintenance costs.

Safety classification is a systems engineering which is closely linked to the design of a nuclear power plant. All safety items are required to determine a reasonable class of safety to guide the design of the item. The nuclear power plant has a large number of items, and the design is complicated. It is impossible to complete the whole classification work by a small number of people, which is more obvious in the design of the new reactor. At the same time, classification work accompanies the entire nuclear power plant design process, and is existed even in the transformation of the operational nuclear power plants. Therefore, it is necessary to develop a classification method which is clear, logical, and highly operational to guide classification work to ensure that nuclear power

Y. Xu et al. (eds.), *Nuclear Power Plants: Innovative Technologies for Instrumentation and Control Systems*, Lecture Notes in Electrical Engineering 455,
https://doi.org/10.1007/978-981-10-7416-5_7

plant systems and equipment are classified under a unified standard system and the appropriate standards for design are selected.

2 Safety Classification Method

2.1 Factors to Consider in Safety Classification

All items important to safety should be identified and classified on the basis of their function and their safety significance.

The safety classification method shall take account of factors such as:

1. the safety function(s) to be performed by the item;
2. the consequences of failure to perform a safety function;
3. the frequency with which the item will be called upon to perform a safety function
4. the time following a postulated initiating event at which, or the period for which, the item will be called upon to perform a safety function.

The design should prevent any interference between items important to safety. Any failure in a lower safety class system will not propagate to a higher safety class system.

Equipment that performs multiple functions shall be classified in a safety class that is consistent with the most important function performed by the equipment.

The safety importance of each function of the instrumentation and control systems are determined by its role in achieving and maintaining the safety status of the nuclear power plant, the potential consequences of the failure to implement the function and the probability of generating such consequences. Therefore, the preliminary safety analysis including functionality, performance and reliability of a nuclear power plant should be completed before classification of instrumentation and control functions.

2.2 Relationship Between Functional Design Process and Safety Classification of Nuclear Power Plant

The safety classification is closely linked to the functional design of the nuclear power plant. All items important to safety need to determine a reasonable safety class to guide the design of the item. The classification work is accompanied with the whole design process including the transformation. It is necessary to comb the relationship between the safety classification and the functional design process to ensure that safety classification is under the standard system. Multi-level functions can be set to meet the basic principles of defense in depth in order to prevent unsafe conditions and mitigate the consequences of accident.

The fundamental objective of a nuclear power plant is to generate electricity safely and effectively, and protect the public from radiation hazards. The fundamental safety objectives are generally broken down into three fundamental safety functions:

1. control of reactivity;
2. removal of heat from the reactor;
3. confinement of radioactive material.

In most relevant standards and regulations, the safety classification is based on the three fundamental functions of nuclear power plants.

The general means of function design is that the following work is done after determining the specific type of the reactor:

1. break down the fundamental safety functions into specific plant safety functions;
2. assign specific plant safety functions to each system;
3. realize the function by each specific equipment action in the system.

The process of assigning the safety function to the system, and then determining the system safety function, and determining the equipments that perform the system safety function, is actually the process of identifying the items important to safety.

In the process of function design, it is necessary to identify the importance of function implemented by the equipment because the reliability of equipment need to be considered. The function is classified according to its importance. Then the system and equipment which implement the function are classified. Then the design and manufacture of the system and equipment is consistent with their importance, so that the equipment can implement the function according to the design requirements. Therefore, the safety classification process is closely related to the entire function design process. The relationship between the safety function design process and the safety classification of a nuclear power plant is given in Fig. 1.

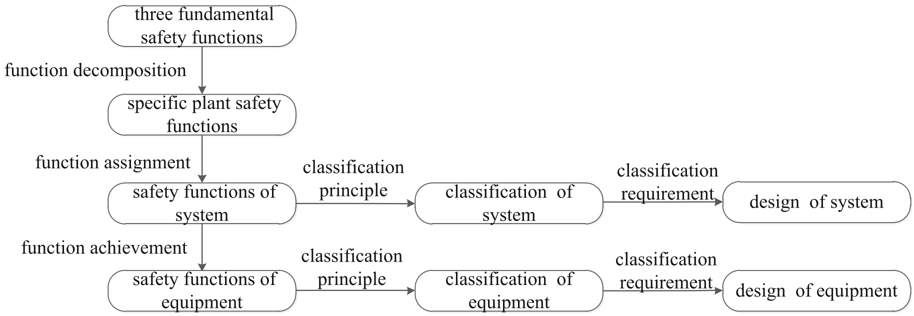
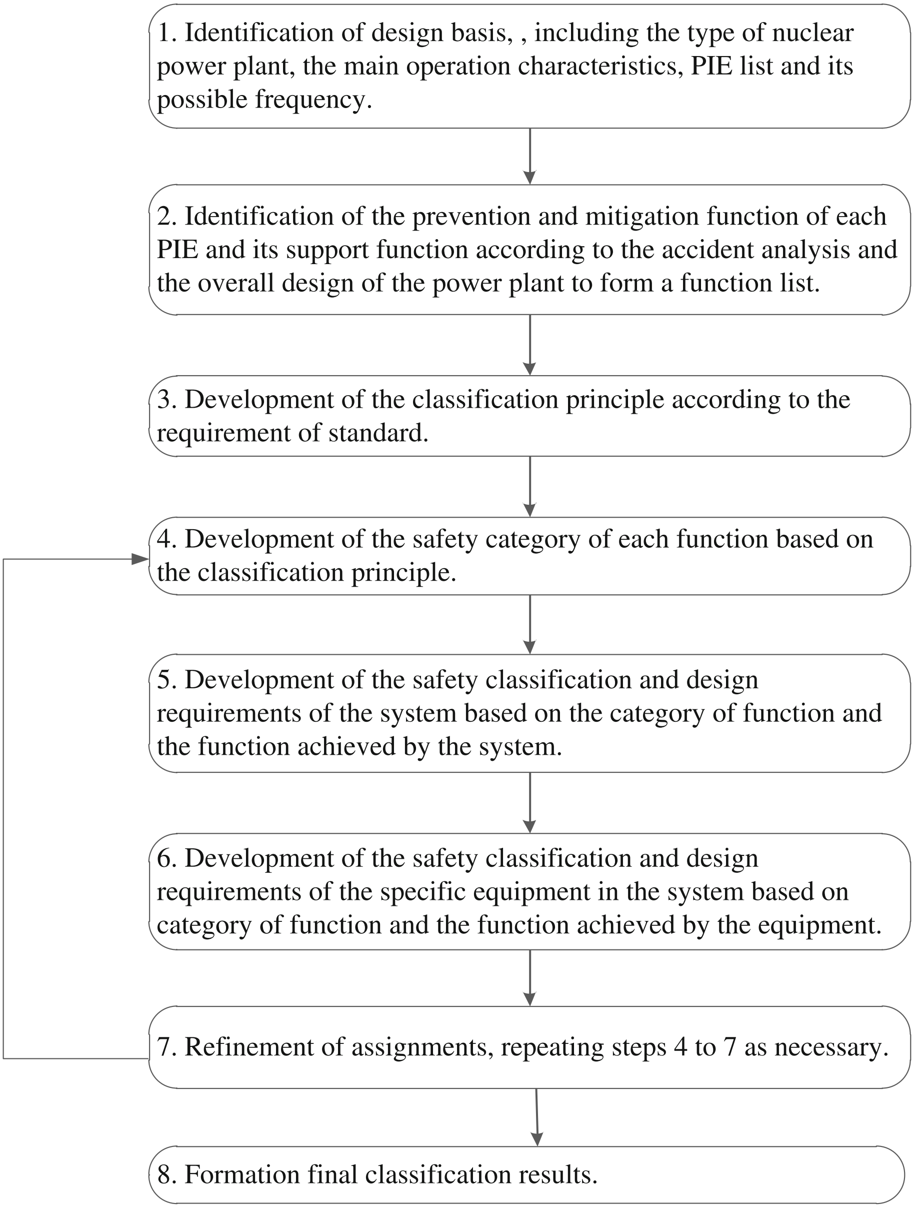

three fundamental safety functions
function decomposition
specific plant safety functions
function assignment
safety functions of system
classification principle
classification of system
classification requirement
design of system
function achievement
safety functions of equipment
classification principle
classification of equipment
classification requirement
design of equipment

Fig. 1. Relationship between the safety function design process and the safety classification

Figure 1 does not give a detailed description of the plant design process. It focuses on clarifying the relationship between the safety classification and the function design of the power plant. From this figure, we can see that the safety classification is based on the classification principle to classify the safety functions implemented by the system and equipment. At the same time, the results of the system function classification will also affect the design of the system and equipment.

2.3 Safety Classification Method

The work of safety classification requires a comprehensive understanding of power plant design, including power plant characteristics, operation modes, postulated initiating event (PIE) lists and its possible frequency, function lists which prevent and mitigate the PIE, etc. The accidents mitigation process is known by the safety analysis. The safety function performed in all operation conditions and the importance of safety function is determined by the safety analysis. Then the safety function is classified according to the classification principle. The items are classified according to the importance of the item



1. Identification of design basis, , including the type of nuclear power plant, the main operation characteristics, PIE list and its possible frequency.

2. Identification of the prevention and mitigation function of each PIE and its support function according to the accident analysis and the overall design of the power plant to form a function list.

3. Development of the classification principle according to the requirement of standard.

4. Development of the safety category of each function based on the classification principle.

5. Development of the safety classification and design requirements of the system based on the category of function and the function achieved by the system.

6. Development of the safety classification and design requirements of the specific equipment in the system based on category of function and the function achieved by the equipment.

7. Refinement of assignments, repeating steps 4 to 7 as necessary.

8. Formation final classification results.

Fig. 2. Safety classification method

in the implementation of the safety function. The safety classification method is given in Fig. 2.

If the results of item classification cannot satisfy the requirement of deterministic or probabilistic safety analysis, or classification list is not complete, the design and classification of the items need to be re-verified or adjusted until the list is complete and meet the requirement of deterministic and probabilistic safety analysis.

It is unlikely to determine all the details of the function in the preliminary design phase of a power plant and therefore the characteristics of a nuclear power plant cannot be determined completely. The design and classification of the function should be repeated throughout all the design phase. Remarks should be made where classification of functions is not clear. After the completion of safety analysis and operation procedures, the classification should be improved to form a final list.

2.4 Process of Classification

2.4.1 Function Classification Process

The classification of safety functions should be based on the various accidents analysis provided by the safety analysis report, and lists the main processes of the accidents. The boundary points of controlled state, safety shutdown state or final state of nuclear power plant is identified. The functions required to achieve these state and time intervals is identified. Then the safety function of the plant is classified according to the classification principle.

Taking an example of EPR, according to the final safety analysis report, the F1A classification applies to the safety function which is required to reach the controlled state and the associated support function after an internal DBC-2 to 4 event. The F1B classification applies to the safety function which is required after the controlled state in order to reach and maintain the safe shutdown state after an internal DBC-2 to 4 event. The F2 classification applies to safety function required to reach and maintain the final state for DEC-A event sequences and function required to prevent significant radiological discharges in DEC-B sequences.

The function should be classified in a safety class that is consistent with the most important function.

2.4.2 System Classification Process

The accident condition related to the system function should be identified first to determine the safety classification of the system. If it is found that there is no accident related to the system function, these functions of the system should be classified according to the application scope and failure consequence of the function based on the classification principle. If there is any accident related to the system function, the accident process shall be listed after the accident condition is identified. Then the analysis of the accident condition is carried out. The boundary points of the controllable state, safety shutdown state, or final state is identified. The phase of the accident sequence which the system function is used is identified. Then the system function is classified according to the classification principle. All the accident conditions related to the system function is analysed, and the safety class of this function is the highest class required for this function.

The safety class of all functions performed by the system is identified by the use of this method. The safety class of the system depends on the highest class of the function that is performed.

If a function performed by the system has been judged to be the highest safety class, for example F1A in EPR, it is not necessary to judge other functions. The system is F1A class system. Figure 3 shows the process of system classification.

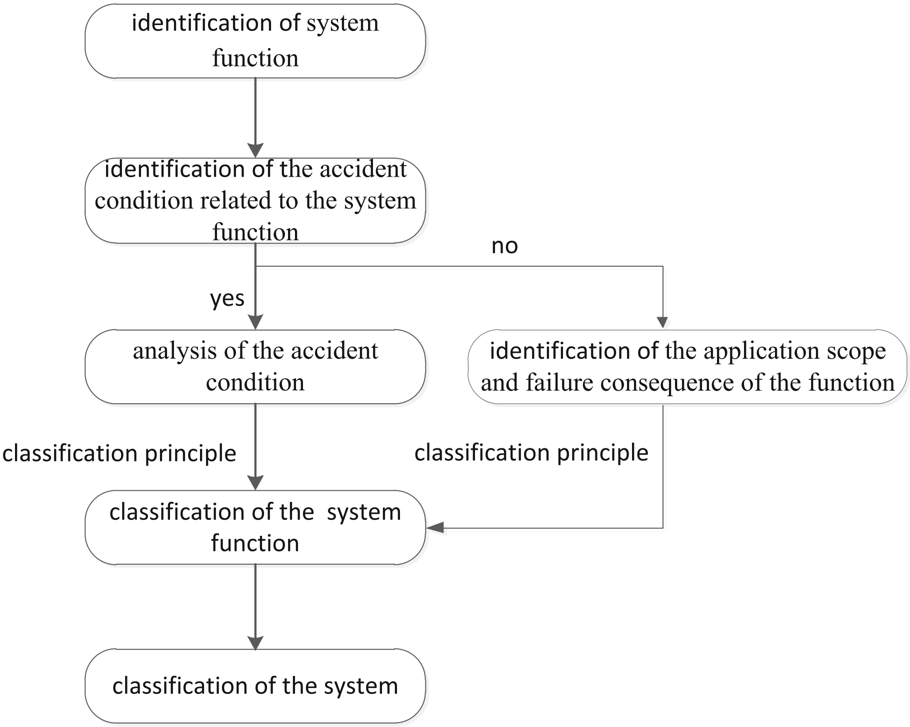

identification of system function
identification of the accident condition related to the system function
no
yes
analysis of the accident condition
identification of the application scope and failure consequence of the function
classification principle
classification principle
classification of the system function
classification of the system

Fig. 3. Process of system classification

2.4.3 Equipment Classification Process

First of all, it is necessary to determine whether the function performed by the equipment has been determined during the process of system classification to determine the safety classification of the equipment. If it have been already judged, it is not necessary to judge again. The safety class is consistent with the results obtained during the process of system classification. If no judgment has been made, the accident condition related to the function of the equipment is selected first. If it is found that there is no accident related to the function of equipment, these functions of the equipment should be classified according to the application scope and failure consequence of the function based on the classification principle. If there is any accident related to the function of the equipment, the analysis of the accident condition is carried out. The phase of the accident sequence which the function of the equipment is used is identified. Then the function of the equipment is classified according to the classification principle. All the accident conditions related to the e function of the equipment is analysed, and the safety class of this function is the highest class required for this function.

The safety class of all functions performed by the equipment is identified by the use of this method. The safety class of the equipment depends on the highest class of the function that is performed.

If the classification of one function performed by the equipment has been judged to be consistent with the system classification, it is not necessary to judge other functions. The safety class of the equipment is consistent with the system. Figure 4 shows the process of equipment classification.

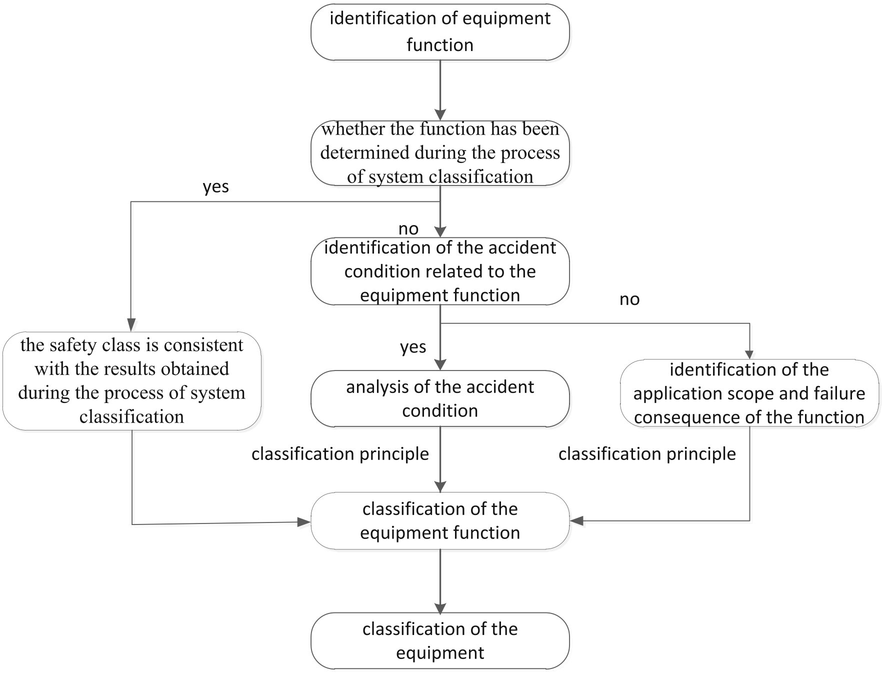

identification of equipment function
whether the function has been determined during the process of system classification
yes
no
identification of the accident condition related to the equipment function
no
yes
the safety class is consistent with the results obtained during the process of system classification
analysis of the accident condition
identification of the application scope and failure consequence of the function
classification principle
classification principle
classification of the equipment function
classification of the equipment

Fig. 4. Process of equipment classification

3 Conclusion

Safety classification is the basic task of design work of nuclear power plant. The classification of items depends on the safety function and importance. This paper presents a systematic method to safety classification and classification procedures for nuclear power plants. The safety classification is combined with function design and accident analysis. The safety classification of the system and equipment is gradually determined according to the role of the system and equipment in the accident process.

The safety Classification Method present by this paper can be used in the design of new nuclear power plants to identify the classification of function, system equipment and to guide the design of systems and equipment.

References

1. ANS 51.1: Nuclear safety criteria for the design of stationary pressurized water reactor plants (1983)
2. ANS 58.14: Safety and pressure integrity classification criteria for light water reactors (2011)
3. IAEA SSG-30: Safety classification of structures, systems and components in nuclear power plants (2014)
4. IAEA SSR 2/1: Safety of nuclear power plants: design (2012)
5. IEC 61226: Nuclear power plants –Instrumentation and control important to safety – Classification of instrumentation and control functions (2009)
6. RG1.201: Guidelines for categorizing structures, system, and components in nuclear power plant according to their safety significance (2006)

The Optimization of Valve Control Strategy for Valve Periodic Test in Nuclear Power Plant

Xiao-Lei Zhan(✉), Yan Liu, and Bin Zeng

State Key Laboratory of Nuclear Power Safety Monitoring Technology and Equipment,
China Nuclear Power Engineering Co., Ltd., Shenzhen 518172, China
zhanxiaolei@cgnpc.com.cn

Abstract. Periodic test can check the time of valve opening and closing, and prevent valve jamming, which impacts the safety and economy of nuclear-power plant directly. For solving the problem of the greater load fluctuation, the control principle of the steam control-valve and the scheme of the valve periodic test are researched. The reason of greater load fluctuation is analysed. An optimization of valve control strategy is provided and introduced. Finally the optimization scheme is verified during field valve test. The field test result indicates that load fluctuation has been greatly reduced during valve periodic test and the total valve test time is greatly shortened, so the nuclear power plant can return to rated power ahead of time. The optimization greatly enhances the safety and economy of nuclear power plant. The optimization scheme mentioned can also provide reference for other turbine units.

Keywords: Periodic test · Nuclear power · Load fluctuation · Optimization
Time shorten

1 Preface

The speed regulation system plays an important role in turbine speed-load control and ensures the safety, stability and economy of nuclear power plant. During normal operation, the opening of the steam valves is changed to change the amount of steam into the cylinder, thereby to change the speed-load control [1]. So in order to ensure the stability of speed-load control in nuclear power plant, the steam valves are required to active smoothly with no jam, and should be closed quickly in case of crisis of the turbine unit [2].

Valve periodic test is an important guarantee for long term stable and reliable operation of the steam emergency stop valves and steam control-valves of turbine unit in the nuclear power plant. It's an important way to prevent the valve jamming and prevent turbine unit over-speed or even runaway accident [3]. National standard and regulation and industry standard require that the valve periodic test should be executed during normal operation of the turbine unit, and no greater disturbance occurs during online valve periodic test under the specified power condition [4]. How to reduce the greater load fluctuation and shorten the test time are the important indications to evaluate the

Y. Xu et al. (eds.), *Nuclear Power Plants: Innovative Technologies for Instrumentation and Control Systems*, Lecture Notes in Electrical Engineering 455,
https://doi.org/10.1007/978-981-10-7416-5_8

valve periodic test [5]. The valve control strategy is analyzed and the optimization scheme is provided to ensure the safety and economy of the nuclear power plant.

During the valve periodic test at 80% rated power platform in nuclear power plant unit 1, there is a load fluctuation of −33.5 MW during NO.3 HPCV closing, which has exceeds the acceptance criteria. And the load fluctuations of the other 3 HP control-valves are all about −30 MW. Although the value doesn't exceed the standard, but with the continuous operation of the turbine unit, the valves condition gets worse. There is a risk that the load fluctuation may exceed acceptance criteria, so analysis and optimization of the valve control strategy must be supplied to ensure the stability of the turbine unit.

2 Valve Periodic Test Scheme and Control Principle

The half-speed steam turbine of SIEMENS is adopted in a CPR1000 nuclear power plant and the rated power is 1086 MW. Valve periodic test logic design adopts the sequential control based on the concept of "one button start" by SIEMENS. The turbine unit is equipped with 1 high pressure cylinder and 2 low pressure cylinders. The high pressure cylinder has 4 high pressure valve-groups (each group contains 1 high pressure emergency stop valve (HPESV) and 1 high pressure control valve (HPCV)). Each of the 2 low pressure cylinders has 2 low pressure valve-groups (each group contains 1 low pressure emergency stop valve (LPESV) and 1 low pressure control valve (LPCV)). The hydraulic actuator accepts the control signal from turbine governing system and turbine protection system to drive the emergency stop valves and control valves. Valve periodic test in the mentioned nuclear power plant shall be carried out below 85% rated power every 4 weeks, and the load fluctuation shall be less than 3% rated power.

2.1 Control Principle of the Steam Control-Valve

The Control-valve module contains one electro-hydraulic servo valve, two trip solenoid valves and one hydraulic actuator. The valve position controller is proportional and it controls the servo valve coils through voltage-current converter. In order to increase reliability, the two coils are controlled separately by separate voltage-current converter. The valve close-loop control is achieved by the deviation between the control set-point and the actual valve position during normal condition. When turbine trip, the trip solenoid valve is de-energized, the control valve closes quickly [6]. The control principle of the control-valve is shown in Fig. 1 as below.

During normal operation, ***Vspl-d*** = ***Vspl*** = 103%, the valves are controlled by valve control set-point controller, ***Vspc*** is calculated through steam demand set-point *OSB.* During valve periodic test and other special condition, reducing ***Vspl*** until ***Vspl-d*** < ***Vspc,*** Valves are controlled by valve limit set-point controller. The valve limit set-point controller is proportional, ***Vspl-d*** tracks ***Vspl*** by a certain gradient, the higher the gradient absolute value is, the sooner ***Vspl-d*** arrives at ***Vspl,*** so the control-valves move faster. However, the rapid action of the control valve will lead to a sudden change in the amount of steam entering the cylinder, which may result in greater load fluctuation.

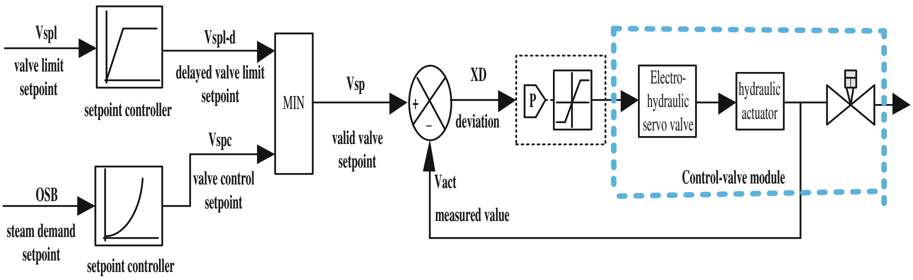


Fig. 1. The control principle of the control-valve

2.2 Scheme of the Valve Periodic Test

Valve periodic test is performed by groups. Each group tests an emergency stop valve and a control valve, verifying whether the time of valve opening and closing can meet the acceptance criteria or not. It can also prevent valve jamming and over-speed during load rejection. Sequential control method is adopted in the logic design for valve periodic

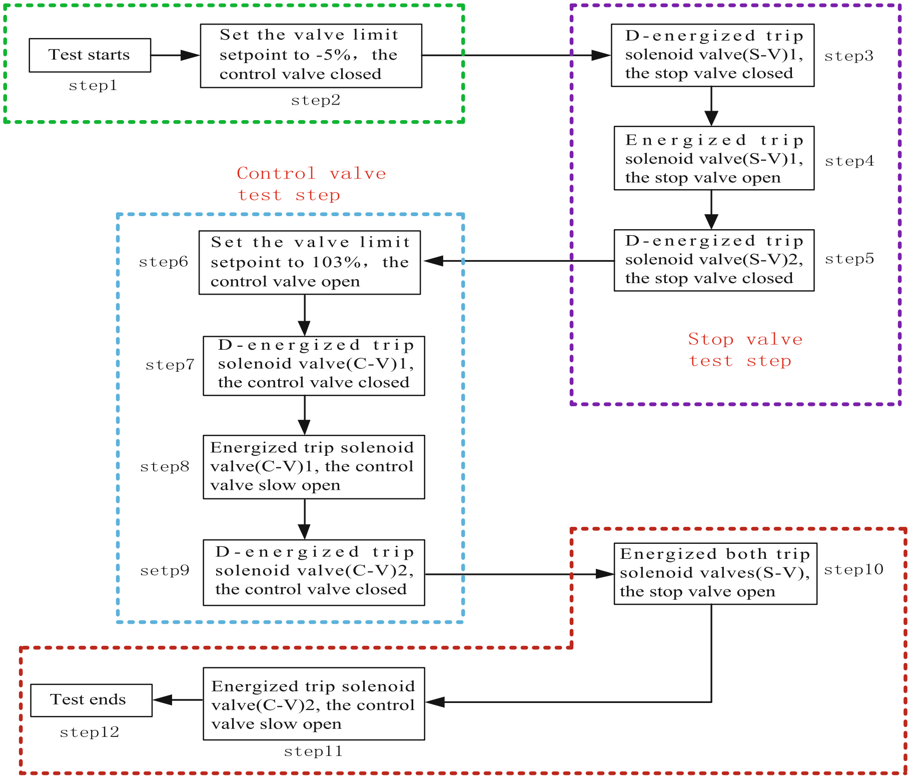

Test starts
step1
Set the valve limit setpoint to -5%, the control valve closed
step2
D-energized trip solenoid valve(S-V)1, the stop valve closed
step3
Energized trip solenoid valve(S-V)1, the stop valve open
step4
D-energized trip solenoid valve(S-V)2, the stop valve closed
step5
Stop valve test step
Control valve test step
step6
Set the valve limit setpoint to 103%, the control valve open
step7
D-energized trip solenoid valve(C-V)1, the control valve closed
step8
Energized trip solenoid valve(C-V)1, the control valve slow open
setp9
D-energized trip solenoid valve(C-V)2, the control valve closed
Energized both trip solenoid valves(S-V), the stop valve open
step10
Energized trip solenoid valve(C-V)2, the control valve slow open
step11
Test ends
step12

Fig. 2. Step diagram of the sequential control

test, performing all valve tests group by group. The step diagram of the sequential control is shown in Fig. 2 as above.

Valve periodic test steps are described as follows:

Item 1: Test preparing, from step1to step2. Setting $Vspl = -5\%$, and then the control-valve is totally closed.

Item 2: Test executing, from step3 to step9.Control-valve keeps closed, verifying closing time of the emergency stop valve (from step3 to step5). Emergency stop valve keeps closed, verifying closing time of the control-valve(from step6 to step9).

Item 3: Recovery, from step10 to step12. Energizing both two trip solenoid valves and the emergency stop valve is open. Setting $Vspl = 103\%$, and then the control-valve is open, so the turbine unit returns to its original condition.

3 Optimization of the Valve Control Strategy

3.1 Analysis of Load Fluctuation

Greater load fluctuation can also leads to frequent operation of control rods of nuclear island and affect the safety of nuclear island. Load fluctuation can be solved directly by modifying the curve of control valve. While the curve of control valve is decided by comprehensive factors of turbine power, pressure and steam demand during valve manufacture. Modification of the curve of control valve should be test by long time factory test to verify whether affecting the turbine performance, which is impossible in the existing circumstances. So it has to analyze and optimize the procedure of periodic test to reduce the greater load fluctuation. The detailed reason of load fluctuation during periodic test is shown as follows.

Item 1: The selection of the proportion coefficient P for the servo valve is unreasonable. It can be seen in Fig. 1 that the larger coefficient P will result in the greater overshoot.

Item 2: Valve limit set-point controller is unreasonable. It can be seen in Fig. 2 that from step3 to step10 no steam entering the cylinder, so no load fluctuation can be produced. While at step2 the control-valve is controlled by valve limit set-point controller, the control-valve closes too fast and exceeds the response speed of other valves opening, resulting in greater load fluctuation. The opening procedure of control-valve at step11 is the same.

3.2 Optimization of the Valve Limit Set-Point Controller

The valve limit set-point controller is a proportional controller. The curve for step2 control-valve closing is shown in Fig. 3 as follows.

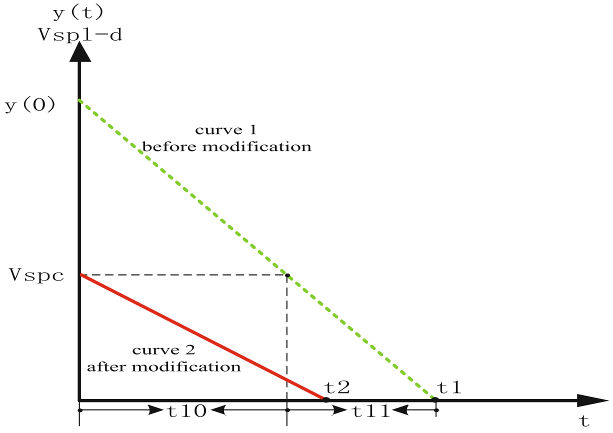


Fig. 3. The curve of valve limit set-point controller during valve closing

Curve 1 is before optimization. t10 is the waiting time, t11 is actual closing time, t1 is the total time and t1 = t10 + t11 and curve 1 can be described by the following function.

$$y(t) = y(0) - (100\% * \boldsymbol{Vspc/T}) * t \tag{1}$$

In which:

$$y(t) = \boldsymbol{Vspl} - d; y(0) = \boldsymbol{Vspl};$$

T is the total time during which the valve position from 0% to 100% or from 100% to 0%.

It can be seen from curve 1 that the bigger parameter *T*, the slower the control-valve closes and the smaller the load fluctuation is. It also can be got that there is no action of the control-valve within time t10.Time t10 has no contribution to valve closing and extends the total time of the test. Long term operation under the lower power is adverse to the safety of the nuclear island and the economy of the turbine unit is also reduced. Therefor it's necessary to shorten or cancel the waiting time t10. So a register is designed to force ***Vspl**-d to* the actual valve value(the actual valve value is equal to ***Vspc***) at that time when the valve closing order is coming. Curve 2 is after optimization, t2 is both the total time and the actual closing time. And curve 2 can be described by the following function.

$$y(t) = \boldsymbol{Vspc} - (100\% * \boldsymbol{Vspc/T}) * t \tag{2}$$

In curve 2, the extending of the actual time reduces the load fluctuation and the canceling of the waiting time shortens the total test time. The time of control-valve opening is the same as closing, so the curve for step11 control-valve opening is shown in Fig. 4 as follows.

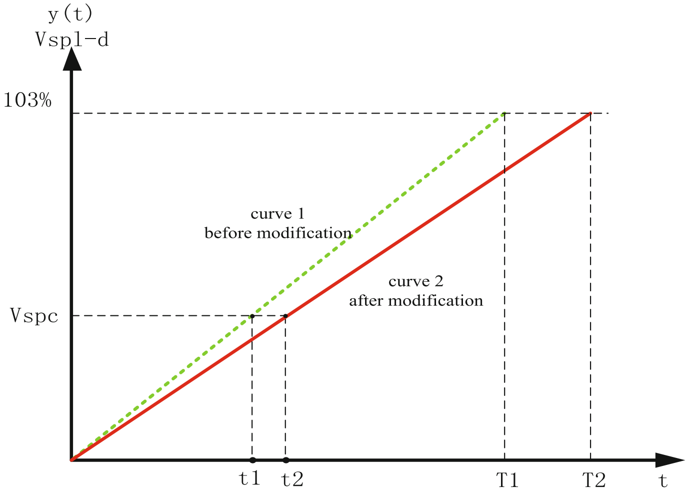


Fig. 4. The curve of valve limit set-point controller during valve opening

3.3 Field Data Base on Optimization

The optimization scheme is proved to be correct and feasible through field commissioning. The proportion coefficient P is set at 20, Time *T* is set at 120 s after optimization without the waiting time. Before modification, *T* is 77 s, which contains both the waiting time and the valve action time. The time 77 s is too short, the greater load fluctuation occurred, finally modifying time T from 77 s to 120 s through analysis and field commissioning. The scheme after optimization reduces load fluctuation about by 50%, the total test time is shortened about 15.3 min from 1901.9 s to 984 s(the total test time is consisted with the valve closing total time of the four HPCVs and the valve opening time of the four HPCVs). The formula of the total test time is as follows:

$$\text{Before modification: } (396.55 * 4) + (77 * 3 + 84.7) = 1901.9\,(\text{s}).$$

$$\text{After modification: } (120 * 3 + 132) + (120 * 3 + 132) = 1901.9\,(\text{s}).$$

The detailed date during the valve periodic test at 80% rated power platform is as follows (Tables 1 and 2).

Table 1. Load fluctuation during HPCV test at 80% rated power

Max load fluctuation (MW)		HPCV1	HPCV2	HPCV3	HPCV4
During valve closing	Before modification	−29	−30	−33.5	−30
	After modification	−16	−16	−17	−15
During valve opening	Before modification	21	19	21	20
	After modification	12	12	13	11

Table 2. Time of valve periodic test at 80% rated power

Test time (s)		HPCV1	HPCV2	HPCV3	HPCV4
Valve closing actual time	Before modification	77	77	84.7	77
	After modification	120	120	132	120
Valve closing total time	Before modification	396.55	396.55	396.55	396.55
	After modification	120	120	132	120
Valve opening time	Before modification	77	77	84.7	77
	After modification	120	120	132	120

4 Conclusion

An optimization scheme is provided for valve periodic test after researching the control strategy of the control-valve. The optimization scheme is proved to be correct and feasible through field commissioning. The load fluctuation is greatly reduced and the total test time is also shortened. As a result, the turbine unit can return to the rated power ahead of time, increasing electric energy and enhancing the safety and reliability of the nuclear power plant. The optimization scheme mentioned can also provide reference for other turbine units.

References

1. Ma, C.L., Wang, Y.M., Jiao, K.: Turbine valve test logic perfection. Northeast Electr. Power Technol. **36**(1), 44–46 (2015)
2. Dong, W., Huang, M.H., Zeng, B.: Study on the valve position fluctuation of turbine main regulator valve in nuclear power plant. Process Autom. Instrum. **36**(11), 50–52 (2015)
3. Xia, W.: Comprehensive optimization measures for unilateral joint valve activity test of high pressure total valve-governing valve of 600 MW supercritical steam turbine. Guangdong Electr. Power **27**(5), 23–27 (2014)
4. Specification of instrumentation and control for turbine in nuclear power plant. NB/T 25019 (2014)
5. Zeng, B., Zhan, X.L., Zhang, C.: Analysis and research on the standardized design of turbine control system in nuclear power plant. Process Autom. Instrum. **36**(11), 36–40 (2015)
6. Sun, X.L., Zhao, S.Y.: Commissioning test of stop valve and control valve for semi-speed steam turbine in 1119 MW nuclear power plant. Electr. Power Constr. **34**(5), 62–65 (2013)

Transient Detection and Identification for HTR-PM Based on Principle Component Analysis

Shu-Qiao Zhou(✉), Chao Guo, and Xiao-Jin Huang

Institute of Nuclear and New Energy Technology, Collaborative Innovation
Centre of Advanced Nuclear Energy Technology, Key Laboratory of Advanced
Reactor Engineering and Safety of Ministry of Education, Tsinghua University,
Beijing, China
{zhousq, guochao, huangxj}@tsinghua.edu.cn

Abstract. For the sake of enhancing safety and achieving more economic benefits, it is very important to timely detect and identify the transients during the operation of nuclear power plants. There are thousands of monitoring signals in a nuclear power plant. It is unfeasible to detect the transients by monitoring all the related signals individually, as the thresholds for a large number of signals are hard to be determined one by one. Also, there might be too many alarms happening simultaneously when a transient occurs. In this case, the operators are hard to make a right judgment about what has happened. In this paper, a method based on principal component analysis (PCA) and T^2 statistic is proposed to detect the transients and the contribution plot is applied to identify the variables relevant to the transients. At last, the proposed method is applied with the sampling data from the simulator of High Temperature gas-cooled Reactor Pebble-bed Module (HTR-PM). The results from the application demonstrate that the proposed method is capable to detect the faults and identify the most relevant variables timely and correctly.

Keywords: Transient detection · Transient identification
Principal component analysis · Contribution plot

1 Introduction

Nuclear power plants are complex systems, as they contain many kinds of devices and relevant processes. Compared with other industrial systems, safety is especially important for nuclear power plants. Several operators are assigned and the monitoring systems are designed to supervise the whole plant [1]. It is the first step to identify what kind of abnormal event was happening, as the operators can make the proper decision only if they have determined what was happening [2, 3]. Moreover, when an abnormal event has happened and turned to be an accident, the number of parameters of the systems and alarms might be too big to be dealt with timely [4, 5]. Thus, it is very important and beneficial to detect and identify the abnormal events before they turn into accidents.

Y. Xu et al. (eds.), *Nuclear Power Plants: Innovative Technologies for Instrumentation and Control Systems*, Lecture Notes in Electrical Engineering 455,
https://doi.org/10.1007/978-981-10-7416-5_9

In a nuclear power plant, there are thousands of measured variables from field devices (i.e. sensors, valves and pumps) and variables synthesized by the controlling stations for the process control. If we only individually monitor the variables for detecting the faults, the number of the signals will be too large and so many simultaneous alarms will be too confusing to let the operators know what is happening when a transient occurs [6]. Moreover, individually monitoring the variables may leave out some variables that responsible for the faults and the correlations among the variables are not considered. In this paper, we propose a method to use PCA-based T^2 statistic to detect the faults. Moreover, the contribution plots [7, 8] are applied to identify the variables most relevant to the faults.

In the remainder of this paper, we first introduce how to use the PCA-based T^2 statistic to detect the faults. Then the contribution plots and their application in identification the relevant variables are described in Sect. 3. In Sect. 4, the proposed methods are verified by sample data from the plant simulator of HTR-PM [9]. At last, we draw a conclusion in Sect. 5.

2 Fault Detection Based on Principle Component Analysis and T^2 Statistic

In many situations, faults are detected by monitoring measured variables individually. However, since there are a large number of measured variables in a nuclear power plant, it is not feasible to monitor all these variables individually and is not easy to determine more suitable variables to be used for fault detection. Moreover, if a plenty of variables are monitored individually and the alarms happen simultaneously, operators will be confused and feel hard to determine which alarm is the most relevant to the fault. Thus, it is necessary to pick up the main components among the variables first. In this section, how to select the principle components from the measured variables by PCA is first addressed. Based on PCA, the correlations among the process variables are also considered. Then based on the principle components, the T^2 statistic is introduced to detect the faults.

2.1 Feature Selection Based on PCA

Suppose there are m sensors used to monitor the running state of the plant, at time t, a sample $v(t) = [v_1(t), v_2(t), \cdots, v_m(t)]$ can be obtained by these m sensors. Suppose n $(n > m)$ samples are selected to be considered for each specific transient, the matrix of the samples can be obtained as

$$X = \begin{bmatrix} v(1) \\ v(2) \\ \vdots \\ v(n) \end{bmatrix} = \begin{bmatrix} v_1(1) & v_2(1) & \cdots & v_m(1) \\ v_1(2) & v_2(2) & \cdots & v_m(2) \\ \vdots & \vdots & \ddots & \vdots \\ v_1(n) & v_2(n) & \cdots & v_m(n) \end{bmatrix} \in R^{n \times m}. \tag{1}$$

In X, each column represents the measures of a state variable at different n time points and each row denotes a sample of m variables at a time.

The covariance of variables can be calculated as

$$C = \frac{1}{n-1} X^T X. \tag{2}$$

By using eigenvalue decomposition, the results can be obtained as follows.

$$\begin{aligned} \Lambda &= V^T C V \\ &= \begin{pmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & \cdots & \lambda_m \end{pmatrix}. \end{aligned} \tag{3}$$

The values $\lambda_1, \lambda_2, \cdots, \lambda_m$ ($\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_m$) are eigenvalues of C. Accordingly, the singular values of X can be denoted by $\sigma_1, \sigma_2, \cdots, \sigma_m$ and the relationships between σ_i and λ_i are $\lambda_i = \sigma_i^2, i \in [1, m]$. The columns in V are the eigenvectors related to $\lambda_i, i \in [1, m]$. Suppose the first a ($a < m$) column of V can be selected to form a new matrix P. Then, P can be used as a projection matrix to select the principal components of X.

2.2 Fault Detection Based on the T^2 Statistic

The current measured values of the variables can be denoted as a vector of $x = [x_1, x_2, \cdots, x_m]^T$ (i.e. the measured values at the time t: $x = v(t)^T = [v_1(t), v_2(t), \cdots, v_m(t)]^T$), combining with the projection matrix P. The T^2 statistic can be calculated as

$$T^2 = x^T P \Lambda_a^{-1} P^T x, \tag{4}$$

where, Λ_a contains the first a rows and columns of Λ. The threshold of T^2 statistic can be obtained by

$$T_\alpha^2 = \frac{a(n-1)(n+1)}{n(n-a)} F_\alpha(a, n-a). \tag{5}$$

In (5), F_α represents the F distribution and α is assigned to be 0.05 in this paper. The T^2 statistic reflects the systematic variations of the process and a fault can be represented by the state that the value of T^2 statistic crosses the threshold.

3 Fault Identification Based on Contribution Plots

Once a fault has been detected, the next important step is to determine what has caused this fault. In a nuclear power plant, usually the process is highly integrated and the number of monitoring variables is large. Thus, it is difficult and challenging to find out what happened correctly and timely. In this section, based on the calculations of T^2 statistic, the contribution plots are used to determine which measured variables are most relevant to the current fault. By focusing on these more relevant variables, the plant operators can get the hints to determine what has happened easier. By the assistance of this fault identification process, the time for the plant operators to know the cause of the fault and then recover the system can be significantly reduced.

The variables responsible for the fault can be prioritized by the total contribution values $CONT_j$. In this case, the plant operators can just focus on the variables with high $CONT_j$ values and then make rational judgments more immediately.

Algorithm 1. The steps for calculating contributions

```
1: Calculate the value of the current observation $x$ after the projection by $P$: $t_i = x^T p_i, i \in [1, a]$, where $p_i$ is the $i^{\text{th}}$ loading vector of $P$. $t_i, i \in [1, a]$ are called scores.
2: Normalize the scores by $\left( t_i / \sigma_i \right)^2$.
3: If $\left( t_i / \sigma_i \right)^2 > \frac{1}{a}\left( T_\alpha^2 \right)$, calculate the contribution of each variable $x_j$ as follows: $cont_{i,j} = \frac{t_i}{\sigma_i^2} p_{i,j} \left( x_j - \mu_j \right)$, where $p_{i,j}$ is the $(i, j)^{th}$ element of the projection matrix $P$. If $\left( t_i / \sigma_i \right)^2 \le \frac{1}{a}\left( T_\alpha^2 \right)$, $cont_{i,j} = 0$.
4: Set $cont_{i,j}$ to be 0 when $cont_{i,j}$ is negative.
5: Calculate the total contribution of the $j^{\text{th}}$ process variable $x_j$:
       $$CONT_j = \sum_{i=1}^{a} \left( cont_{i,j} \right).$$
6: Plot $CONT_j$ for all $m$ variables on a single graph.
```

4 Application of the Methods

This section describes the application of PCA-based T^2 statistic and contribution plots to HTR-PM. As Table 1 shows, the normal state and two typical transients related to the postulated accidents in HTR-PM are selected to verify the methods described above. These two transients are key events related to the safety of the reactor and the whole power plant.

Table 1. Normal status and two typical transients of HTR-PM

Transients	Name
T_1	Normal status
T_2	Control rod ejection accident
T_3	Water ingress accident (p1) with relief-pressure failure

There are many state variables related to these transients while only four relevant state variables are chosen here: helium flow, reactor heat power, inlet helium temperature and outlet helium temperature. The data of these transients are from the plant simulator, since HTR-PM is still under construction.

The sample data of T_1 is used to form the matrix in (1). The sample data of T_2 and T_3 are used as testing data.

During the simulation, it is supposed that the data from the sensors are sampled with an interval of 1 s and the total simulation time period is 200 s. In the beginning, the plant works in normal state and the transients happen at 50 s. Accordingly, the related parameters referred above are: $n = 200$, $m = 4$. The curves of the variables are shown in Fig. 1.

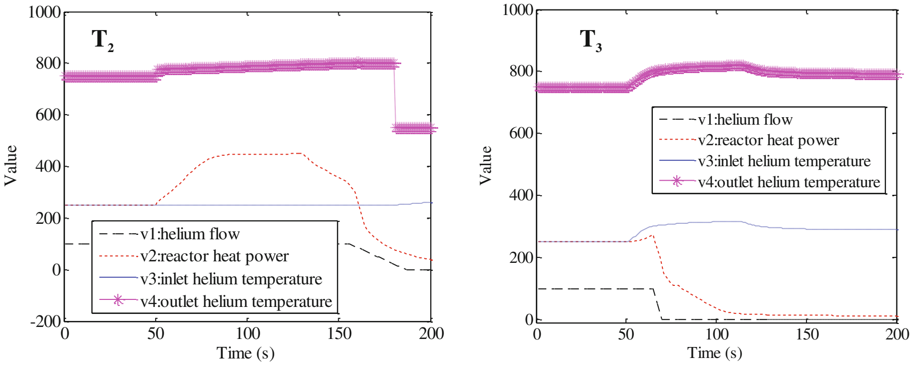


Fig. 1. Values of measured variables from the sample data (T_2 and T_3)

4.1 Application of T^2 Statistic to Detect the Fault

The T^2 statistic can be calculated based on the formula (4) and the related threshold can be obtained by (5). The key parameter a can be determined by the values of the singular values of C. As Fig. 2 shows, there is only one principle component in C, thus the parameter a can be chosen to be 2 according to the experience about using the T^2 statistic.

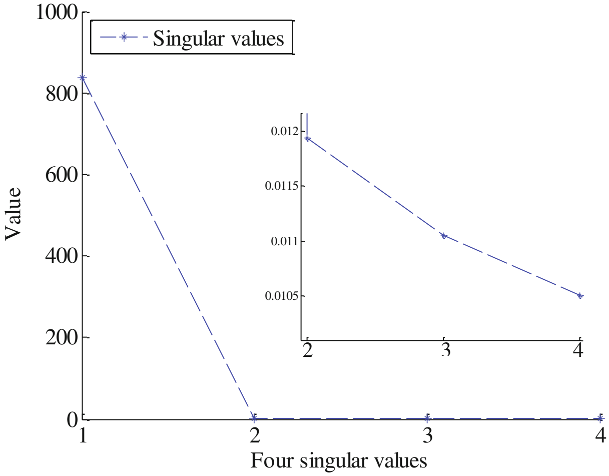


Fig. 2. Singular values of sample-data matrix *X*

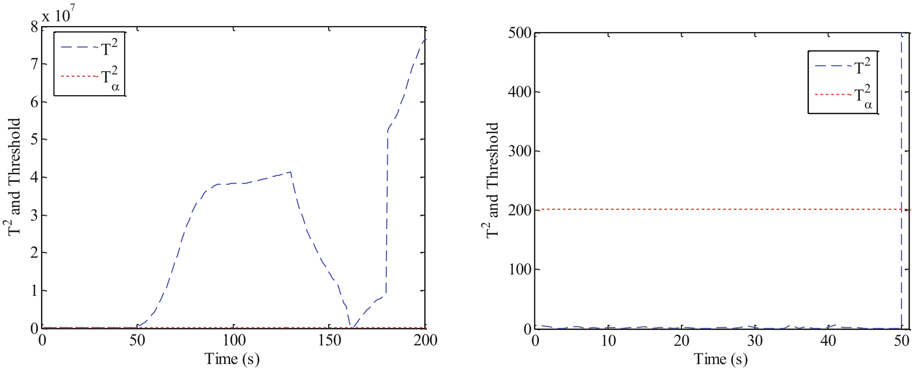


Fig. 3. The results of T^2 statistics and their related thresholds for transient T_2

For the transients of T_2 and T_3, the results of the calculations of T^2 statistic are shown in Figs. 3 and 4, respectively. The right sub-figures in Figs. 3 and 4 are the results of calculations from 1 s to 51 s, which are the same as that of left sub-figures. However, the results in the right sub-figures are zoomed to be clearer to show the relationships between the T^2 statistics and the related threshold. By comparing the results of T^2 statistic and the threshold, we can see that: (1) during the first 50 s, the values of T^2 statistic are lower than the threshold; and (2) the transients T_2 and T_3 can be timely detected right after their happening.

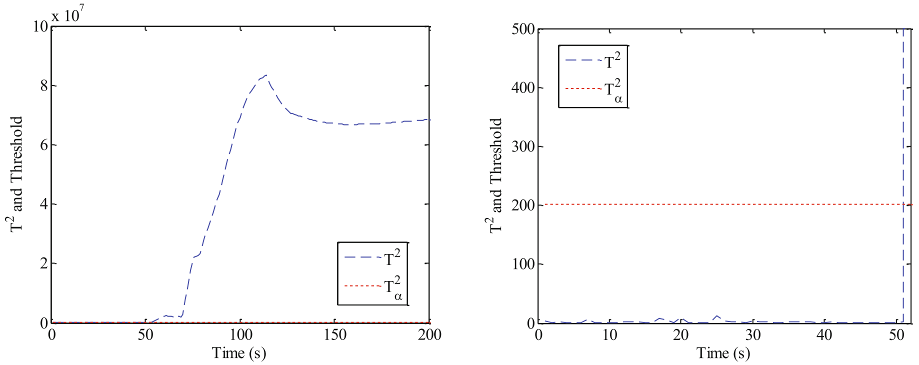


Fig. 4. The results of T^2 statistics and their related thresholds for transient T_3

4.2 Application of Contribution Plots

The contributions of each measured variable can be computed according to Algorithm 1. The results are shown in Fig. 5, in which the colour depth represents contributions.

According to the left sub-figure in Fig. 5, which is for the transient T_2, the most significant two variables are v_2 and v_4. These results meet the fact shown in Fig. 1, in which the variables reactor heat power (v_2) and outlet helium temperature (v_4) fluctuate most. The variable v_3 provides almost no contribution compared to that of other three variables. Accordingly, the inlet helium temperature (v_3) is almost stable in Fig. 1.

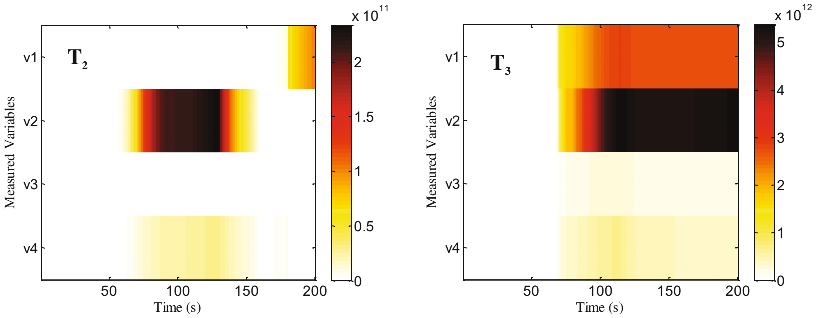


Fig. 5. The contribution plots of transient T_2 and T_3

For the transient T_3, the variable v_2 provides the most contributions. The variable v_1 provides less contributions and the variable v_3 provides the minimal contributions. These results also meet the fact shown in the right sub-figure of Fig. 1.

Based on the contribution plots, more significant variables can be selected. The plant operators can pay more attention to these key variables and ignore the less important ones, which helps to make the decision about the fault identification more rapidly and correctly.

5 Conclusion

For supporting the operators to make the judgements timely and correctly, related transient detection and identification techniques are very important and beneficial. In this paper, how to apply PCA-base T^2 statistic and contribution plot for the transient detection and identification for a nuclear power plant are introduced. The proposed methods are verified by the sample data from the simulator of HTR-PM. The results from the verification demonstrate that the proposed methods are capable to detect the fault timely and identify the relevant variables correctly.

Acknowledgments. This work has been supported by the Tsinghua University Initiative Scientific Research Program (Grant No. 20151080382 and no. 20151080380) and National Natural Science Foundation of China (Grant No. 71401169).

References

1. Jia, Q., Huang, X., Zhang, L.: Operation of shared systems via a common control system in a multi-modular plant. Sci. Technol. Nuclear Install. **2014**, 1–9 (2014)
2. Ma, J., Jiang, J.: Applications of fault detection and diagnosis methods in nuclear power plants: a review. Prog. Nucl. Energy **53**(3), 255–266 (2011)
3. Jun, L.S., Poong-Hyun, S.: Design of an integrated operator support system for advanced NPP MCRs: issues and perspectives. Nucl. Saf. Simul. **1**(4), 348–365 (2010)
4. Roverso, D.: Plant diagnostics by transient classification: The ALADDIN approach. Int. J. Intell. Syst. **17**(8), 767–790 (2002)
5. Na, M.G., Shin, S.H., Lee, S.M., et al.: Prediction of major transient scenarios for severe accidents of nuclear power plants. IEEE Trans. Nucl. Sci. **51**(2), 313–321 (2015)
6. Chang, Y., Huang, X., Hao, Y., et al.: Linear representation and sparse solution for transient identification in nuclear power plants. IEEE Trans. Nucl. Sci. **60**(1), 319–327 (2013)
7. Chiang, L.H., Russell, E.L., Braatz, R.D.: Fault Detection and Diagnosis in Industrial Systems. Springer, New York (2002)
8. Jiang, B., Huang, D., Zhu, X., et al.: Canonical variate analysis-based contributions for fault identification. J. Process Control **26**(2015), 17–25 (2015)
9. Zhang, Z., Wu, Z., Wang, D., et al.: Current status and technical description of Chinese 2 × 250 MWth HTR-PM demonstration plant. Nucl. Eng. Des. **239**(7), 1212–1219 (2009)

Research on Test for Spray/Immersion Conditions with Extreme pH of Third Generation Nuclear Class 1E Cables

Xin-Yu Wang[1], Fei-Fei Zhu[2(✉)], Qi Wu[1], and Jing-Yuan Yang[1]

[1] Nuclear and Radiation Safety Center, Beijing 100822, China
[2] State Nuclear Power Engineering Corporation, Shanghai 200233, China
zhufeifei_seu@yeah.net

Abstract. In the Section 7 of the latest IEEE 383-2015 [1], it is required that the qualification of the cables located in the mild environment shall include long-term water immersion testing for 1 year period. Also, in some third generation nuclear power plant, it is required that the 1E or non-1E shall be conducted the test for spray/immersion conditions with extreme pH in non-DBA Conditions. Based on this, the test for spray/immersion conditions with extreme pH is more and more paid attention. However, the research on this test has not been done in China. The aim at this article is doing the research of test of spray/immersion conditions with extreme pH, and is to discuss and introduce the qualification method.

Keywords: Extreme pH spray · Immersion test · Cable · Qualification method

1 Introduction

In the current three generations of nuclear reactor type, the total cable length is more than 1,500 km/s, including low-voltage cables, control cables, instrument cables, communication cables and special cables and other major categories. The main function of these IE cables are to provide power and control signals for the plant's power equipment, Or transfer instrument monitoring signal, or to achieve the whole plant communications.

According to the classification of nuclear safety, nuclear power cables can be divided into two categories: Class 1E and Non-1E. Among them, Class 1E cables shall perform safety function during and after the Design Basis Accident (DBA). Non-1E cables are not available during and after Design Basis Accident (DBA), but some third generation nuclear power plants (e.g. AP1000) proposes that the Non-1E cables in the containment must maintain the integrity of the jacket after the accident to reduce the occurrence of cable jacket debris flaking. It is to prevent the accumulation of debris on the pit filter of the recirculation system in the containment, which can plug the pit filter. Therefore, such these Non-1E cables also need to verify the ability of such non-functional requirements by equipment qualification.

Y. Xu et al. (eds.), *Nuclear Power Plants: Innovative Technologies for Instrumentation and Control Systems*, Lecture Notes in Electrical Engineering 455,
https://doi.org/10.1007/978-981-10-7416-5_10

IEEE 383 is the most widely recommend standard for the qualification of the nuclear cables. The latest version was published in September 2015. Compared with the version of 2003, the relevant equipment qualification of requirements has changed. In Chap. 7 of this standard, it is stated that for low voltage control cables under the mild environment conditions, long-term water immersion testing for 1 year period is required. Also, in some third generation nuclear power plant, it is required that the 1E or Non-1E cable in/out the containment shall be conducted the test for spray/immersion conditions with extreme pH in Non-DBA Conditions. At present, there is no comprehensive experience of spray/immersion conditions with extreme pH test according to IEEE 383-2015 [1].

In this paper, it takes the latest published IEEE 383-2015 [1] <IEEE Standard for qualifying Class IE Electric Cables and Field Splices for Nuclear Power Generating Stations> as the cornerstone, and takes the extreme pH test with spray/immersion conditions that are applicable to the nuclear cables as the object of study. It is focused on the test of the design idea, test programs and related test practice, and is in order to form a standardized test method.

2 Qualification Requirements and Methods for Cable Spray/ Immersion Test with Extreme pH

2.1 Purpose of Spray/Immersion Test with Extreme pH

During the operation of a nuclear power plant, soluble boric acid is added to the primary coolant to control the reactivity of the reactor core. In addition, in order to control the influence of water pH value on the corrosion behavior of metals and the migration of corrosion products in the loop, the primary coolant must maintain a higher pH value. All these actions lead to both the acidic solutions and alkaline solutions will be presented in the auxiliary system pipelines. So, inside and outside the containment of a NPP, there are many pipes used to transport such high pressure and high velocity acid and alkaline fluids. These pipelines have been designed to have capacity of the high energy fluid. The pressure fluctuant and peak pressure often occur on the pipes. Also, the change of the fluid pressure and temperature corporate with vibration due to the fluid velocity will produce cavitation and corrosion, fatigue and creep effect. All these conditions may lead to the middle and high energy pipeline rupture accidents. The broken pipes would hit the equipment around. And the high temperature and pressure liquid would spray room and makes low-lying immersion with fluid [3].

The middle and high energy pipeline broken off have more damaging on the equipment around. The domestic and foreign NPP designers, owners and safety reviewers have paid more attention on it. The analysis of the pipeline break, thawing and anti-rejection device analysis methods continuous improve, and more advanced anti-rejection technologies are constantly applied, it contributes little impact of middle and high energy pipeline broken off on the safety operation of the NPPs. However, the impacts of high temperature and pressure liquid spraying and short time liquid contamination on instruments, cables and other equipment near the pipeline need prompt attention. In this paper, it is focused on the simulation of extreme pH spray/immersion in cable qualification due to the medium and high energy pipeline rupture. And the influence of the accident on the cable is analyzed (Fig. 1).

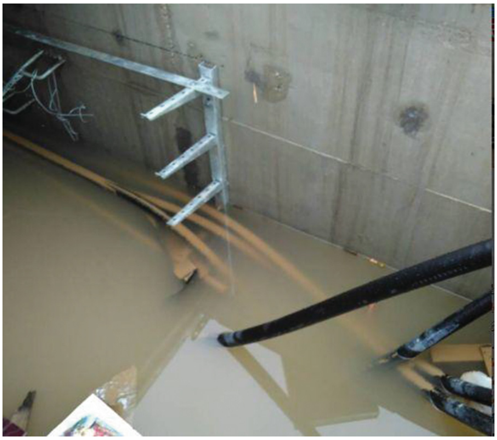


Fig. 1. Cable under spray and immersion accident

2.2 Test Requirements for Spray/Immersion Conditions with Extreme pH

Based on IEEE 383-2015 and the technical specification of the third generation NPPs, the requirements of the test for Spray/Immersion Conditions with Extreme pH is listed below. The temperature profile of the spray/immersion test is shown in Fig. 2.

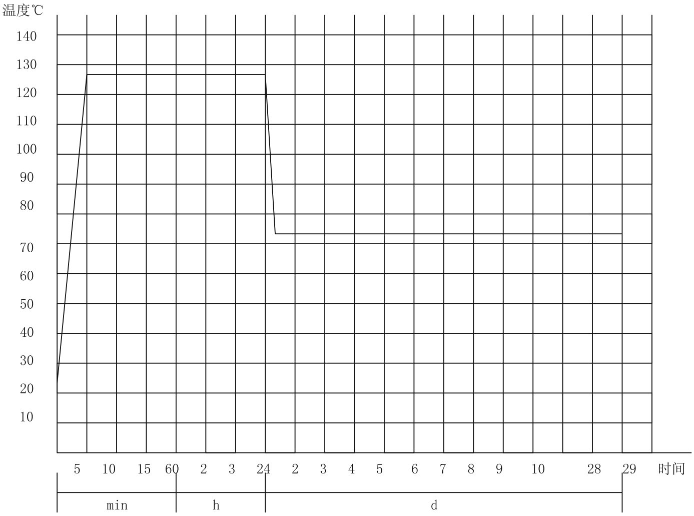


Fig. 2. Temperature profile of the spray/immersion test(With 8.3 °C Margin)

1. The thermally/radiation aged cable shall be subject to the test conditions detailed below, and the electrical integrity of the insulated conductors is required. The

- Acidic conditions, 4375 ppm B (aqueous solution), equivalent pH 4.2 (approximate). Minimum event peak temperature 129 °C for 24 h total; Minimum event temperature 73.9 °C for 29 days total for all events.
- Alkaline conditions, pH 11.5 sodium hydroxide (NaOH) solution, Minimum event peak temperature 129 °C for 24 h total; Minimum event temperature 73.9 °C for 29 days total for all events.

2. The un-aged cable shall be subject to the test conditions detailed below, electrical integrity of the insulated conductors is the requirement.

- Acidic conditions, 4375 ppm B (aqueous solution), equivalent pH 4.2 (approximate). Minimum event peak temperature 129 °C for 24 h total; Minimum event temperature 73.9 °C for 29 days total for all events.
- Alkaline conditions, pH 11.5 sodium hydroxide (NaOH) solution, Minimum event peak temperature 129 °C for 24 h total; Minimum event temperature 73.9 °C for 29 days total for all events.

2.3 Qualification Method of the Test for Spray/Immersion Conditions with Extreme pH

Based on the standard IEEE 323 [2] and IEEE 383, the cable qualification has following four methods:

1. Type Test;
2. Operating Experience;
3. Analysis;
4. Combined Qualification.

The test for spray/immersion conditions with extreme pH is one item of the cable qualification test. It can also follow the above qualification methods. The type testing is the preferred method. Qualification by analysis alone is not acceptable. But analysis can be performed as a supplement to the type testing and operating experience. Considering the spray/immersion test is still in the research step without any experience and reference data, the type testing method is adopted in this paper.

2.4 Type Test Sample Selection

The samples applied to spry/immersion test with extreme pH shall be representative of the cables being qualified in accordance with the requirements of IEEE 383. The routine areas (Inside or outside containment) and the cable types (such as medium, low voltage cables and instrumentation cables) shall be considered in the sample selection. Also, the preparation of the sample quantities shall be per the following test flow chart in Fig. 3. The test samples shall be separated into two parts, including aged and un-aged samples.

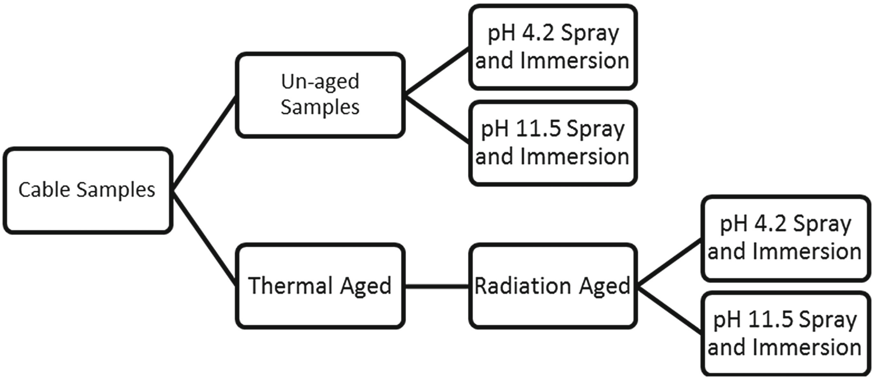

Cable Samples
Un-aged Samples
pH 4.2 Spray and Immersion
pH 11.5 Spray and Immersion
Thermal Aged
Radiation Aged
pH 4.2 Spray and Immersion
pH 11.5 Spray and Immersion

Fig. 3. Spray/Immersion test flow chart

2.5 Procedure for Spray/Immersion Test with Extreme pH

The procedure for Spray/Immersion Test with Extreme pH shall follow the below steps.

1. Choose suitable size container, fix cable samples in the container, and seal two tops and fixed in container.
2. Keep container pressure constantly at 137 kPa (contain 10% margin).
3. Preparation acidic/alkaline conditions (room temperature), the variation of temperature as Fig. 2, rise temperature to 129 °C (the time of rise temperature process not more than 5 min) and spray for 24 h total. Than stop spray and cool to 73.9 °C. Flood all the events for 696 h (29 days).
4. Electrical integrity test should be done after flooding.

- Test voltage, 3 kV alternating current, continue 5 min, insulation should not be breakdown.
- Insulation resistance constant at 20 °C, the measured value should not less than 0.3 MΩ.km.

5. Jacket integrity is not a requirement, but it should be noted in the report (jacket integrity is not the judgment for the qualified).

3 Cable Spray/Immersion Conditions with Extreme pH Test Practice

3.1 Plastic Insulation Cables

According to the above sample selection and test procedures, and based on the requirements of IEEE 383 and related technical specifications, it is carried out a Spray/Immersion test on an instrumentation cable with polyolefin insulation and jacket used in a third generation nuclear power plant.

3.2 Cable Sample Preparation

According to the above sample selection in Sect. 2.4, the numbers of samples of the plastic insulation instrument cables can be selected as shown in Table 1 below.

Table 1. Sample selection and quantity arrangement

Serial number	Structure	Number of samples/group
1	$1 \times 2 \times 1.5\ \text{mm}^2$	4(Each 20 m)
2	$8 \times 2 \times 0.75\ \text{mm}^2$	4(Each 20 m)
3	$19 \times 2.5\ \text{mm}^2$	4(Each 20 m)

3.3 Aging Test

Due to the assessment of the function of the aged cable after the spray/immersion test, the thermal and radiation aging tests of the cable shall be done firstly. The relevant aging conditions and parameters are shown in Table 2 below.

Table 2. The aging parameters of the plastic cable

Type	Equivalent thermally aging 60 years	γ radiation aging Mrad	Dose rate kGy/h
Control cable	155 °C,1728 h(72D)	25	10

Note:1728 h is calculate thermally aging test hour with long-term work at 90 °C.

3.4 Electrical Integrity Check Before the Spray/Immersion Test

Before the spray/immersion test, the AC voltage test and the 20 °C insulation resistance constant test were carried out for all test samples (4 groups in which two groups were aged and two groups were not aged). The test results are shown in Table 3 below.

Table 3. Electrical integrity check before spray/immersion test

No.	Structure	Test projects	Test voltage/kV	Pressure/min	Test results	20 °C Insulation resistance constant test/ (MΩ*km)
1	1 × 2 × 1.5 mm^2 8 × 2 × 0.75 mm^2 19 × 2.5 mm^2	Alkali on-aged	3.0	5	Not be breakdown	>0.3
2	1 × 2 × 1.5 mm^2 8 × 2 × 0.75 mm^2 19 × 2.5 mm^2	Acid on-aged	3.0	5	Not be breakdown	>0.3
3	1 × 2 × 1.5 mm^2 8 × 2 × 0.75 mm^2 19 × 2.5 mm^2	Alkali not-aged	3.0	5	Not be breakdown	>0.3
4	1 × 2 × 1.5 mm^2 8 × 2 × 0.75 mm^2 19 × 2.5 mm^2	Acid not-aged	3.0	5	Not be breakdown	>0.3

3.5 Spray/Immersion Test Sample Placement

In the test process, the first 24 h of the spray test was performed in a LOCA test chamber. And then the following high temperature immersion test was conducted in an immersion test chamber. The placement of the test samples was as shown in Fig. 4 below.

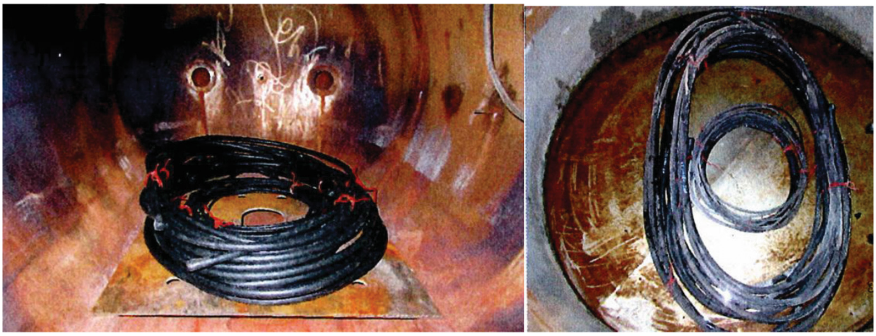


Fig. 4. Placement of the spray/immersion test sample

3.6 The Temperature and Pressure Are Maintained During the Spray/Immersion Test

During the first 24 h of the spray/immersion test, a certain pressure was maintained for the spray solution and the temperature in the test chamber was set at 129 °C. The first 24 h temperature and pressure curve of the extreme alkaline solution spray/immersion test is shown in Figs. 5/6.

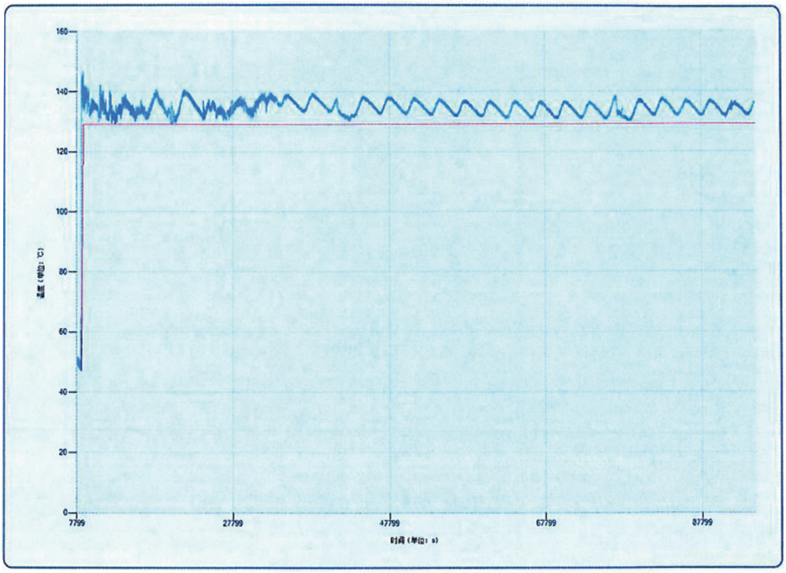


Fig. 5. The 24 h temperature curve of extreme spray/immersion test

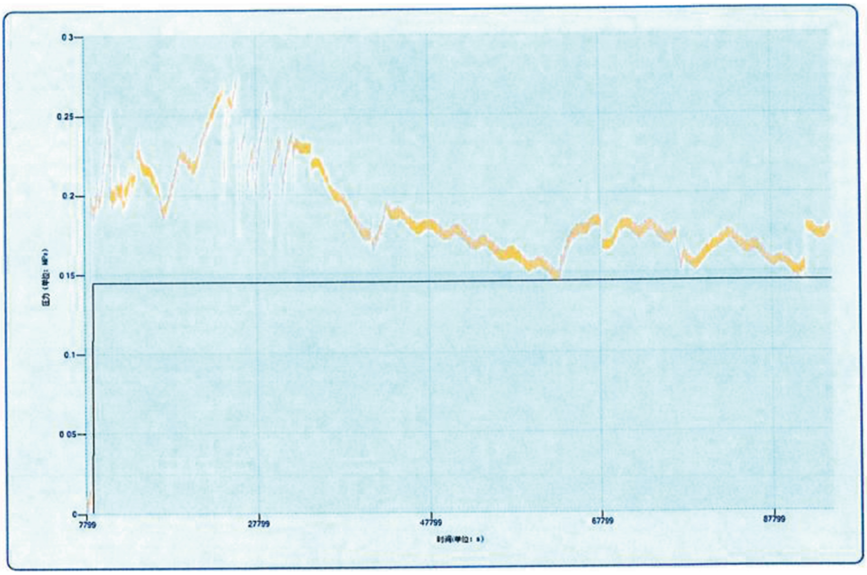


Fig. 6. The 24 h pressure curve of extreme spray/immersion test

3.7 Acceptance of Spray/Immersion Test

In accordance with the test procedure in Sect. 2.5 above, acceptance tests shall be carried out after the spray/immersion test, including visual inspection and electrical tests. The following section takes the extreme alkaline solution spray/immersion test practice as an example to discuss the acceptance test.

1. Visual Check

- After the 24 h spraying test in extreme alkaline solution, visual check on the sample control cable was performed. No cracks, damaged and shedding occurred, see Fig. 7. And then the test samples were transferred from the LOCA spray test chamber to the immersion test chamber.

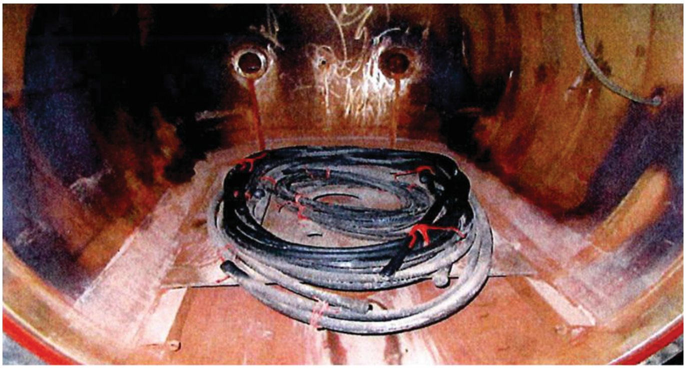


Fig. 7. Cable sample state after spray in extreme alkaline solution

- After the immersion test, open the immersion test cover, visual check on the sample control cable was performed. No cracks, damaged and shedding occurred, see Fig. 8.

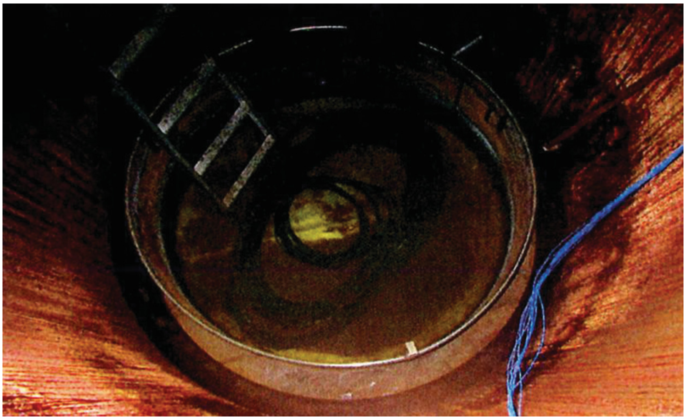


Fig. 8. Cable sample state after immersion in extreme alkaline solution

2. Electrical Test

After the end of the spray/immersion test, the AC voltage test and 20 °C insulation resistance constant test were performed on all cable samples. The test results were shown in Table 4 below.

Table 4. Electrical Test

No.	Structure	Test projects	Test voltage/kV	Pressure/min	Test results	20 °C insulation resistance constant test/ (MΩ*km)
1	1 × 2 × 1.5 mm^2	Alkali not-aged	3.0	5	Not be breakdown	6310, 7380
2	8 × 2 × 0.75 mm^2		3.0	5	Not be breakdown	5530, 4260
3	19 × 2.5 mm^2		3.0	5	Not be breakdown	2810, 2070, 2170
4	1 × 2 × 1.5 mm^2	Alkali aged	3.0	5	Not be breakdown	0.69, 0.64
5	8 × 2 × 0.75 mm^2		3.0	5	Not be breakdown	0.56, 0.73
6	19 × 2.5 mm^2		3.0	5	Not be breakdown	0.56, 0.62, 0.75

Based on the above Table 4, the un-aged samples carried out the Spray/Immersion Conditions with Extreme Alkali pH,the insulation resistance constants is abnormal,but still meet the acceptance criteria 0.3 MΩ*km requirement. But based on the comprehensive analysis of Spray/Immersion Conditions with Extreme acid pH test results, it can be initially judged that the cause of the abnormal may be due to the cable termination sealing is not tight, which can be resulting in insulation damp in the Spray/Immersion test process.

In addition, according to the results of the above test practice, it can also be concluded that the short-term (one month) high temperature Spray/Immersion Conditions with Extreme pH has limited influence on the structure and electrical performance on the polyolefin insulated and jacket cable.

4 Conclusion

The test for spray/immersion conditions with extreme pH has increasingly become the focus of the qualification for the cables and instruments near the high-energy pipeline,But there is no practice of such tests in domestic. Based on the qualification methods in the latest version of IEEE 383-2015, it is listed the qualification requirements of the test for spray/immersion conditions with extreme pH for the third generation NPP cables in this article. This article emphatically discussed the sample selection and test procedure that is not mentioned in the standards IEEE 383-2015, and the test practice was conducted based on the discussed test procedure. An conclusion obtained is that the short-term (one month) high temperature Spray/Immersion Conditions with Extreme pH has limited influence on the structure and electrical performance on the polyolefin insulated and jacket cables. This article can be reference for the NPP designers, and guide the domestic suppliers to do the follow-up qualification.

References

1. IEEE Standard for Qualifying Class 1E Electric Cables and Field Splices for Nuclear Power Generating Stations, IEEE 383-2015, 9 (2015)
2. IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations, IEEE 323-2003, 1 (2004)
3. Ding, Kai: Study on Pipe Whip Analysis of High Energy Pipe Break. Shanghai, China (2014)

The Selection of Neutral Grounding Method for Stationary Medium Voltage Power Supply System in Nuclear Power Plant

Jing Kong, Qi Zhang(✉), Da-Hu Liu, Peng Liu, Yan Feng, and Zi-Xi Chen

Nuclear and Radiation Safety Center, Beijing, China
jingkong2011@126.com

Abstract. The rational choice of the neutral-point grounding mode of the medium-voltage system directly influences the reliable operation of the nuclear power plant. The selection of neutral-point grounding mode shall ensure the reliability of power supply and limit the over-voltage, and take into account the influence of system voltage, insulation level, communication, grounding protection and other aspects. Compared with thermal power plants, the preliminary design and protection configuration of the NPP neutral-point grounding mode of the medium-voltage system is similar, but nuclear power plants require higher reliability and safety. At present, the neutral-point grounding mode is different in CPR1000, EPR and AP1000 nuclear power plants. In this paper, the neutral grounding method and its selection basis of the medium voltage system of the NPP are introduced, and the calculation method of the ground fault capacitive current in the different operating modes is proposed, and the proposal to deal with the excessive ground-fault capacitive current is put forward.

Keywords: Nuclear power plant · Neutral-point grounding
Single-phase grounding fault · Over-voltage

1 Neutral Grounding Method and Protection Configuration of the Plant Power Supply System

1.1 Introduction

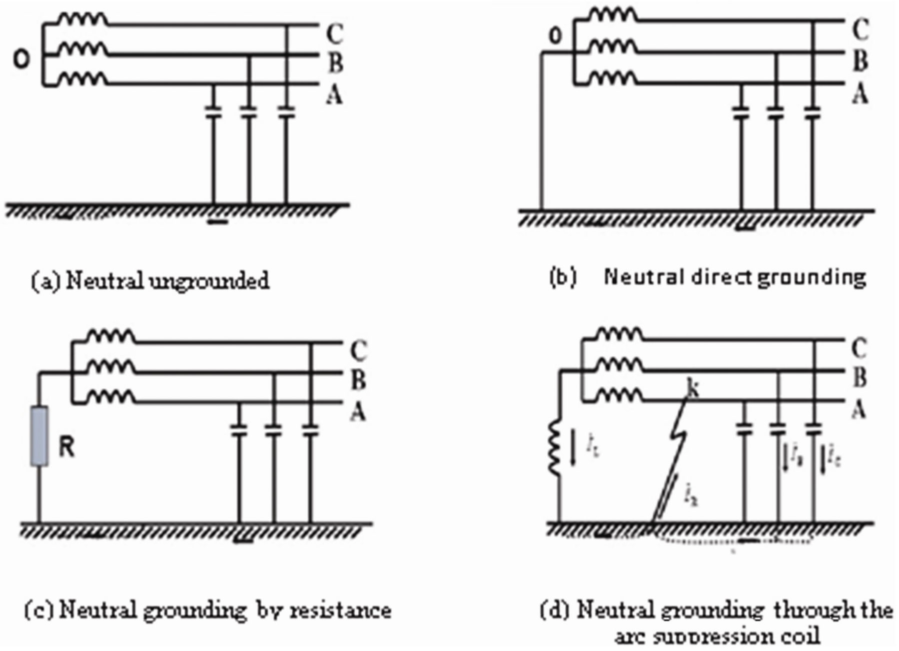
To ensure nuclear safety, the plant power system of a nuclear power plant should be designed to reliably supply power for the necessary equipment in the event of a radioactive hazard to the plant personnel and the environment; an operational failure or external disaster affecting the supply of electricity will not cause a radioactive accident [1]. Compared with thermal power plants, the preliminary design and protection configuration of the NPP neutral grounding is similar, but nuclear power plants require higher reliability and safety. At present, there are three main types of the running and under construction CPR1000, EPR, AP1000. The neutral grounding method is different in three types of nuclear power plants. The selection of neutral grounding method shall ensure the reliability of power supply and limit the over-voltage, and take into account

Y. Xu et al. (eds.), *Nuclear Power Plants: Innovative Technologies for Instrumentation and Control Systems*, Lecture Notes in Electrical Engineering 455,
https://doi.org/10.1007/978-981-10-7416-5_11

the influence of system voltage, insulation level, communication, grounding protection and other aspects. In this paper, the neutral grounding method and its selection basis of the medium voltage system of the NPP are introduced, and the calculation method of the ground-fault capacitive current in the different operating mode is proposed, and the proposal to deal with the excessive ground capacitive current is put forward.

1.2 Operation Mode of Neutral Grounding in Power System

The neutral is the neutral point of the star-connected transformer or generator. The neutral grounding methods used in the plant power supply system of the power plant include neutral ungrounded, direct neutral grounding, neutral grounding by resistance(including low, medium and high resistance), and neutral grounding through the arc suppression coil (Fig. 1) [2]. At present, three major methods of neutral grounding of the medium voltage system of the NPP, are neutral ungrounded, neutral grounding through the resistance and neutral grounding through the arc suppression coil.



(a) Neutral ungrounded

(b) Neutral direct grounding

(c) Neutral grounding by resistance

(d) Neutral grounding through the arc suppression coil

Fig. 1. Operation mode of neutral grounding in power system

1.3 Neutral Ungrounded System and Its Protection Configuration

Neutral ungrounded system refers that the neutral point and the earth do not set any connection, but in the actual system there is a capacitance distribution between the three phase lines and the earth. In normal operation, there is no voltage between the neutral point and the earth, when the single-phase ground fault occurred, the voltage of grounding phase decreases, the voltage of non-fault phase increased the line voltage, which cause a threat to the insulation of the equipment, but the system's three-phase line voltage remains balanced, thus the system is allowed to continue to run for 2 h, the reliability of power supply is improved. This grounding method has the advantage of continuous power supply, a lower contact voltage and step voltage. To a certain extent, neutral ungrounded can effectively reduce the damage rate of electrical equipment, and ensure the reliability and safety of the personal and equipment. Due to the presence of distributed capacitance to the earth, the ground-fault point and the earth forms a current loop through the conductor, the ground-fault current will flow through the ground fault point, where the current may produce a stable or intermittent arc, so the value of ground-fault capacitance current in neutral point ungrounded system has certain requirements (the value is no more than 10 A).

When the single-phase ground fault occurred in three-phase symmetrical neutral-point ungrounded system, the zero-sequence current at the beginning of the non-fault phase line is its own capacitive current. The direction of the capacitive reactive power flows from the bus to the line, the zero-sequence current at the beginning of the fault phase line is the sum of the capacitance current of the entire system of non-fault components. The direction of the capacitive reactive power flows from the line to the bus, in the event of single-phase ground fault, the neutral point will produce zero-sequence voltage due to the relative ground voltage drop.

Due to the above-mentioned characteristics of the single-phase ground fault in the neutral ungrounded system, the single-phase grounding protection is configured as, (1) Insulation monitoring, mainly monitor the zero-sequence voltage after grounding and actuate as the alarm signal. (2) Zero-sequence current protection, when the single-phase ground fault occurs, the zero sequence current of the fault phase is larger than the current of the non-fault phase, thus selectively send out signals or actuate trips. (3) Zero-sequence power direction protection, the selective protection can be achieved according to the difference of zero-sequence power direction between the ground-fault phase and non-fault phase.

1.4 Neutral Grounding Through the Arc Suppression Coil System and Its Protection Configuration

Neutral grounding system through the arc suppression coil refer that the inductance coil is set between the neutral point and the earth in order to protect the power supply system. If the ground-fault capacitive current is too large in the event of the single-phase ground fault, usually the current will be in the form of arc, Unstable arc combustion also can causes arc overvoltage. When the protective measures is absent or equipment insulation level is low, the insulation of the device is easily punctured, two phase short circuit or interphase short circuit will be occurred, which will be a serious threat to plant power system security. Inductance coil in the action of zero-sequence voltage of the neutral provide inductive current as compensation capacitor current, and reduce the residual current of the ground-fault point, so the arc is extinguished and the failure is eliminated. After the arc suppression coil neutral is installed, in the event of single-phase is grounded, the single-phase ground-fault capacitor current is compensated by the inductive current of the arc suppression coil. The residual current of the fault point is reduced to such an extent that the arc does not easily reignite. Therefore, the single-phase ground-fault of the power supply system can be automatically eliminated instantaneously.

The installation of the arc suppression coil reduces the ground fault current makes the characteristics of fault after the failure not obvious, so the selective grounding protection configuration will be more difficult, although the protection only needs to actuate on the signal alarm. Secondly, the arc coil in operation can't be adjusted according to the flexibility of the system to adjust the compensation, it is possible that the arc does not automatically turn off and the over-voltage problem is occurred again.

1.5 Resistance Neutral Grounding System and Its Protection Configuration

Resistance neutral grounding system refers that the suitable resistance is connected between the neutral point and the earth. Compared with the mode of neutral ungrounded and neutral grounding through the arc suppression coil, the resistance neutral grounding can avoid resonant overvoltage or intermittent arc grounding overvoltage. When the system occurs the single-phase grounding, the ground resistance can generate an induced current to initiate zero-sequence voltage protection, at the same time the fault can be effectively cut off in time. The voltage of the fault phase will not have a large increase. So the time equipment withstand over-voltage will be significantly shortened, which is conducive for equipment to reduce the insulation level. Without reducing the level of insulation equipment conditions, the insulation margin of equipment is increased, the operation reliability of system equipment is improved.

A large short-circuit current will be produced as single-phase grounding of the power system. If the protection device does not actuate in the tripping fault line quickly, which will cause serious damage to the equipment. According to the zero-sequence current after the ground fault, can be directly grounded or a small resistance grounding system of zero-sequence current protection, which can be configured as zero-sequence current protection of grounding system via small-resistance or directly grounding. Usually combined with the scope of protection, zero-sequence current setting value, the zero-sequence current protection can be divided into three sections, zero-sequence current instantaneous speed protection, zero-sequence current limit speed protection, zero-sequence over-current protection. When a single-phase ground fault occurs, whether the fault is permanent or not, the fault line will trip, the reliability of the system power supply is reduced. When a single-phase ground fault occurs, a higher ground voltage is generated. If the zero-sequence protection failure, the adjacent cable and the equipment of the fault point are subject to damage.

2 Selection of Neutral Grounding Method of Medium Voltage System in Nuclear Power Plant

2.1 The Requirement of Standards and Specifications

From the following criteria (show as Table 1) can be seen that the ground-fault capacitor current is an important parameter to choose in determining the power plant neutral grounding method, the system should firstly calculate the single-phase ground-fault capacitance current, and thus determine the grounding method to reduce the node capacitance current hazards. For ungrounded system, the limit of ground-fault capacitance current is 10 A [3]. When the capacitor current exceeds 10 A, the arc will occur. When the resistance at the ground point recovers more slowly than the voltage, the arc current will exceed the rated voltage, resulting in a continuous arc, over-voltage and other issues, endangering the safe operation of power plants.

Table 1. The requirement of standards and specifications

Standards and specifications	Requirement
GB 50064-2014	A system consisting of 6 kV – 20 kV cable lines not directly connected to the generator can select Neutral ungrounded mode when the single-phase ground-fault capacitive current ≤10 A; When the corresponding current is more than 10 A and need to run in ground-fault conditions, the system should be used resonant grounding or resonant - low resistance grounding
GB 50660-2011	When the ground-fault capacitance current of the high-voltage power supply system is less than 10 A, the neutral point can be ungrounded or be grounded through high-resistance
IEEE Std C62.92.3-1993	For an ungrounded station auxiliary system, ground-fault currents on the order of 10 A or less would be expected
RCC-E (2005)	The auxiliaries MV system is operated with an insulated neutral to allow continuously monitoring of line insulation and operation for a limited period with a phase-to-earth fault

2.2 The Calculation of Ground-Fault Capacitance Current

Ground-fault capacitive current depends on the capacitance of the cables and other devices in the bus circuit, such as the motor, transformer, and measuring inductor unit. The ground-fault capacitor current is calculated mainly by the following formula:

$$\mathrm{Ic} = \sqrt{3}Un \times 2\pi f \times C \times 10^{-3} \tag{1}$$

Ic — Single-phase grounded capacitor current (A);
Un — Rated voltage of auxiliary power supply system (kV);
f — Rated frequency (Hz);
C — The relative capacitance of the auxiliary power supply system (uF);

The capacitance per unit length of the cable and most of the motor capacitor is given by the manufacturer. Capacitance values for other devices are calculated for general measuring or estimating values.

Nuclear power plant ground-fault capacitor current is the maximum sum capacitor value of different bus lines and the motor transformer and other equipment current in different modes of operation. The capacitor (C) of the calculation formula in theory includes the capacitance value of the main equipment carried by the auxiliary power system, including cables, motors, low voltage transformers, etc. But in the domestic nuclear power plant (CPR1000), the actual calculation of the system is only used to calculate the cable value of the system, and then 1.25 times the margin, the cable of each capacitor given by the cable manufacturer, different types of cable cross-section capacitance is different, according to the length of the cable used to calculate out of the ground capacitance current value. Figure 2 shows a CPR1000 nuclear power plant in the medium voltage power plant system. The calculation of the ground-fault capacitor current value in the three operation modes (load, auxiliary transformer load, emergency diesel generator with load) during the grid-connected test was calculated [4] (show as Table 2). It is found that, due to the increased cable length and equipment of nuclear power plant transformer or auxiliary transformer, the single-phase grounding capacitor current of the CPR1000 and EPR nuclear power plants will be larger than 10 A. In the auxiliary transformer with load, the maximum ground-fault capacitor current during operation may reach 30 A, which exceeds the current standard requirement. However, based on the current design of nuclear power plants under construction still require the plant to run with faulty distribution system, it is still used neutral ungrounded in the medium voltage system of the plant. If the ground-fault capacitor current is too large which can

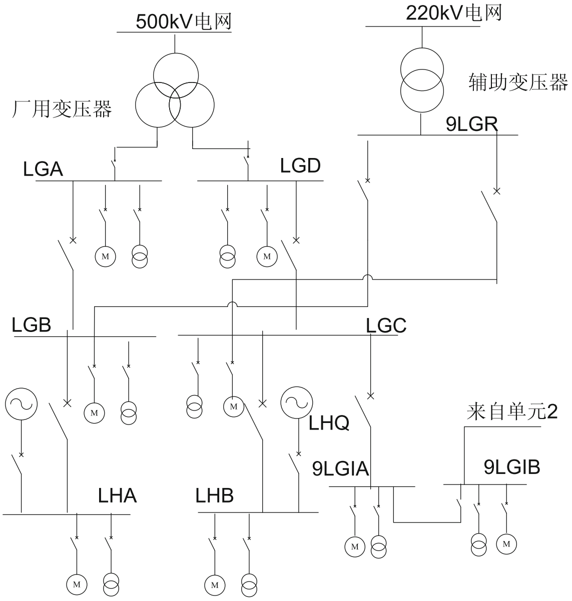


Fig. 2. Stationary medium voltage power supply system of NPP

lead to two-phase grounding fault short circuit or interphase short circuit, which may damage the plant electrical equipment insulation and the power system crash, reducing the reliability of nuclear power plant operation.

Table 2. The calculation of ground-fault capacitance current in CPR1000 NPP

Operation mode	Load	Auxiliary transformer load	Emergency diesel generator with load
Bus line	LGD + LGC + LHB + 9LGIA	9LGR + LGC + LHB + 9LGIA	LHB
Ground-fault capacitive current (maximum)	1.25*∑Ic(cables)	1.25*∑Ic(cables)	1.25*∑Ic(cables)

2.3 Selection of Neutral Grounding Method for Domestic Nuclear Power Plant

At present, there are three main types of nuclear power plants in China, CPR1000, EPR and AP1000. The neutral grounding method of the medium voltage system is different in CPR1000, EPR and AP1000 nuclear power plants. AP1000 adopts low-resistance neutral grounding method, while EPR and CPR1000 adopt neutral ungrounded (or arc-suppression coil grounding) method.

AP1000 NPP is based on the concept of passive system design, the AC power system is non-safety class. In normal operation, the medium voltage system adopts low-resistance neutral grounding method, when the emergency diesel generator is switched on, the power supply network is changed to a neutral ungrounded system. Such a neutral grounding method has the protection of high sensitivity, the protection of equipment is safe and reliable, but the reliability of the power supply system continuity is lower, in the event of a single-phase ground fault, the corresponding ground fault load will directly cut off, it will not have a significant impact on nuclear safety.

The design of CPR1000 and EPR power plant is following the RCCE rules, EPR and CPR1000 adopt neutral ungrounded (arc-suppression coil neutral grounding). The nuclear safety related equipment has accessed to the medium-voltage system. If the load is removed at the time of single-phase grounding, the safety operation of the plant may be unnecessarily affected [5]. So the adopting of neutral ungrounded system, can improve the reliability of power supply. When the single-phase is grounding, the medium-voltage system is allowed to run with grounding point, which is conducive to the continuous operation of nuclear power plants. However, due to the location of transformer and auxiliary transformers in the nuclear power plant is far away from the load position, and a large number of cables was used, and the length of the cable increased and BOP sub-equipment also increased which result in the ground-fault capacitive current increasing, the value of ground-fault capacitive current exceeds the provisions of the national standard (no more than 10 A). If the value of capacitor current is too large, the arc can,t be quickly extinguished or re-ignition repeatedly, and finally result in over-voltage, will endanger the entire equipment insulation of the medium-voltage system [6].

In order to reduce the ground-fault capacitor current and prevent single-phase ground-fault into two-phase ground or indirectly more serious accidents, the nuclear power plant take measures to reduce the potential hazards of the excessive capacitance current.

1. The medium-voltage system adopts neutral parallel arc-suppression coil grounding method. The system chooses neutral ungrounded mode in normal operation. In the event of single-phase ground fault, arc suppression coil is automatically put in order to compensate for inductive current, reduce the ground capacitance current (such as the inductive current) and prevent over-voltage generation and failure to further spread. However, this kind of neutral grounding method has not been verified by running experience. Whether it can effectively and rapidly switch to reduce the capacitance current in the event of single-phase ground fault is yet to be verified. And this method requires additional arc suppression coil device, the medium-voltage system constitutes an increase in the operational aspects of the operation of the plant because the nuclear power plant system is more complex, different power supply and distribution network corresponding to the different capacitor current, the inductive current produced by the arc suppression coil must be changed accordingly (Arc suppression coil inductance capacity need to be a corresponding change). The change of the inductive load can,t be determined, the operating procedures must be changed accordingly, which is not conducive for the normal operation of the medium-voltage power system. Therefore, the neutral grounding through arc suppression is carefully selected.
2. In order to reduce ground-fault capacitive current of the cable, some power plant with neutral ungrounded method of medium voltage power system reduce the use of cables, use casting bus to replace some of the cable. The advantage is that the system's ground-fault capacitive current will be reduced, the floor space is relatively small, but the pouring bus is not grounded, the presence of induced voltage is relatively large, there is electromagnetic interference on the control communication lines, as well as the maintenance of personnel has a higher demand.

3 Summary

Neutral ungrounded method of medium-voltage power system in NPP has a wider application, which ensures the reliable and continuous power supply, the safe and stable operation of nuclear power plant. However, due to the increase of cable length and equipment of the nuclear power plant, the excessive capacitance ground-fault current is also a potential safety hazard for nuclear power plants. The arc overvoltage caused by the single-phase ground fault current in the medium-voltage power system has an adverse effect on the insulation of the downstream safety-grade equipment. Although the nuclear power plant and design units are aware of the potential risks, by increasing the insulation level of cables and equipment, but it is difficult to fundamentally solve the problem of the ground capacitance current is too large. Based on the current design of nuclear power plants in the construction of the plant still requires the design of faulty distribution system with the operation, if the change in neutral grounding method, the entire nuclear power plant operating system must undergo a series of changes, nuclear power plants and multi-party units need further research and analysis.

References

1. NB/T20051: Nuclear Power Plant Power System Design Guidelines. Beijing: Atomic Energy Press (2011)
2. Ge, D.F.: Electrical design manual for electric power engineering (electric primary part). China Electric Power Press, Beijing
3. GB 50064: AC electrical installations over-voltage protection and insulation coordination design (2014)
4. Yang, S.: Nuclear power plant study on ground fault capacitance current of the ungrounded power system. Nucl. Power Eng. (2014)
5. Fei, Y.Y.: Study on neutral grounding modes of medium voltage power supply system in a domestic nuclear power plant. Technol. Exch. (2014)
6. Xiao, M.N.: Analysis and application of neutral grounding method of auxiliary power system in nuclear power plant. Electr. Worlds (2015)

Discussion on Application of FPGA Technology in Safety Instrument and Control System of Nuclear Power Plant

Jing-Yuan Yang[1], Qi Wu[1](✉), Xin-Yu Wang[1], and Shao-Hua Han[2]

[1] Nuclear and Radiation Safety Center, Beijing, China
wuqi_nsc@163.com
[2] China Nuclear Power Engineering Co., Ltd., Shenzhen, China
hanshaohua@chinansc.cn

Abstract. FPGA technology with its clear behaviour, fast response, easy to transplant, long life and other advantages, more and more used in nuclear power plant safety instrument and control system. This paper analyzes the FPGA technology and CPU technology from the aspects of design flow, technical principle and performance characteristics, and analyzes the relevant regulatory standards and technical documents that can guide FPGA development, V&V and review. At the same time, this paper analyses the application of FPGA technology to the hardware description language, how to achieve the diversity design, how to avoid the metastable effect and the CGD technology Evaluation and acceptance for IP core and development tools, which related to FPGA technology applied to nuclear power plant safety instrument and control system.

Keywords: Nuclear power plant · Safety instrument and control system
FPGA technology

1 Overview

FPGA is a field programmable gate array, which is a semi-custom logic device of a special integrated circuit ASIC. FPGA technology has been widely used in the communications, electronic engineering and aerospace and other fields, but not yet widely used in the field of nuclear energy. At present, the domestic can be achieved based on FPGA technology, the main products include the china nuclear control system Engineering Co., Ltd. NicSys series of DCS products, state nuclear power automation system Engineering Co., Ltd. Nu series of nuclear power plant digital instrument control system and china techenergy Co., Ltd. FitRel Nuclear Power Station Digital Diversity Instrument Control System Platform.

FPGA technology and CPU technology are based on the code as the carrier, but the final product FPGA is a chip, therefore, FPGA development process is the hardware development and software development process. Typical FPGA development process including functional definition/device selection, design input, functional simulation, integrated optimization, integrated after simulation, implementation, post-wiring simulation, board-level simulation and chip programming and debugging and other major steps [1].

Y. Xu et al. (eds.), *Nuclear Power Plants: Innovative Technologies for Instrumentation and Control Systems*, Lecture Notes in Electrical Engineering 455,
https://doi.org/10.1007/978-981-10-7416-5_12

CPU technology von Neumann architecture, a series of instructions executed serially. In contrast, FPGA technology can achieve parallel operation, like multiple CPUs at the same time; its performance is several times a single CPU. In principle, the software can achieve the function, FPGA can be achieved. However, FPGA in dealing with similar multiplication and other high-level operations need to call a lot of resources, which FPGA chip performance requirements are relatively high. FPGA-based systems, compared to CPU-based systems, reduce the complexity of hardware and logic, isolate key and auxiliary functions, and have better portability and diversity design [2]. Compared with CPU technology, FPGA technology has many advantages such as high integration, small size, high flexibility, reconfiguration, low experimental cost and low risk.

2 Regulations and Standards

Currently, due to the FPGA it is different from the previous software system, has the dual characteristics of hardware and software, most of the national nuclear safety regulators no specific evaluation criteria FPGA system. Some of the digital system development standards and guidelines already available in the field of nuclear energy have been adopted by many national nuclear safety regulators for review based on FPGA systems. The regulations, guidelines, standards, and technical documents on which the NRC is based on the FPGA-based nuclear safety control system is shown in the following Table 1.

IEC61513 gives general requirements of nuclear power plant safety and important functions of the instrument control system and equipment, which includes the main requirements of the overall security lifecycle framework, the system life cycle framework, the computer system software, the computer system hardware and control room design related content. It is the overall guidance standard for safety-grade instrumentation systems and equipment. Hardware-level standards (IEC 60987 and IEC 62566) and software-grade standards (IEC 60880 and IEC 62138) are supplemented from two aspects. IEC62566 is the only standard to guide the development of integrated circuits for HDL programming in the nuclear power plant safety instrument and control system. It is actually a supplement to IEC 60987, but it also refers to the relevant requirements of IEC 60880 when it comes to project management, quality assurance planning, and configuration management issues that are the same as software development. At the same time, IEC62566 provides guidance in the HPD technical specifications, design and implementation and verification.

NUREG/CR-7006 is the NRC audit guidance document for specific areas of FPGA. This document mainly includes solving the problems of system security assessment, design and life cycle, V&V, configuration management and document requirements. It gives general requirements of reliability, robustness, traceability, maintainability of the views. It presents some suggestions for improving FPGA security design from design practice and V&V aspects. EPRI TR 1019181 summarizes the experience of FPGA technology in nuclear safety instrument control system. EPRI TR 1022983 proposed the

FPGA-based nuclear safety instrument control system in the design standards, development and implementation, development tools, V & V, safety evaluation and other aspects of the principle of recommendations.

Table 1. Regulations and standards on the FPGA-based nuclear safety control system

Type	Name
Regulations	10 CFR 50.55a(h) for safety I&C systems
Guidelines	RG 1.152 Criteria for Digital Computers in Safety Systems of Nuclear Power Plants
	NUREG/CR-7007, "Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems"
	NUREG-0800, SRP Chapter 7 for I&C Systems
	NUREG/CR-7006, Review Guidelines for FPGAs in NPP Safety Systems
	NUREG-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems"
	BTP 7-14, "Software Reviews for Digital Computer-Based I&C Systems"
	BTP 7-21, "Digital Computer Real-Time Performance"
	BTP 7-19, "Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based I&C Systems"
	DI&C-ISG-02, "Diversity and Defense-in-Depth Issues"
Standards	IEC 61508-2 Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems
	IEC 62566, Development of HDL-Programmed Integrated Circuits for Systems Performing Category A Functions, Edition 1.0
	IEC 60987 Nuclear power plants - Instrumentation and Control Important to Safety - Hardware Design Requirements for Computer-based Systems
	IEC 60880 Software for computers in the safety systems of nuclear power stations
	IEC 61513 nuclear power plants - instrumentation and control important to safety - general requirements for systems
Technical documents	EPRI TR 1019181 Guidelines on the Use of FPGAs in NPP I&C Systems
	EPRI TR 1022983 Recommended Approaches and Design Criteria for Applications of FPGAs in NPP I&C Systems
	IAEA No. NP-T-1.4 Implementing Digital Instrumentation and Control Systems in the Modernization of Nuclear Power Plants
	IAEA No. D-NP-T Application of FPGAs in Instrumentation and Control Systems of NPPs (Draft V1.4)
	NASA-HDBK 8739.23 NASA Complex Electronics Handbook for Assurance Professionals
	RTCA/DO-254 Design Assurance Guidance for Airborne Electronic Hardware
	VTT TECHNOLOGY The Current State of FPGA Technology in the Nuclear Domain

The above guidelines, standards and technical documents are the main documents that guide FPGA development, V & V and review at this stage. Due to the lack of comprehensive guidance and binding documents, other relevant standards and technical documents listed in the table for nuclear industry and aviation industry can provide useful reference and reference for FPGA development, V & V and review.

3 Some Concerns of FPGA Technology Applied to Nuclear Power Plant Safety Instrument and Control System

3.1 Hardware Description Language

FPGA design is usually expressed in hardware description language (HDL).

Hardware description language design technology is complete, flexible method, support a wide range of system hardware description ability, can be independent of the process of programming, language standards, norms, easy to share and reuse, with a short design cycle, investment risk and so on. Computer software programs are generally in the order in which they are written, while HDL has the characteristic of describing the concurrent activity of the hardware circuit, which is not available in other programming languages.

VHDL and Verilog are the most commonly used hardware description languages. As the industry standard text format language VHDL, can support simulation and synthesis, support for structured design and TOP-DOWN design method, the multi-style description of the method has nothing to do with the process. Relative to Verilog, VHDL is more rigorous in grammar, although it also makes it lose some flexibility and diversity, but from the nuclear safety instrument and control system security, reliability and nuclear quality assurance system features VHDL is a better choice.

VHDL has many concepts that are directly related to the structure of digital circuits, and the most commonly used is component, which is an abstraction of digital hardware architecture. The elements in VHDL are described by both entities and structures. Where the entity describes the interface of the element with the external environment, its internal behavior and structure is hidden. The function of the entity is defined in the structure. The structure specifies the input and output of the physical circuit and the behavior and function between each other. The presence of components in the hardware circuit makes VHDL out of the common programming language category, a description of digital circuits dedicated hardware design language [3].

NRC NUREG/CR-7006 FPGA design for safety instrument control system for reliability, durability, traceability, maintainability and so put forward a very specific coding requirement [4]. But as a hardware description language, VHDL in the application to the nuclear power plant safety instrument and control system, not only to follow the existing industry standard coding rules, but also should be noted in the following areas:

1. Make full use of functional structures such as packages, functions, processes, and libraries to reduce code complexity and make the necessary simplicity.

2. Organize the code according to the various calculation or processing functions performed along the critical path, making it easier for the verifier and the reviewer to verify the design and viewing.
3. Strictly regulate the naming of modules, functions, programs, signals, etc.
4. In the development document, the specific structure recommended and the specific structure to be avoided.
5. Provides observability and register status for critical signals to enhance testability and verifiability.
6. In the design should take full account of a single failure criteria, the necessary redundant design.
7. In the design of potential common cause of the fault should be assessed to carry out the necessary diversity design.

3.2 Diversity Design

The diversity design is one of the important design principles of nuclear power station control system to realize defense in depth. Diversity design can use different methods to achieve the desired purpose, effectively reducing the probability of occurrence of common cause failure. NUREG/CR-6303 mentioned in six aspects to achieve diversity design. FPGA technology design diversity can be reflected in different architectures, which mainly include CLB, input and output ports, logic modules, storage units, placement and routing and IP core aspects. In terms of device diversity, distinguish between different manufacturers, different FPGA types, different models, and so on. In terms of functional diversity, FPGA are based on CLB operation to achieve, which mainly includes the excitation signal, control logic, drive methods and response. In terms of human diversity, it mainly includes designer organizers or companies, management teams, design and development teams, implementation and validation teams. Signal diversity is triggered using different sensing parameters, depending on the input of the external port. FPGA software diversity and general software diversity is similar, including the run sequence, algorithm, logic control and operating environment. In the realization of diversity design FPGA safety instrumentation system, the diversity of the use should focus on solving those most concerned about the common cause of failure, a variety of design modules and circuits should be maintained between the full isolation and independence to ensure diversity is not affected by relevance [5].

3.3 Metastable Effects

The reliability of FPGA programming is an important factor affecting the reliability of the system in the development of nuclear power plant safety instrument and control system. And in the whole design process, how to minimize the number of metastable effects become the key to improve reliability. The metastable effect is a unique phenomenon in hardware programming. In the process of cross-clock domain signal and asynchronous signal transmission, the data may reach the destination register at any time, so the register signal settling time and hold time can not meet the requirements, there is a metastable effect [6]. As shown in the Fig. 1, the output data is oscillated when the metastable state is generated, “0” or “1” when the oscillation is back to the steady state. This is random and the logic of the output error will have a serious effect on the system function.

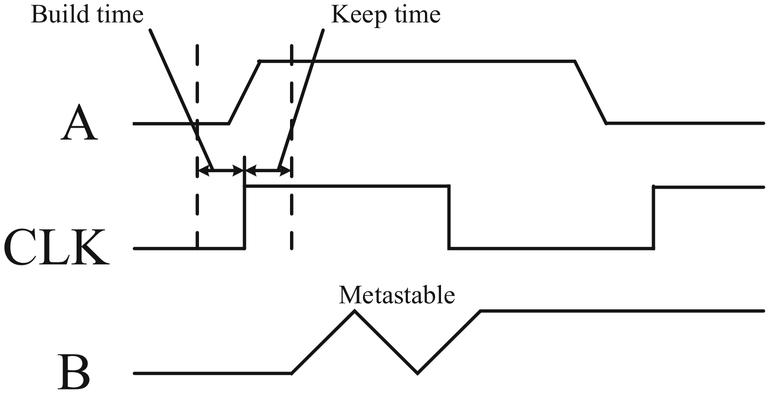


Fig. 1. Metastable effects

In the nuclear power plant safety instrument and control system FPGA design, deal with the signal establishment and maintenance time to fully consider, as far as possible in the data set up time or near the read data, the specific content of the following aspects:

1. For a cascaded functional module or a digital logic device, the working clock of the latter module or device typically takes the inverted signal of the previous module or the device operating clock, thus ensuring that the edge of the clock is within the hold time of the data.
2. Reliable clock design is critical because poorly designed clocks in digital circuits are subject to systematic error behavior at extreme temperature, voltage, or manufacturing process deviations. FPGAs generally have specialized global clock pins, and the global clock should be used when designing the project.
3. Stable and reliable clock is an important condition to ensure reliable operation of the system, the design cannot be any possible burr output as a clock signal, and as far as possible only use a global clock, the multi-clock system to pay special attention to asynchronous signals and non-Homology clock synchronization problem.
4. When the level value of the multiplexed signal changes, the output state of the combinational logic is uncertain at the moment the signal changes, and some false spikes are often generated. These spikes are called “glitches”. There are many ways to eliminate the glitch signal, usually using the “sampling” method.

3.4 CGD for IP Core and Development Tools

In the FPGA development process, developer often using IP core to achieve some mature and complex logic. IP cores can be implemented at different hardware levels, resulting in three types of IP cores: soft, solid and hard cores. Most of the IP cores used in FPGAs are soft cores that allow users to adjust parameters and enhance reusability [7]. Soft cores are usually provided in encrypted form, so that the actual RTL is invisible to the user, which is a challenge for the determinism of the security system. In addition, IEEE7-4.3.2 Section 5.3.2 specifies that the software tools used to support the software development process and the validation and validation process should be included in the configuration management. Therefore, the safety and reliability evaluation of FPGA development tools is very important. Commodity items are manufactured under conventional industrial systems and are provided with a reasonable acceptance process to provide reasonable assurance that they can perform their target safety functions. IP cores and development tools are third-party products, the manufacturing process has not been through the corresponding nuclear quality assurance system for control. The system development unit can carry out technical evaluation and acceptance of the IP core and development tools to be used, learn from the Method of CGD.

4 Concluding Remarks

FPGA-based nuclear power plant safety instrumentation system on the nuclear power plant put forward higher security and reliability requirements. This paper analyzes the FPGA technology and CPU technology from the aspects of design flow, technical principle and performance characteristics, and analyzes the relevant regulatory standards and technical documents that can guide FPGA development, V&V and review. At the same time, this paper analyses the application of FPGA technology to the hardware description language, how to achieve the diversity design, how to avoid the metastable effect and the CGD technology Evaluation and acceptance for IP core and development tools, which related to FPGA technology applied to nuclear power plant safety instrument and control system.

References

1. IEC. Nuclear power plants Instrumentation and control important to safety-Hardware design requirements for computer-based systems. Standard IEC 60987:2007. International Electrotechnical Commission (2007)
2. Zhao, J.Y.: Overview and regulatory summary of FPGA/PLD based applications in US Nuclear Industry. In: 5th International Workshop on Applications of FPGAs in Nuclear Power Plants Beijing, P.R. China, 8–11 October (2012)
3. EPRI. Recommended Approaches and Design Criteria for Application of Field Programmable Gate Arrays in Nuclear Power Plant Instrumentation and Control Systems. Technical report 1022983: 2011, Electric Power Research Institute, Palo Alto, Canada (2011)
4. Bobrek, M., Bouldin, D., Holcomb, D.E., Killough, S.M., et al.: Review Guidelines for FPGAs in NPP Safety Systems. NUREG/CR-7006, US Nuclear Regulatory Commission (2010)
5. EPRI. Guidelines on the Use of Field Programmable Gate Arrays (FPGAs) in Nuclear Power Plant I&C Systems. Technical report 1019181:2009, Electric Power Research Institute, Palo Alto, Canada (2009)

6. IEEE. Metastable Behavior in Digital System. Standard IEEE 1987, The Institute of Electrical and Electronics Engineers, New York, USA (1987)
7. IEC. Nuclear Power Plants-instrumentation and Control Important to Safety-development of HDL-Programmed Integrated Circuits for Systems Performing Category a Functions. Standard IEC 62566:2012. International Electrotechnical Commission (2012)

Research of Critical Reactivity Control Online Early Warning Technology in Nuclear Power Plant

Hong-Yun Xie(✉), Ji-Xue Li, Zhen-Yu Yan, and Ke Tan

State Key Laboratory of Nuclear Power Safety Monitoring Technology
and Equipment, China Nuclear Power Engineering Co., Ltd.,
Shenzhen 518172, China
xiehongyun@cgnpc.com.cn

Abstract. During the restart process of Pressurized Water Reactor (PWR) nuclear power plant, in order to let the reactor reach critical state safely and quickly, the critical reactivity control online early warning system can be designed. In this paper, the design scheme and implementation for critical reactivity control online early warning system are proposed, which can track and predict the nuclear power plant operation through two independent online simulation systems, and guide the operator to operate. The design scheme possesses various functions of reactivity online monitoring, calculate, predict, display and alarm; when the reactor does not reach the period limit or the reactivity does not reach the critical value, it can provide operator relative information and guide the operator to get back the critical state. This online early warning system has been realized and applied to operation, which possesses high availability.

Keywords: Nuclear power plant · Critical reactivity control
Early warning system · Online simulation

1 Introduction

The start-up process of the pressurized water reactor is roughly divided into three stages: the temperature and pressure rise, the subcritical state reaches the critical state and the promoting power. The lifting the control rod with the reactor from the subcritical state to the critical state is the most critical operation. In this process, the main task of reactive control is to control the boronization, dilution and control rod lift, so that the reactor can safely, smoothly and quickly reach the critical state.

In order to facilitate the control of the reactors of the nuclear power plant operators, the reactor is more secure, fast and smooth to reach the critical state, and the safety and economy of the reactors can be improved. The critical reactivity control can be set up in the power plant. This paper presents the design and function of the critical response control online warning system suitable for advanced nuclear power plant, the realization mode of the system, and gives the feasibility and necessity of the early warning system from the practical application.

Y. Xu et al. (eds.), *Nuclear Power Plants: Innovative Technologies for Instrumentation and Control Systems*, Lecture Notes in Electrical Engineering 455,
https://doi.org/10.1007/978-981-10-7416-5_13

2 Reactor Critical State Reactivity Control Principle

2.1 Reactor Reaches a Critical State

In the process of starting the pressurized water reactor, it is necessary to judge the critical state of the reactor. In practice, it is difficult to determine whether the reactor reaches the critical state by measuring the reactivity, usually by measuring the reactor multiplication cycle. According to this state, combined with the estimation of critical rods to control the introduction of reactivity, and determine whether the reactor reaches a critical state. At a certain shut down depth, when the neutron density is stabilized, the reactor multiplication cycle is calculated as:

$$\mathrm{T} = \mathrm{l}/(\mathrm{k} - 1) \tag{1}$$

The l is the average lifetime of the neutrons in the reactor per-second and k is the effective multiplication coefficient of the reactor.

When the reactor is near the critical, k = 1, the neutron density is almost constant, $|\mathrm{T}| \rightarrow \infty$. In the process of considering the neutron source, the reactor critical will have tens of seconds of positive period rather than infinity. There is a reactor with a neutron source. Before the reactivity is introduced, the reactor is in a cold shutdown state, the neutron density in the reactor is in a steady state, and the reactor cycle tends to be infinite. Near the critical, the reactor doubling cycle tends to be infinite. In the vicinity of the critical, the reactor multiplication period will enter the critical multiplication period identification region, the closer the reactor is to the critical, the longer the reactor multiplication period is in the critical multiplication period, In the critical multiplication cycle recognition area to maintain more than a certain time, that is to determine the reactor has reached a critical state.

2.2 Reactor Critical State Control

In response to the reactivity of the reactor from the subcritical state to the critical state, the reactor is initially operated by the operator, which is controlled by the operator in accordance with the best lifting procedure. The operator can control reactivity by the rod adjustment and the boronization or dilution. By observing the change in the reactor double period, operator can adjust the control rod and boron concentration in time and control the introduction of reactivity and rate. When the reactor is gradually approaching the critical state from the subcritical state, the reactor double period is gradually shortened until it enters the critical recognition region. At this time, the reactivity is stopped. After that, the reactor double period will gradually increase and the multiplication period will increase to a certain value. When the reactor is gradually approaching the critical state, the rate and increment of the reactivity is reduced until the reactor double period is maintained in the range. The reactor double period is reintroduced into the critical period recognition zone. Within a certain period of time, then the reactor has reached a critical state.

Based on this operation, two kinds of control methods are designed. The control method of fixed reactivity and the reactive control method using fuzzy control are introduced. The fixed reactivity control method need adjust rod several times with the introduction rate of reactivity unchanged. The fuzzy control effect is better. The upper limit of the reactor multiplication cycle is automatically adjusted according to the degree of criticality of the reactor, and the frequency of reactivity in the reactor is obviously reduced.

3 Design of Critical Reactivity Control Online Early Warning System

Critical Reactivity Control working process of the online early warning system can be divided into two parts. The first part is the operation of the approach to the critical state, and the other is the critical reactivity control online warning system operation.

3.1 Approaching Critical State

This part is mainly based on on-site collection of data, according to the start of the critical approach and the balance of the calculation of reactivity, to guide the operator to operate on the reactor.

According to the reactive equilibrium calculation, operator can calculate the critical rod position and critical boron concentration to determine the critical conditions. Then, the critical boron concentration, the differential value and the integral value of control rod, the temperature coefficient, the power coefficient and the xenon poison effect are calculated according to the collected data. The reactivity curve and the reactor neutron multiplication cycle are obtained by the controlled reactivity formula. According to the reactivity curve and the neutron multiplication cycle, the operation of the operator is guided by the alternation of the control rod and the dilution or boronization of the boric acid, so that the reactor gradually approaches the critical state.

3.2 Critical Reactivity Control Online Early Warning System

Critical Reactivity Control Online warning system operation flow chart is shown in Fig. 1.

Firstly, through the super real-time calculation based on the real-time simulation system, the change trend of the reactivity and the change of the neutron multiplication time in the critical process of the reactor are obtained in advance. The input condition of the critical reactivity online early warning system is available. During the start-up process, if the conditions of online warning are met, the warning signal is issued and the critical reactivity control online warning system is started. Each of the decisions in the critical reactivity online warning system requires the operator to determine whether to proceed to the next step. If the following steps are required, the same operation is taken.

After the on-line early warning system is started without additional intervention, we need calculate the amount of reactivity of the current state, the time required to reach

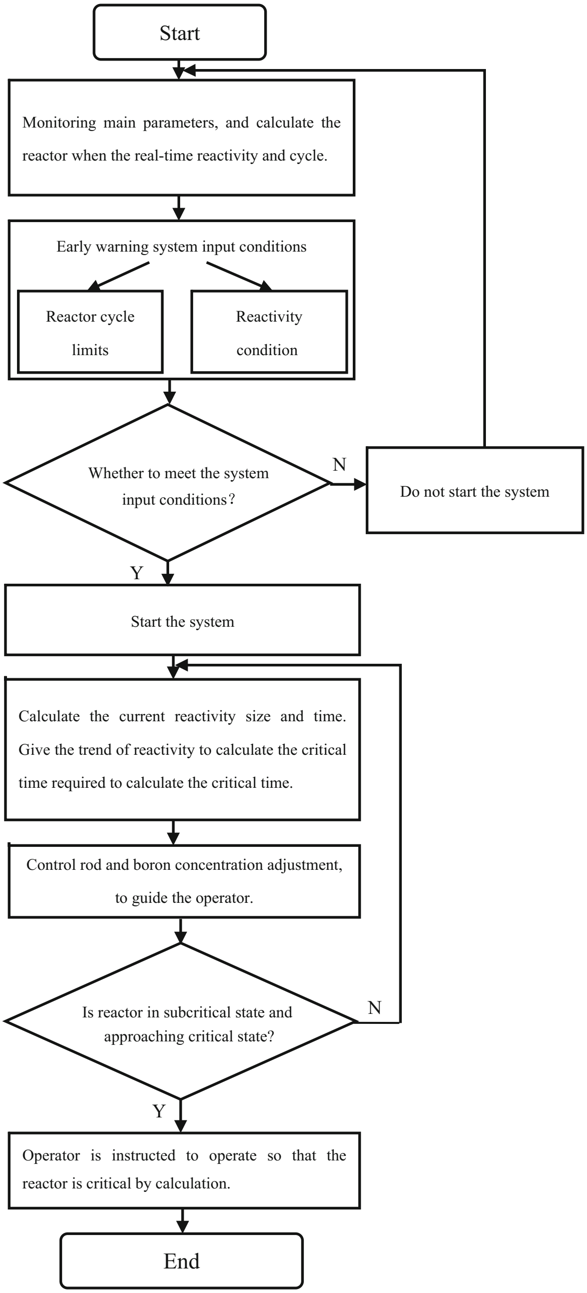

Start
Monitoring main parameters, and calculate the reactor when the real-time reactivity and cycle.
Early warning system input conditions
Reactor cycle limits
Reactivity condition
Whether to meet the system input conditions?
N
Do not start the system
Y
Start the system
Calculate the current reactivity size and time. Give the trend of reactivity to calculate the critical time required to calculate the critical time.
Control rod and boron concentration adjustment, to guide the operator.
Is reactor in subcritical state and approaching critical state?
N
Y
Operator is instructed to operate so that the reactor is critical by calculation.
End

Fig. 1. Critical reactivity control online early warning system flow chart

the critical state, and the time at which the warning signal is issued when the online warning system is in operation. We can anticipate the possible malfunction in advance, analyse the cause of the malfunction, and give the time for the change in reactivity and the time required for criticality.

According to the critical approach at the time of start-up, the operator can be guided by adjusting the power control rod and boron concentration. Approximate critical operation flow chart is shown in Fig. 2. In this process, according to the on-line simulation, the critical boron concentration and critical rod position need to be recalculated after each calculation to obtain changes in the reactor and the change of the cycle. We need further calculate the control rod speed and dilution or boronization rate.

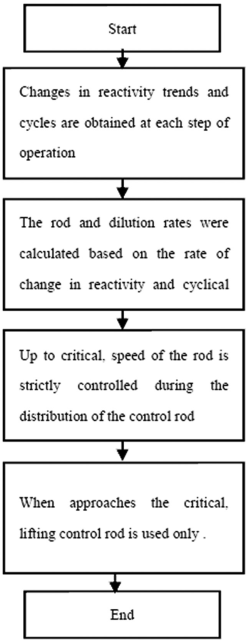

Start
Changes in reactivity trends and cycles are obtained at each step of operation
The rod and dilution rates were calculated based on the rate of change in reactivity and cyclical
Up to critical, speed of the rod is strictly controlled during the distribution of the control rod
When approaches the critical, lifting control rod is used only .
End

Fig. 2. Online warning system operation flow chart

By re-determine the recovery process through the control rod and boron concentration adjustment, the reactor is back to the subcritical state gradually approaching the critical state with no neutron multiplication cycle less than 18 s, or reactivity is greater than 0. It is above-critical state. If the reactor is above-critical state, the operator is instructed to operate the reactor to a critical state. If the control rod and boron concentration adjustment, it will not occur above-critical accident in the start-up process, then we can exit the critical reactivity control online warning system. If the reactor in the reactor process in above-critical state, then we need to recalculate.

4 Implementation of Critical Reactivity Control Online Early Warning System

4.1 Feature Design

Critical Reactivity Control online early warning system can be calculated by two sets of parallel online simulation models, one for real-time calculations and the other for super real-time calculations. The real-time model is used to predict the change trend of the reactivity and the neutron multiplication period in the field, and the super real-time model is used to predict the reactivity and neutron multiplication cycle during the start-up process. The main implementation process is as follows.

- In the critical reactivity control online warning system, there are two sets of the same online simulation model for parallel computing, two sets of models are carried out independently. One set is based on the actual operation of the power plant real-time model, the other is based on the actual operation of the power plant super-real-time simulation model. All of the input conditions and boundary conditions of the two sets of online simulation models are consistent. The real-time simulation model can predict the change trend of reactivity and the change of neutron multiplication period in the future heap. Therefore, it is possible to determine whether it is necessary to put a critical reactivity control online warning system through the change trend of the reactivity and the neutron multiplication period to guide the calculation of the real-time model.
- If we need to start the critical reactivity control online warning system, we need to recalculate the current state of the critical rod and critical boron concentration. With the critical bar and critical boron concentration, the on-line early warning system instructs the operator to operate again to determine if it is a super-critical state, and that does not cause a super-critical accident. After each operation, the real-time model needs to be re-passed to the super-real-time simulation model, so that the current state of the time to re-super-real-time prediction.
- After each operation, parallel simulation of the two sets of simulation system, the reaction trends and neutron multiplication cycle, through the calculation of the operator to guide the next step.

4.2 System Design

The critical response control online early warning system operation interface is divided into three parts: monitoring, early warning and recommended measures. The specific displays are shown in Table 1. The monitoring module shows the real-time reactivity balance, boron concentration, core and fuel temperature. When the online warning system is put in service, the core simulation model enters the super real-time operation mode and reacts from 2 times to 8 times (optional) real-time speed. The simulation model will predict the time to reach the critical time and the double period, the current multiplication time value and the arrival time value are displayed in numerical form on the warning module. After the warning occurs, the warning indicator light of the warning module will light up and the operator in the recommended action prompts the operator to take actions. In the proposed action module, the power rod is divided into the current rod and the target rod position. The operator is recommended to manually adjust the power rod to the target value; and the dilution or boronization adjustment. It shows dilution and boronized water volume or acid volume target value, it is recommended that the operator manually adjust the boron concentration to the target value.

Table 1. Critical reactivity control online early warning system operation interface content

Module	Operation visualization interface
Monitoring	Real-time reactive equilibrium, boron concentration, core temperature, fuel temperature
Early warning	Early warning indicator, reactivity and multiplier set point, current doubling time value, predicted critical time value
Recommended Action	G control rod position display and target value, dilution target value, boronization target value

5 Conclusion

In this paper, the control scheme of reactivity with re-reaching critical reaction is studied, the design scheme and realization method of critical response control online warning system are proposed. This online early warning system has been successfully applied after design verification and feasibility assessment. The evaluation results show that the system can monitor the trend of reactivity in real time and give an early warning when the reactor is not up to the cycle limit or reactivity, and prevent the super-critical state. The whole system is flexible and stable, and providing online warning support for critical reactivity control of nuclear power plants.

References

Zhang, J.M., Jiang, J.: Nuclear Reactor Control. Atomic Energy Press, Beijing (2008)

Guangdong nuclear power training center: Devices and systems of 900 MW PWR. Atomic Energy Press (2007)

Maillart, H.: Design of the I&C for the European pressurized water reactor. Nucl. Eng. Des. **187**, 135–141 (1999)

van der Hoek, A.: Configurable software architecture in support of configuration management and software deployment. In: International Conference on Software Engineering, Los Angeles, USA (1999)

Prehler, H.J.: Advanced I&C systems for nuclear power plants feedback of experience. In: International Conference on Nuclear Energy in Central Europe, Portorož, Slovenia (2001)

Analysis and Optimization of Layout Solution of Instrumentation and Control (I&C) Cable Channel for Digital NPP

Ying Meng(✉), Nian-Wu Lan, Tian Deng, and Li-Ping Zhong

State Key Laboratory of Nuclear Power Safety Monitoring Technology and Equipment,
China Nuclear Power Design Co., LTD, Shenzhen, China
mengying@cgnpc.com.cn

Abstract. At present, a series of engineering problems are encountered in NPPs (Nuclear Power Plants) built or under building, such as cable channel overload, cable cost increase and cable layout difficulty. Optimization of Layout Solution of I&C Cable Channel for digital NPP can eliminate the problems and improve the construction quality. The optimization can be realized by analysis and design of DCS layout in different islands, coordination layout between cable channel and equipment, and finally the cable channel layout solution under special circumstance. Based on the optimization of layout solution of I&C Cable Channel, the overload problem of I&C cable tray can effectively be controlled in NPP. Also the optimization can reduce cable cost to improve the reliability and economical efficiency for digital NPP. The economy and reliability of engineering construction can be integrally increased.

Keywords: DCS · Cable channel layout · Overload · Isolate principle
Optimization

1 Introduction

With the rapid development of modern nuclear power technology, the function of various systems continues to be improved for the improvement of safety and reliability of 3rd generation advanced NPP. The normal function of process system is achieved by complete control and monitoring system under control of the operators [1]. Since the digital control system (DCS) has been widely used in NPPs, more and more systems are integrated into DCS because of the advantages of decentralized control, centralized management and high reliability [2]. As consequence, the scale of DCS is expanded and the cable quantity is largely increased.

At present, a series of engineering problems, such as cable channel overload, cable cost increase and cable layout difficulty, are encountered in NPPs built or under building [3]. The control and measurement cables are the neural network of NPP, therefore any problem of the cable will directly affect the normal operation. Under this circumstance, the optimization of cable channel layout solution for digital NPP gains its importance. During the layout design of equipment, the feasibility and rationality of the cable channel

Y. Xu et al. (eds.), *Nuclear Power Plants: Innovative Technologies for Instrumentation and Control Systems*, Lecture Notes in Electrical Engineering 455,
https://doi.org/10.1007/978-981-10-7416-5_14

layout should be fully taken into account, so as to reduce the construction cost and improve the construction quality of cable channel layout.

The cable channel overload problem has brought much difficulty for construction of NPP. The frequent modification and detour of cable path cannot help much for the problems. With the expansion of DCS scale, the problem of cable channel overload could be more serious in new NPPs, especially for the electrical equipment rooms in nuclear island electrical plant, which are the layout rooms of DCS cabinets. Meanwhile the isolation of security level and non-security level signal cable hasn't been considered in the early cable planning, therefore the identification level increase of non-security level signal cable results in the cost increase. Outside of the nuclear island plant, the problems have been encountered that the cables of different redundancy sequence or different security level are laid in the same cable channel, and safety related cable and low level cable are laid in the same cable channel. Those mentioned problems are complex to solved, which results in significant cost increase in design, procurement, construction and other aspect of engineering project.

Based on engineering practice and layout design analysis, the overload of control and measurement cables, increase of high level cable and irregularity of some cable channel construction, all those problems above are due to three factors: (Table 1)

Table 1. Three factors and their description

Factors	Description
Large DCS scale	Too many system functions included in DCS control and monitoring. The cable layout is concentrated and space is not enough in the electronic equipment rooms
Utilization rate of cable channel	Lack of coordination of equipment layout and cable route planning. Some cable route is not well planned and the use efficiency is low for cable channel
Design rules of special cable channel layout	In special circumstances the design of cable channel layout is not detailed enough. It is difficult to meet the requirements of common-mode point isolation for cable channels of different security sequences. The principle of cable channel isolation for related circuit [4, 5] is complex, which raises construction difficulty and decrease construction quality

Therefore those three factors mentioned should be considered in the overall planning stage of layout solution of I&C cable channel for digital NPP. Meanwhile effective optimization measures should be taken to ensure the reasonable layout of I&C cable channel and construction quality of cable laying.

2 Isolation Principle Analysis

The optimization of I&C cable channel for digital NPP should meet the requirements of relevant domestic and foreign design standards. Those design standards include isolation distance for different voltage level, safety distance between process pipe and other items and same support requirement for cable channel as the requirement for the whole NPP. All the requirements should be met during the design of the cable channel.

The main difficulty for I&C cable channel layout is to meet the isolation requirements of different safety level or protection group and the relevant 1E circuit.

There are special chapters in the RCC, IEC, IEEE, national standards and other series of standards for the isolation requirements of NPP cable channel. The principles in the standard RCC-E-D7000-2005 are relatively general, while the principles in national standard GB/T-13286-2008 come from IEEE standard. There is no need for the comparison and analysis of the two standards.

IEC 60709-2004 [4] and IEEE 384-2008 [5] both emphasize the independence of redundant safety divisions is realized by the physical separation and the electric separation. The methods to achieve the separation are same, too. The cable channels of different safety divisions or protection groups should be separated and achieve the requirements of physical separation. The non-safety class cables should be separated from the safety class cables following the requirements of redundant safety divisions. If the non-safety cable routing cannot achieve the separation requirements near the safety class cables, these non-safety cables have to be designed as the associated circuits. Then they belong to the safety class circuits related. The associated circuits should be separated from other redundant safety divisions, unless the associated circuits are analyzed to demonstrate that safety circuits are not degraded below an acceptable level [4, 5]. The main principles are same in these two different standards.

The comparison details of the standards are showed as Table 2. For separation distance, IEEE 384 defines the minimum separation distance by different areas. The separation methods are more applicable. For associated circuits, the descriptions of two standards are same.

After the comparative analysis of the standards, IEEE 384 is more rigorous and has more detailed measure. Therefore common-mode isolation requirements of different safety-level cable channel and the cable channel design of relevant circuit should follow this standard.

3 Optimization of Layout Solution

The layout solution of I&C cable channel for digital NPP, should be in the overall stage. The space of electronic equipment room should be considered, as well as conventional cable channel design methods and the cable channel isolation design under special circumstances.

Against the factors of cable routing problems, three aspects of optimization are proposed according to the layout rules. Summarized as Fig. 1:

At first, the electronic equipment rooms should be laid out in both nuclear island and conventional island, and based on the control and monitoring functions by DCS cabinets, a reasonable allocation of DCS cabinets should be done to increase the cable channel layout space in electronic equipment rooms.

Secondly, the equipment layout and the cable channel layout should be combined with each other. The relative position of holes, shaft and DCS cabinets should be reasonably planned. A reasonable allocation of DCS cabinets function should be done. The layout distance of cross-plant and cross-rooms cables should be shortened and the

Table 2. Comparison and analysis of isolation requirements between IEC 60709 and IEEE 384

Technical items	IEC 60709 requirements	IEEE 384 requirements
Separation distance	6.2 Separation Separation distance of redundant cables: 30 cm for horizontal cable tray, 80 cm for vertical cable tray。 If the distance cannot follow the requirements, the cable tray should be sealed with the barriers of fir-resistant material	5.1 Cables and raceways These areas of NPP shall be classified as non-hazard areas, Limited-hazard areas and Hazard areas. Define the different minimum separation distance for different kinds of cable tray in the different areas, based on the material of cables and metal pipe achieves the requirements of IEEE/ASTM / NEMA. If the distance cannot follow the requirements, the cable tray should be sealed with the barriers of fir-resistant material. Also give out the minimum size of barriers
Associated circuits	6.2.3 associated circuits If the non-safety cable routing cannot achieve the separation requirements near the safety class cables, these non-safety cables have to be designed as the associated circuits. Then they are a part of the safety class circuits related. The associated circuits should be separated from other redundant safety divisions, unless the associated circuits are analyzed to demonstrate that safety circuits are not degraded below an acceptable level	4.5 associated circuits The description is same with IEC 60709

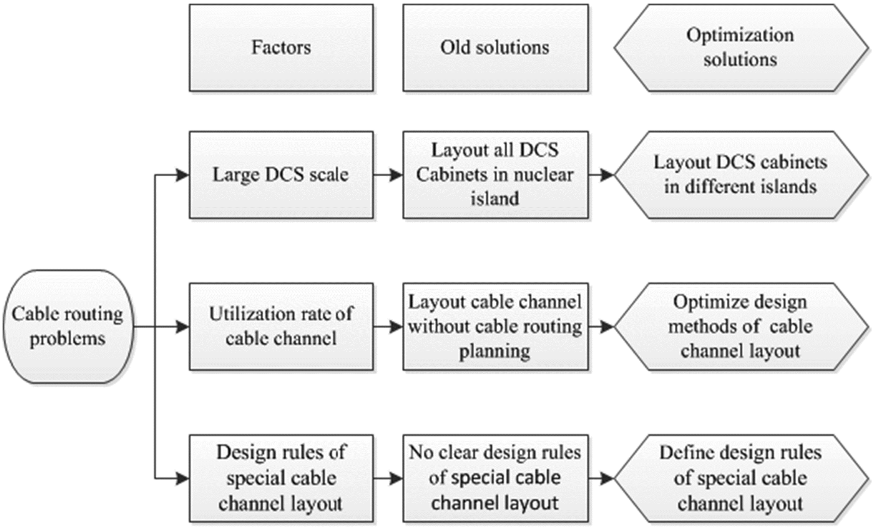

Factors
Old solutions
Optimization solutions
Cable routing problems
Large DCS scale
Layout all DCS Cabinets in nuclear island
Layout DCS cabinets in different islands
Utilization rate of cable channel
Layout cable channel without cable routing planning
Optimize design methods of cable channel layout
Design rules of special cable channel layout
No clear design rules of special cable channel layout
Define design rules of special cable channel layout

Fig. 1. Summarize of optimization solutions

bypass cable should be reduced in the cable channel. All those measures can enhance the service efficiency of cable channels.

Finally, for the more complex special area in the NPP, a detailed analysis of region and category should be carried out, and the detailed isolation planning of cable channel should be made for the common mode and the related circuit design of the redundant sequence, and the corresponding isolation measures should be taken. Especially for the cable channel design of relevant circuit in nuclear island, a new NPP which has the condition to implement, should adopt cable channel program where 1E circuit and NC circuit are separately set up. For a NPP where the cable channels of different safety sequence lack of distinction, it'd be better to improve the safety level of equipment in NC circuit. For the plant without safety requirements, it only needs to set separate cable channels for different sequences and to set up a separate cable channel for the cable of important SR function signal cable and to meet the requirements of safety distance.

4 Conclusions of Optimization of Layout Solution

Based on the research results above, the overload problem of I&C cable can effectively be controlled in NPP. The economy and reliability of engineering construction can be integrally increased.

At present, this optimization method has been adopted in a certain NPP under construction in China and the overload problem of electronic equipment rooms in nuclear island has been greatly improved. As a result the plot ratio of related cable channel decreases from more than 90% to less than 70% and more than 10 million of construction cost has been saved. The details are showed by Table 3.

Table 3. Optimization results

	Before optimization	After optimization	Optimization results
Cable volume rate	90%–100%	≤70%	No overload problem
Cable length	1800000 m	90000 m	The cost has been reduced by two million dollars
Cable routing condition	Some of associated circuits cables are routed in the same tray with non-safety cables	The cables of important signals are routed in the special cable channel	Eliminate the risk of low grade cables affecting important functional signals

5 Expectation of Layout Solution of I&C Cable Channel

The optimization research of layout solution of I&C Cable Channel for digital NPP is of great significance to the safety, reliability and economy of NPP construction.

The conclusions of this research make effective design guidance and construction protection for the domestic independent research and development of advanced 3rd generation NPP, and provide design basis for the improvement of NPP built or under construction. Meanwhile, it is a good example of significance for layout design of I&C cable channel in the follow-up NPPs. Also the design rules of special cable channel layout are being applied to add into the industry standard.

References

1. Dong, X.S.: Study on upgrade with digital I&C NPP. In: Nuclear Science and Engineering, 31st edn., Shenzhen (2011)
2. Zhang, L.Q.: Discussion on incorporating monitoring and control functions of electrical system into DCS for CPR1000 NPP. In: Nuclear Science and Engineering, 33rd edn., Shenzhen (2013)
3. Zhang, S.D.: Detection signal transmission system for NPP, China (2015). 2014207488577
4. IEC 60709-2004: NPPs-I&C system important to safety-Separation. International Electro Technical Commission, Switzerland
5. IEEE 384-2008: Independence of Class 1E Equipment and Circuits. Electrical and Electronics Engineers, USA

Research and Comparison of Combination Control Schemes Between Reactor and Turbine in Different PWR Nuclear Power Plant

Xu-Feng Wang(✉) and Le-Yuan Bai

China Nuclear Power Engineering Co., Ltd., Shenzhen 518172, China
wangxufeng@cgnpc.com.cn

Abstract. In pressurized water reactor nuclear power plant (PWR), the steam generated by nuclear reactor is used to drive the steam turbine, which turns generator to produce electric energy. The power combination control between reactor and turbine is directly related to the conversion and balance between nuclear energy to electrical energy, so it is very important for the plant. The safe and reliable combination control between reactor and turbine can ensure the plant safely and economically. This paper researches the power combination control between reactor and turbine, and compares the implementation schemes in different plants, and puts forward the advantages and disadvantages, which can provides reference or assistance for similar investigation on other plant.

Keywords: PWR · Combination control · Reactor and turbine
Two-types of steam turbine

1 Introduction

In pressurized water reactor nuclear power plant (PWR), the steam generated by nuclear reactor is used to drive the steam turbine of conventional island, which turns generator to produce electric energy. The power combination control between reactor and turbine is directly related to the conversion and balance between nuclear energy and electrical energy, so it is very important for the plant. The linear control program between the average coolant temperature and reactor power is used for steady state operation in PWR, as well as the reactor-follow-turbine mode which means that the reactor power is regulated according to the turbine load. The combination power control between reactor and turbine is composed by reactor power control, turbine load control and the requisite interfaces which assure the coordination between reactor and turbine, the balance between nuclear energy and electrical energy, and the stability and security, as well as economic of the plant.

Two types of steam turbines are used in the operated plants of a nuclear power corporation, which are named A and B turbines. Because of the differences of turbine governing structure and scheme between A and B turbines, the differences of commination control between turbine and reactor shall be researched.

Y. Xu et al. (eds.), *Nuclear Power Plants: Innovative Technologies for Instrumentation and Control Systems*, Lecture Notes in Electrical Engineering 455,
https://doi.org/10.1007/978-981-10-7416-5_15

2 Functional Requirements

The essential functional requirements for combination control between reactor and turbine include the reactor power tracking target, the reactor overpower prevention, the reactor power rapid decrease, frequency regulation limit, etc.

The reactor-follow-turbine mode demands that the reactor power is regulated according to the turbine load in real time. The reactor needs a physical parameter as power tracking target which represents the turbine load. As the reference set point of the power control rod position, the target load can be one of the following parameters: turbine load reference (signal 72), turbine opening reference (signal 74), turbine inlet steam pressure reference (signal 76), and steam flow limit (signal 82), as shown in Fig. 1.

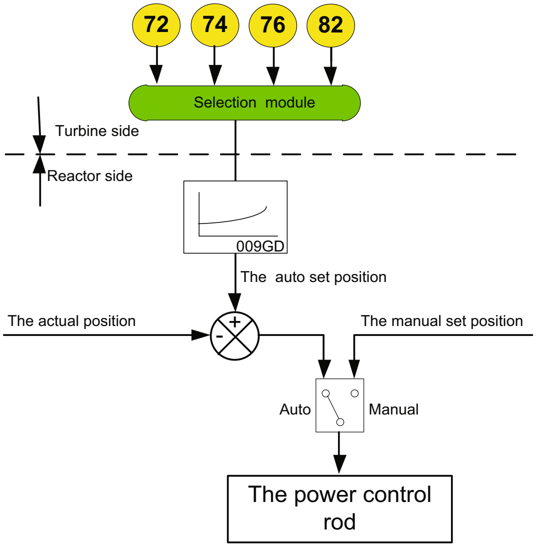


Fig. 1. The mechanism of load set point for reactor power control

To prevent the reactor from overpower, the steam turbine shall be of a load limitation function to ensure the safety of the reactor.

In some conditions (such as, reactor overpower, reactor over-temperature, etc.), the reactor has to fast decrease power for the purpose of protection of itself, thus it can returns to safety status. The implementation of the method is that the nuclear island immediately notifies turbine to decrease load rapidly in the condition of the reactor load rejection. Then the reactor tracks the changes of steam turbine load, and finally realizes the purpose of rapid decrease.

In normal operation, the nuclear power plant should have a certain capacity to participate in frequency regulation to support for the grid. However, the power grid fluctuations in a large scale will cause a disturbance in the turbine load control, and also the change of the reactor power control, which affects the reactor adversely.

3 Differences and Research in Combination Control

3.1 Differences of Functional Interface

For type A turbine, the reactor rod control system principle, the steam turbine control (DEH) principle and the interfaces are shown in Figs. 2 and 3. The power control of steam turbine includes two modes: manual open loop and automatic closed-loop power. The reactor governing system (RGL) is informed by signal 80 whether the turbine is in automatic or manual control. When the steam turbine is in automatic mode, RGL tracks the sum of the turbine load reference (signal 72) and the effect of frequency control (signal 78). In manual mode, RGL tracks the sum of the turbine open reference (signal 74) and the effect of the frequency contribution (signal 83). In order to prevent the reactor from power overshoot, and limit the impact of power grid frequency fluctuations and turbine accidents on the reactor, the turbine will be in the load limited model (indicated by signal 79). RGL will track steam flow limit signal (signal 82) or turbine inlet steam pressure reference (signal 76), to ensure the safety of the reactor. When there is a demand for rapid load decrease of the reactor itself or others (such as feed water pump fault, generator fault, generator transformer protection, etc.), the signal of turbine load runback (signal 71) is triggered. The reactor fast tracks the turbine opening reference (signal 74) as the target load, to satisfy the protection of the reactor or turbine, etc.

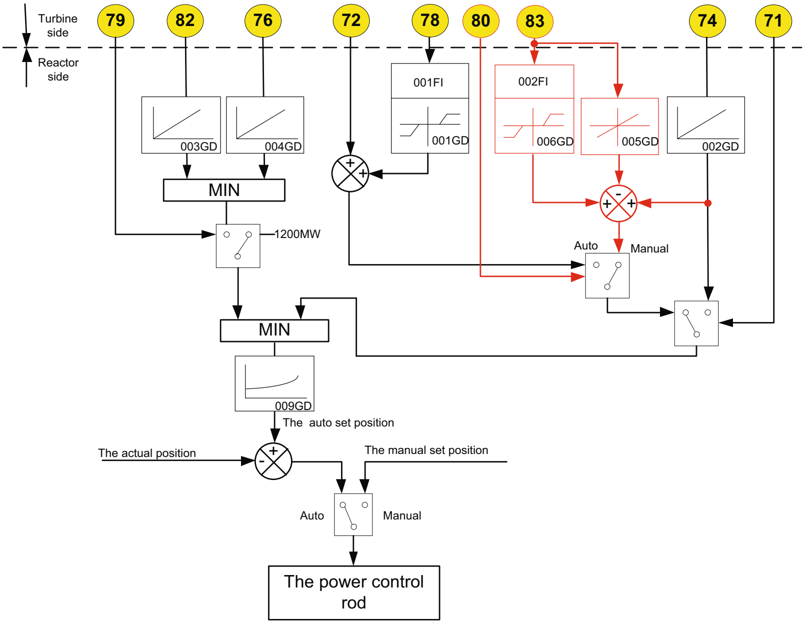


Fig. 2. The mechanism of reactor rod control system

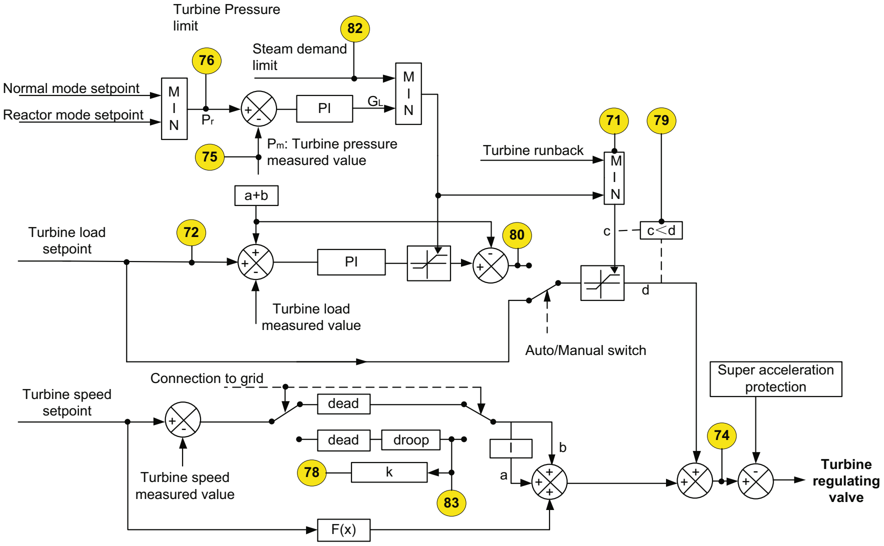


Fig. 3. The principle of DEH for turbine A and the interface with reactor

For type B turbine, there is only automatic closed-loop power control mode, and no manual open loop power control, as shown in Fig. 4. Therefore, the reactor side will not need to set the load target of manual mode in power combination control, namely that the red part in Fig. 2, signal 80 and 83 is canceled for type B turbine. The switching module will maintain at the automatic side in the same time.

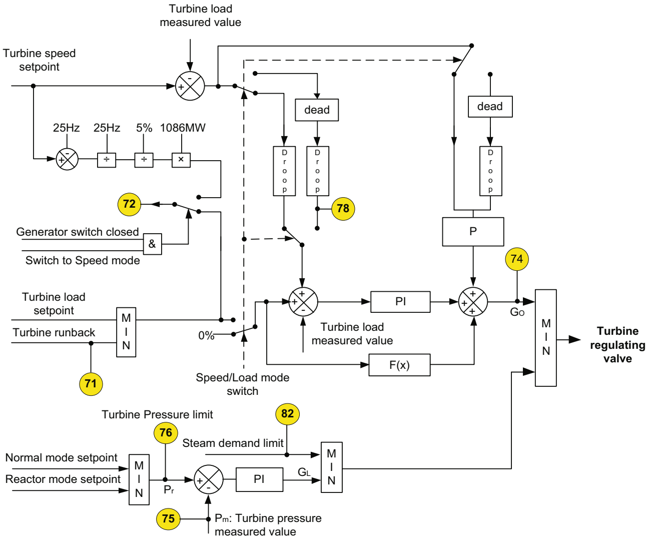


Fig. 4. The principle of DEH for turbine B and the interface with reactor

3.2 Differences of Turbine Load Reference

For type A turbine, the turbine load reference (signal 72) to the reactor is directly from the power set point given by the operator, as shown in Fig. 3.

For type B turbine, the power set point is provided by the operator when the turbine is switched to the load control mode after synchronization. At the same time, the turbine can also be switched to speed control mode according to the consistency principle of power and frequency. In speed control mode, the power set point is provided by speed difference (ΔS) between speed set point and its measured value after proportional element (diversity factor, λ). As known from Fig. 3, if copy the implement of type A turbine, the signal 72 of type B turbine will be 0 when switched to speed control mode. The reactor power will automatically fall down to 30% rate power (P_n) if the reactor power is greater than 30% P_n. In order to maintain power level, the turbine will continue to open valve, causing the over cooling of reactor and nuclear safety accidents. So it is unsuitable for type B turbine to copy the signal 72 implementation method of type A turbine.

According to the consistency principle of power and frequency, when type B turbine is switched to the speed control mode, the value of signal 72 shall be:

$$\text{signal 72} = \frac{\Delta S}{S_n \times \lambda} P_n \tag{1}$$

The speed setting value must be more than the rated speed of 1500 RPM (S_n), otherwise the turbine will stop automatically. When the operator switches turbine from load mode to speed mode, the speed setting value will be calculated out instantaneously based on the measured value of power before switching, in order to ensure the undisturbed switching. After switching, it is to increase the speed setting value in order to increase the power, and vice versa. If the diversity factor λ is 5%, the speed setting value will be increased to 1575 RPM at full power, and reduced to 1500 RPM at zero power.

In case of load rejection to the house load for type B turbine, the turbine control will be in speed mode. At this time the speed set point is also 1500 RPM. The rated speed will not be 1500 RPM, but will automatically reduce to the corresponding value for house load. Due to the power supply frequency, the operator should immediately manually increase the speed setting value to ensure that the rated speed automatically increases to 1500 RPM.

3.3 Differences of Turbine Load Runback

For type A turbine, the turbine load runback signal (signal 71) is used as the upper limit of the load control loop output. When the runback signal produced, because the runback target is less than the output value of load circuit before drop, the turbine automatically decreases load. At the same time, the power set point automatically tracks the power measured value to ensure that power control is stable and undisturbed, as shown in Fig. 3. Because signal 71 of type A turbine is the upper limit of the load control loop output (after PI), the limit directly impacts on the steam demand (SD). In case of feed water pump failure, the turbine efficiency may decrease (caused by the rise of condenser pressure), so the load control loop output shall be more than 50% SD to maintain 50% P_n. However, the turbine may not be able to operate in the power setting level because of the limited of signal 71.

Therefore, it is more appropriate for the target load of runback to replace the power set point after comparing. Type B turbine adopts this approach as shown in Fig. 4.

Compared to that of type A turbine, signal 71 of type B turbine takes part in the integral element of load control loop, which may affect the rapidity of runback and cannot lead the turbine down to the target power. The worst condition from the rated power down to 10% Pn at the rate of 200%/min is simulated by MATLAB. The left figure of Fig. 5 is the result of type A turbine runback which directly effects on the load controller output, and the right one is the result of type B turbine runback which used as power set point goes through the integral element. According to the results, the runback of two type turbine from the rated power down to 10% Pn are identical, and integral element does not affect the runback.

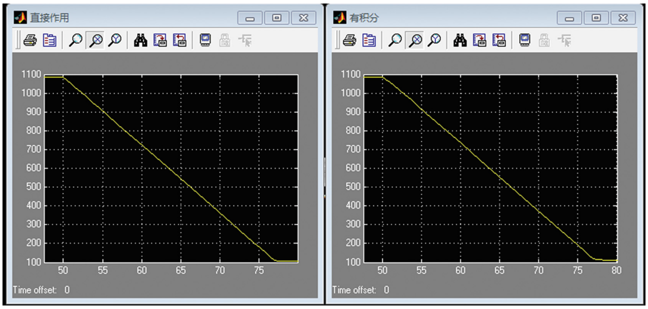


Fig. 5. The load runback curves of turbine A and B

Because it can avoid that the turbine cannot run on the setting power level after load runback in case of the turbine efficiency fall, the load runback implementation of type B turbine is better than that of type A turbine.

3.4 Differences of Turbine Load Limitation

For type A turbine, the load limit signal is used as the upper limit of the load control loop output. When the load limit signal is smaller, the load limit works; otherwise, the load limit exits. In case of load limit, the power set point automatically tracks the power measured value to ensure that power control is undisturbed, as shown in Fig. 3.

For type B turbine, DEH is of modular structure and has strong scalability. Due to the requirements of different users, DEH can be extended by more sub controller, such as the main steam pipe pressure limit controller, high pressure cylinder exhaust temperature controller, high pressure cylinder pressure ratio controller, etc. Multiple controllers go via a selector and the minimum as the final effective output to adjust the turbine valves. Because of the extensibility of DEH, the function of load limit can be implemented as a sub controller for type B turbine, as shown in Fig. 4. The function of load limit includes pressure limit and steam flow limit, and pressure limit is divided into the normal pressure mode and the reactor pressure mode. For type B turbine, pressure limit and the steam flow limit act on the original speed/load controller as independent sub controllers, and the minimum of three controllers finally adjust the turbine valves.

However, the PI operation of pressure limit between A and B turbines are different. For type A turbine, the ratio integral PI is shown in Fig. 6. When the measured value of turbine pressure (P_m) is below P_r, the output of the proportional part (G_p) is 105% SD, and the output of the integral party zero. The total output G_L is 105% SD, and there is no limit to load loop. When P_m is beyond P_r, G_p is less than 105% SD, the integrator output increase gradually and G_L decreases. The G_L plays the role of pressure limit when it is less than the steam demand from the normal load circuit. When the measured pressure reduces to the reference pressure, the integrator resets, G_L is back to 105% SD, and the pressure limit exits.

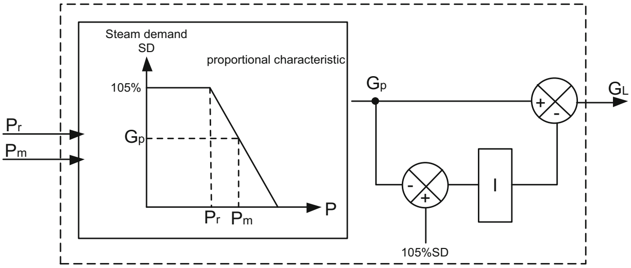


Fig. 6. The PI part of load limit by steam pressure for turbine A

For type B turbine, the ratio integral PI is shown in Fig. 7 (right). When the measured value of turbine pressure (P_m) is below P_r, the total output G_L is always 5% more than the output of the speed/load circuit (G_o). When P_m is beyond P_r, G_o tracks G_L, to implement the undisturbed switch.

Compared to type A turbine, type B turbine can basically implement the undisturbed switch in pressure limit. For type A turbine the pressure limit PI of the type A turbine has disadvantages: When 96% signal occurs, the output of reactor model gradually decrease from 105% after PI, causing that turbine power has a significant fluctuation, as shown Fig. 7 (left); At the same time, when the pressure is close to the reference pressure, the pressure limit works and then exits quickly, causing a power fluctuation because of lack of dead zone.

Therefore, the pressure limit control of type A turbine shall be optimized in the subsequent plant, and the method of rapid tracking of type B turbine is recommended.

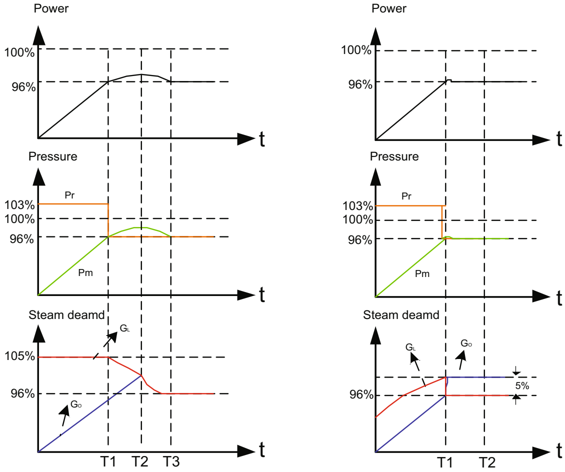


Fig. 7. The curves of load limit by steam pressure for turbine A and B

4 Conclusions

Through the study of this paper, the basic principle of combination control between reactor and turbine in PWR nuclear power plant is researched, and contrastive analysis between type A turbine and type B turbine in combination with reactor are carried out, which can providing reference and assistance for the combination control research on other type of reactor and turbine.

Study on Three-Dimensional Virtual Visualization Monitoring Method and System of Real-Time Information in Nuclear Power Plant

Jing Zeng[1(✉)], Tian-Nan Yang[1], Zhen-Yu Yan[2], and Zhi-Yong Li[1]

[1] Yangjiang Nuclear Power Co., Ltd., Yangjiang 529941, Guangdong, China
z-jing@cgnpc.com.cn
[2] China Nuclear Power Design Co., Ltd., Shenzhen 518116, China
yan_zhenyu@cgnpc.com.cn

Abstract. The real-time information of NPP (nuclear power plant) production can be monitored by three-dimensional visualization method and integration of DCS (Digital Control System). In this paper, the three-dimensional virtualized visualization modeling and dynamic effects method of DCS operation system are described. The three-dimensional virtual visualization modeling of the nuclear reactor core and the transparent reactor method are researched. This paper briefly analyses both the data connection method between the real-time data of the NPP and the three-dimensional virtual visualization system, and the closed-loop design method of the thermal visualization of the thermal hydraulic three-dimensional visualization, which using the container as the reactor core. This method can be used outside the three-dimensional virtual visualization system to realize the connection with the simulator system of NPP, and can be used in post-analysis after an accident.

Keywords: Digital control system
NPP real-time information monitoring system
Three-dimensional virtual visualization · Replaying

1 Introduction

DCS technology is the NPP within the control level and process monitoring level composed of communication network as the link of multi-level computer system, integrated computer, communication, display and control technology, the basic idea is decentralized control, centralized operation, Flexible configuration and easy configuration [1, 2].

Three-dimensional visualization technology is a new technology with the development of computer hardware and software technology [3]. Firstly, designers use the Three-dimensional animation software to create a virtual world, build the model and scene base on the shape, size, movement characteristic of the object, then setup the trace of the model according to its dynamic movement rules. A Three-dimensional visualization scene will make after finishing all the calculators by the computer [4, 5].

Y. Xu et al. (eds.), *Nuclear Power Plants: Innovative Technologies for Instrumentation and Control Systems*, Lecture Notes in Electrical Engineering 455,
https://doi.org/10.1007/978-981-10-7416-5_16

KNS (Nuclear power plant real-time information monitoring system) is a nu-clear power plant real-time information monitoring system [6]. It's main function is to establish real-time and historical database by collecting the producing process data. KNS can provide the whole plant production process real-time management and monitoring services for the operation, maintenance, technical support and other field.

KNS is an extension of the DCS system of the NPP. The system adopts the same style as the DCS intermediation interface. It can only characterize the running status of the NPP through the static element, dynamic numerical display and the colour change of the two-dimensional plane icon [7].

The HMI (Human Machine Interface) of the current NPP DCS and KNS adopts the two-dimensional display technology, it can represents the operation of NPP by the changes of graphic icon's colour and numerical. These methods have a greater limitation; it can't monitor the internal structure and operating status of the equipments. All pipelines, containers, and equipment are static primitives that can't characterize the operation of the media inside the pipe.

To solve these limitations, this paper provides the method to virtual all operating systems and equipments of NPP by three-dimensional visualization technology, and development of three-dimensional visualization of the model of reactor, the development of a container as the core of the virtual three-dimensional visualization of the media loop. Three-dimensional visualization system can virtual the dynamic effects of equipment, containers, medium of pipe internal by collect the real-time data of DCS system.

2 Create the Three-Dimensional Virtual Visualization System

Three-dimensional virtual visualization system of NPP can be created by three-dimensional virtual technology. Three-dimensional virtual models should include plant, operating system and important equipments. And realize the connection between production real-time data and three-dimensional virtual visualization system, the three-dimensional animation and animation effects can displayed on the HMI, and then to achieve the monitoring of real-time operation of NPP.

2.1 Create the Three-Dimensional Virtual Visualization of NPP

Create the three-dimensional visualization model of NPP, such as reactor plant, containment, electrical plant, conventional island plant and other plants. Construct virtual three-dimensional environment scenes as the same as the actual NPP by get the plant design parameters. We can roam anywhere in the three-dimensional visualization model of NPP by the interaction of HMI.

2.2 Create the Three-Dimensional Virtual Visualization of NPP Operation System

The three-dimensional virtual visualization of nuclear power plant operation system is based on the process control system of DCS in the NPP; it can be established by the computer graphical interface. NPP reactor core, a circuit operating system, the second loop operating system, electrical system, containment system and other operating related systems included in this virtual system. And all the pipelines are modeled by three-dimensional virtual visualization technology. The animation effect of internal medium in the pipeline can represent according to the real-time production data of the NPP.

2.3 Create the Three-Dimensional Virtual Visualization of Important Equipments

The important equipments related to the operating of the NPP can be modeled by three-dimensional virtual visualization technology with high precision. All three-dimensional virtual models are created based on the operating principle and characteristic of the equipment. Pressure vessels, steam generators, steam turbines, generators, regulators, pumps, valves, electrical switches, containers, heat exchangers and other equipments included in this system.

2.4 Create the Three-Dimensional Virtual Visualization of Reactor Core

The three-dimensional virtual visualization model of the reactor core in the NPP can be constructed to show the appearance and internal structure of the reactor core. The dynamic model of the reactor core can reflect the changes of the temperature of the water, the changes of the core temperature with control rod and the direction of the water in the reactor core.

3 Realization of Three-Dimensional Virtual Visualization Dynamic Model

3.1 The Design Process of Three-Dimensional Virtual Visualization Models

Model is the basis but also an important part of the three-dimensional virtual visualization system. Thermodynamic system of NPP contains medium both liquid and gas. Construct a three-dimensional virtual visualization model for container-centered closed-loop monitoring. Through HMI of the closed-loop loops can guide the NPP production staff quickly monitor the movement and changes of all mediums. Production staffs intuitive and vivid understanding the mediums where from and where to go. The modelling system of three-dimensional virtual visualization will provide the support for operators to control of NPP.

The flow chart of three-dimensional virtual visualization models' design is shown in Fig. 1.

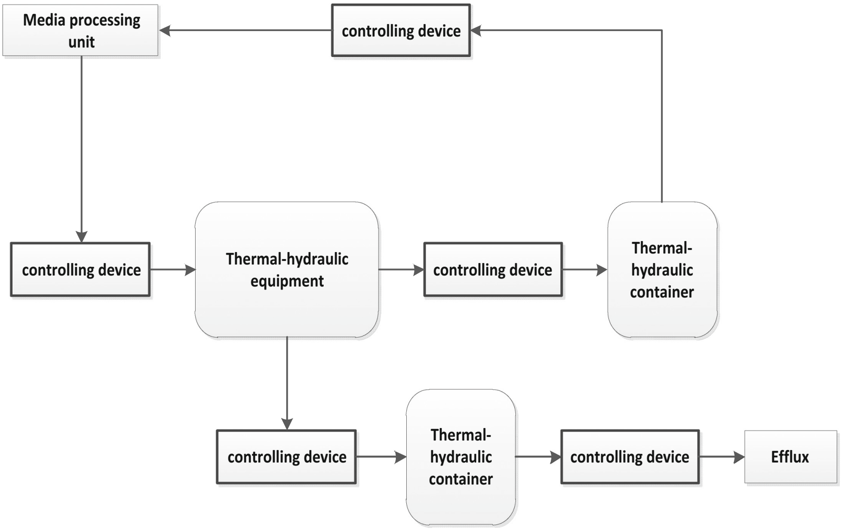


Fig. 1. Thermal-hydraulics of three-dimensional virtual visualization with container as the core to monitor closed loop

3.2 Synchronization of Real-Time Data Between NPP and Three-Dimensional Virtual Visualization System

Create a interface software to communication with KNS which can realize the synchronization of real-time data between NPP and three-dimensional virtual visualization

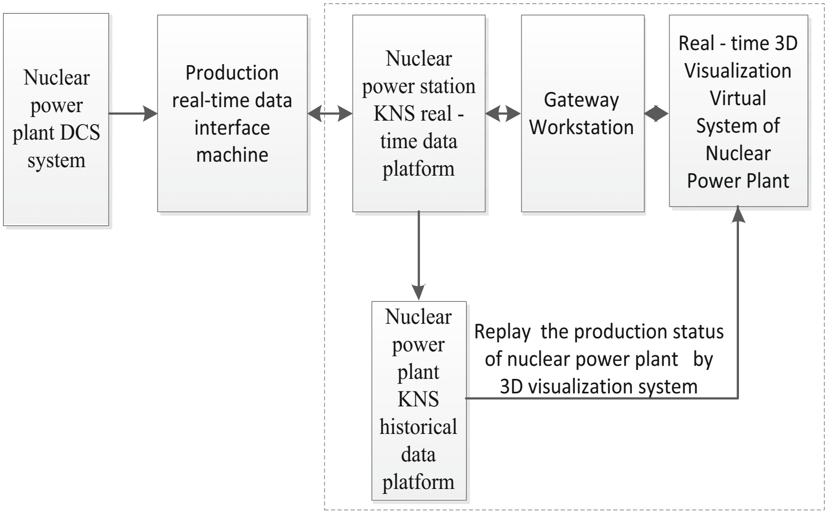

Nuclear power plant DCS system
Production real-time data interface machine
Nuclear power station KNS real - time data platform
Gateway Workstation
Real - time 3D Visualization Virtual System of Nuclear Power Plant
Nuclear power plant KNS historical data platform
Replay the production status of nuclear power plant by 3D visualization system

Fig. 2. The method of real-time data synchronization between NPP and three-dimensional virtual visualization system

system. And then establish a point-to-point association to make sure the display of real-time data in the three-dimensional virtual visualization system as the same as the operation of NPP.

The method of real-time data synchronization is shown in Fig. 2.

The real-time data get from the DCS of NPP stored in share memory of computer, the advantage of this storage method is provide parallel access for the terminals such as the three-dimensional plant model, three-dimensional virtual visualization model, HMI and so on. They do not affect each other. Monitoring function of HMI in the three-dimensional virtual visualization system as the same as the DCS of NPP. The method of real-time data storage and access is shown in Fig. 3.

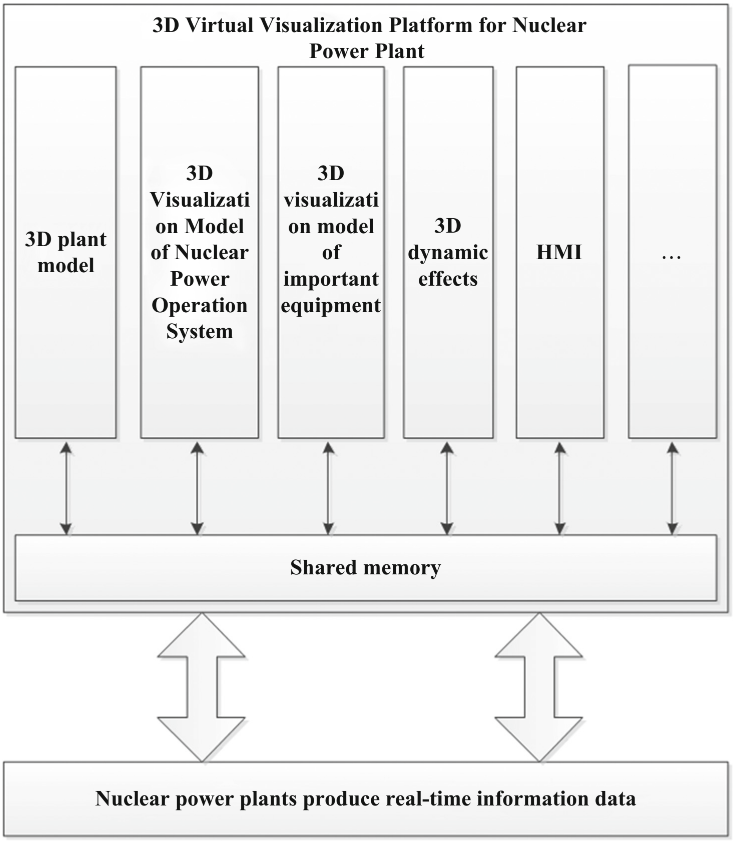

3D Virtual Visualization Platform for Nuclear Power Plant
3D plant model
3D Visualizati on Model of Nuclear Power Operation System
3D visualizati on model of important equipment
3D dynamic effects
HMI
…
Shared memory
Nuclear power plants produce real-time information data

Fig. 3. Dynamic monitoring data activation of three-dimensional virtual visualization system for real-time data of NPP

4 HMI Monitoring System of Three-Dimensional Virtual Visualization for NPP

In DCS, the operator realizes the transmission of control information and acts on the process control by the DCS HMI. According to the functions of DCS HMI, three-dimensional visualization technology is used to realize the three-dimensional monitoring screen of the important system process of NPP, and the system integration of the screen is also completed to establish the HMI monitoring system of three-dimensional virtual visualization.

This system adopts two-dimensional and three-dimensional technology to build the import equipment and pipes network of NPP, and the switch flexibility with interactive technology allows operator to switch any graphical system and equipment to suit the operator's requirements.

In this monitoring system, operators of NPP can monitor the status of the unit on the standard configuration screen, and control the equipment by using the keyboard and mouse. And decision-making ability of operators can be improved through this system. It also interface with the serious accident simulator, the full scope of simulator, optimize and enhance the use value of the simulator, and make it easy for the external visitors to show and explain the running status of the simulator.

4.1 Characteristics of HMI Monitoring System

Main characteristics of HMI monitoring System in three-dimensional virtual visualization system of NPP as follows:

- More realistic: from complanation or two-dimensional to three-dimensional, what you see is what you get.
- Operation and monitoring more intuitive.
- Improve the decision-making ability of operator.
- Support historical data's replay of NPP.
- Provide the reanalysis after the accident.

4.2 Replay of NPP's Historical Data

Consider the data analysis, which is very important for NPP in the post-accident.

The real-time data stored in the historical database by data acquisition system. By setting the period of data query in the HMI of three-dimensional virtual visualization system, It can retrieve the historical data of any time period to replay the production process, which can realize the reanalysis after an accident.

The flow chart of historical data's replay is shown in Fig. 4.

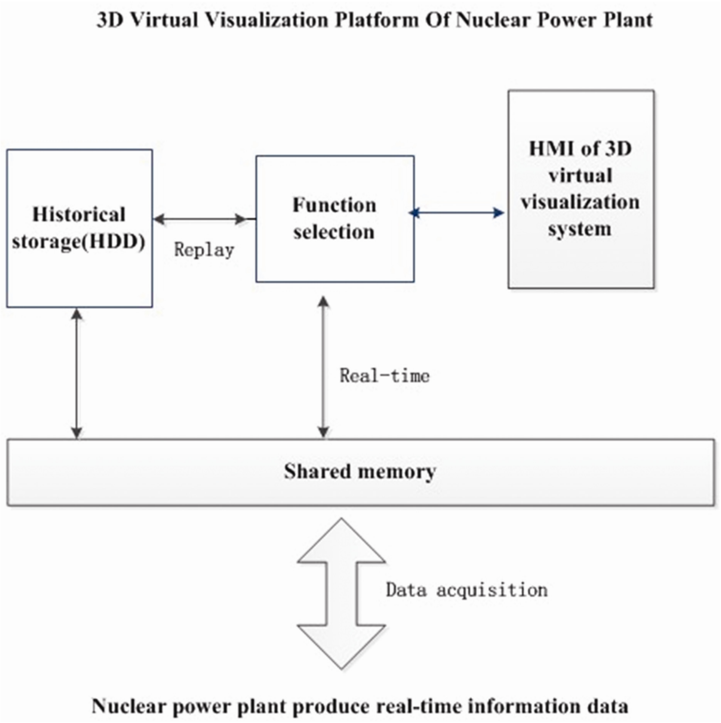

3D Virtual Visualization Platform Of Nuclear Power Plant
Historical storage(HDD)
Replay
Function selection
HMI of 3D virtual visualization system
Real-time
Shared memory
Data acquisition
Nuclear power plant produce real-time information data

Fig. 4. Historical data's replay of NPP in three-dimensional virtual visualization system

5 Conclusions

The paper presents a method to achieve three-dimensional virtual visualization monitoring of real-time information of NPP, which can make sure equipment and process system of the plant more realistic. Improve the decision-making ability of operator by more intuitive and dynamical HMI. And it is advantageous for the operator to analyze the status of the unit, and this method can be used in post-analysis after an accident, also can be used in precautions by analyzing the probability of potential risk of the object being evaluated. At the same time it can be used for NPP production personnel training, and three-dimensional virtual visualization system of NPP with high fidelity to quickly grasp the composition structure of realistic, the running way and work principle of systems and equipment.

The paper research on HMI monitoring system of three-dimensional virtual visualization, three-dimensional virtual visualization real-time monitoring of digital instrument control system and post-accident analysis in NPP, it also can be used in precautions by analyzing the probability of potential risk of the object being evaluated.

References

1. Zhan, S.H., Ren, Y.Z.: AP1000 nuclear power plant instrument control system. Autom. Instrum. **31**(10), 48–51 (2010)
2. Ang, K.H., Chong, G., Li, Y.: PID control system analysis, design, and technology. IEEE Trans. Control Syst. Technol. **13**(4), 559–576 (2005)
3. Tu, J.S., Liu, J.Z.: 3D GIS technology research and development. J. Yangtze Univ. Natural Sci. Ed. J. Med., (5), 117–119 (2005)
4. Li, Q.Q., Yang, B.S., Shi, W.Z., et al.: Real-time acquisition, modeling and visualization of 3D spatial data. J. Wuhan Univ. Inform. Sci. Ed., (12), 98–102 (2003)
5. Chen, J., Sun, H.B., Tang, L., et al.: Power system control center three-dimensional visualization technology and its real-time application. Power Syst. Autom. **32**(6), 20–24 (2008)
6. Wang, T., Jiang, G.J., He, D.Y.: Construction and development trend of real-time information monitoring system (KNS) in nuclear power plant. Nucl. Sci. Eng., (S2), 1–5 (2012)
7. Liu, G.J., Ni, L.G., Yin, J.L., et al.: The function realization and verification of CPR1000 project of nuclear power plant real-time information monitoring system. Nucl. Sci. Eng., (S2), 87–91 (2012)

The Overview in Safety Review of Human Factors Engineering and Control Room Design in Chinese AP1000 Nuclear Power Plant

Yan Feng, Zhong-Qiu Wang, Qi Wu, Yun-Bo Zhang(✉), and Jing-Bin Liu

Nuclear and Radiation Safety Center, Beijing, China
zhangyunbo@chinansc.cn

Abstract. The first AP1000 nuclear power plant is constructed in SanMen county in Zhejiang Province in China, which has creative and distinctive design characteristics. Human factors engineering disciplines are applied to the design of the AP1000. In addition to the elements of the program review model, the minimum inventory of controls, displays, and alarms present in the main control room and at the remote shutdown workstation. These contents mentioned above are reviewed according to standards, rules and regulations. This article introduces review process and several important issues during the reviewing process. These issues include many elements, such as operating experience review, task analysis, human system interface design, verification and validation, and so on. This paper emphasizes on the main control room design (including environment and layout). Background noise in the actual main control room may exceed too much to design value. Another important issue is about main control room habitability systems (VES) changes to satisfy post-actuation performance requirements in AP1000 design change proposal. All the wall panel displays will be closed in this design change proposal. Review process and proposal are described in the paper. Since the AP1000 unit in China is the first constructed all over the world, verification and validation are especially important and necessary. The plan of verification and validation, the results summary report of verification and validation, the report of human engineering discrepancies are focus attention. Verification and validation in human factors engineering include HSI task support verification, HFE design verification and integrated system validation. This paper introduces the review process of verification and validation, the issues found in verification and validation.

Keywords: Control room design · AP1000 · Human factor engineering (HFE)
Safety review · Verification and validation · Integrated system validation (ISV)

1 Introduction

Since AP1000 nuclear power plant has a 60 year design objective based on conservative assumptions, the plant design objective is 60 years without the planned replacement of the reactor vessel. The plant adopts the digital instrument control system and the

Y. Xu et al. (eds.), *Nuclear Power Plants: Innovative Technologies for Instrumentation and Control Systems*, Lecture Notes in Electrical Engineering 455,
https://doi.org/10.1007/978-981-10-7416-5_17

advanced human system interface. The operation and control centers system is the most important human system interface and includes the main control room, the technical support center, the remote shutdown room, emergency operations facility, local control stations and associated workstations for each of these centers. The main control room is able to control the plant during normal and anticipated transients and design basis accidents. The indications and controls in the main control room can monitor and control the plant safety systems and the non safety-related control systems. The remote shutdown room contains the indications and controls that allow an operator to achieve and maintain safe shutdown of the plant following an event when the main control is unavailable. Both the main control room and the remote shutdown workstation are designed in accordance with human factors engineering principles and practices. The application of the human factor engineering disciplines to the design of the AP1000 includes 12 elements: human factors engineering program management, operating experience review, functional requirements analysis and allocation, task analysis, staffing, integration of human reliability analysis with human factors engineering, human system interface design, procedure development, training program development, human system interface verification and validation, design implementation, human performance monitoring.

2 Review Process

China AP1000 PSAR had been reviewed from March, 2008, and the review period is one year. There are 182 staff participating in the review work. During the review, National Nuclear Safety Administration issued 《Technical Position of safety reviewing AP1000 self-reliance supporting project》, and identified the review basis. China AP1000 FSAR has been reviewed from October, 2012, and there are 119 staff participating in the review work.

3 Review Concerns

3.1 Background Noise in the Main Control Room

Background noise refers to any interference that is not relevant to the useful signal in the occurrence, inspection, measurement and recording system. Ambient noise refers to the noise produced by industrial production, construction, transportation and social life. In the design control room working environment of nuclear power plant, background noise refers to the noise that equipment is working in the main control room.

There are many standards stating the requirement about background noise in the main control room.

NUREG0700 (Human-system interface design review guidelines) refers to that the acoustic design of the control room should ensure that verbal communications among personnel are not impaired; auditory signals are readily detected; and auditory distraction, irritation, and fatigue are minimized. And background noise should not impair verbal communication between any two points in the main operating area. NUREG0700 also considers that verbal communications should be intelligible using normal or slightly raised voice levels. Figure 1 shows the voice levels needed for spoken communication over specified distances in the presence of different levels of background noise. Intelligibility of speech in noise is affected by the frequency spectra of the noise and of the speakers' voices and by the speakers' hearing sensitivity.

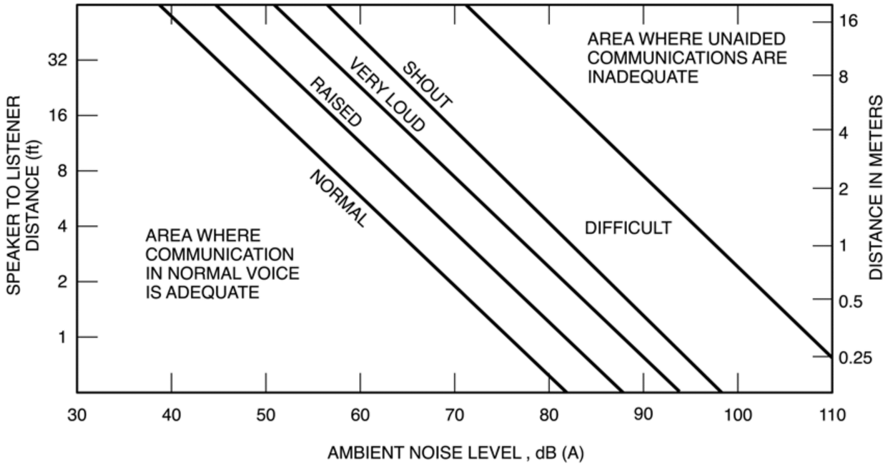


Fig. 1. Voice level as a function of distance and ambient noise level

Auditory environment is also addressed in the IEC 60964-2009 (Nuclear power plants – Control rooms – Design). Design of the auditory environment shall ensure easy communication within the operating team, minimal disturbance by ambient noise, and reliable perception of acoustic messages, alarms and emergency signals. Guidance for environmental specifications under normal conditions is provided in ISO 11064.

ISO 11064-6 (Ergonomic design of control centers, Part 6: Environmental requirements for control centers) sets that the ambient noise in the control room should not exceed 45 dB $L_{Aeq,T}$ and the background level should be in the range 30 dB to 35 dB $L_{Aeq,T}$. $L_{Aeq,T}$ means equivalent continuous A-weighted sound pressure level, and is given by the equation as following:

$$L_{Aeq,T} = 10lg\left[\frac{1}{t2 - t1}\int_{t2}^{t1}\frac{pA^2(t)}{p0^2}dt\right] \tag{1}$$

where t2- t1 is the period T over which the average is taken started at t1 and ending at t2.

EUR 2.10 also addresses the ergonomic design of main control room. Each control station, which is continuously manned on a routine basis such as the MCR (main control room) and TSC (technique support center), shall have an ambient noise level no greater than 50 dB from installed equipment in its immediate neighbourhood and plant equipment which may be operated for long periods. This limit shall be met for all normal or emergency HVAC (Heating, Ventilation and Air Conditioning) system line-ups in all areas.

In China AP1000 nuclear power plant, the background noise in main control room should not exceed 50 dBA, and noise peaks should not exceed 65 dBA. During the review of FSAR, the applicant submits the technical support document: Plant startup human factors engineering main control room (MCR) and remote shutdown room (RSR) environment verification specification. This document provides the detailed guidance and identifies the specific methods for performing the human factors engineering (HFE) design verification assessment at plant startup on the as-built working environmental conditions, including the noise in the main control room and remote shutdown room. The applicant measured and collected data on noise in the MCR and RSR when the Nuclear Island Nonradioactive Ventilation System (VBS) is in operation and data on noise when the Main Control Room Emergency Habitability System (VES) is in operation. The real data exceeded 50 dBA firstly, and many treatment measures have been done, so the real data doesn't exceed 50 dBA lastly.

3.2 Main Control Room Habitability System (VES) Changes to Satisfy Post-actuation Performance Requirements (DCP4733)

The license limit value of the main control room temperature is less than the effective temperature 85 °F (29.5 °C) within 72 h after emergency habitability system (VES) operation in accident conditions, considering the requirement of main control room habitability of personnel and equipment qualification. According to the description of the DCP4733 report, combined with the heating intensity of the internal heat of the main control room, the existing design of the VES system can not achieve the requirement of controlling the temperature rise. To maintain the main control room pressure boundary (MCRE) in requiring qualification of equipment and personnel activities, the existing design for license related must be changed. The specific approach about DCP (design change proposal) is to close the non-safety related instrument equipment in the MCR after starting VES. The equipment includes WPIS (wall panel information system), ELS (no battery supply lighting system), the main control room area radiation monitor/processor, TVS video controller, office equipment, kitchen equipment. When the VES system is started in the design basis accident (DBA) after the implementation of the change, air temperature in MCR will not exceed the relevant requirements of the license application. At the same time the non- safety related instrument equipment can be manually operated.

According to the content of the specific implementation of the design change, applicant addresses that the non-safety level of heat load will be closed into two stages after VES triggers. The equipment needed to shut down in the first stage includes 15, 16 LAN large screen display and a main control room area radiation monitor/processor, TVS video controller, water heater, convection heater (shift office), water dispenser, refrigerator and printer etc. There is no impact for safety function of nuclear power plant after closing the first stage equipment, so reviewers think that the influence on nuclear power plant is acceptable. At the same time, the applicant analyzes by test the influence after closing the ELS, and shows that the light illumination is changed litter in MCR, so reviewers think that the closure of ELS is acceptable. But reviewers think the operator may gain less information of nuclear power plant, or not easy and rapid access to information after closing the 14 large screens in the second stage. Thus the operator's load may increase to some extent, and the main control room temperature may rise at the same time, human error may cause under accident conditions. Also other personnel to enter the main control room can not quickly understand the current state of nuclear power plant after closing the large screen displays in second stage, so that reviewers think that it is not appropriate for closing all the large screen displays concerning the operation of MCR and the staff load.

3.3 Integrated System Validation

Integrated System Validation (ISV) is an evaluation, using performance-based tests, to determine whether an integrated system's design (i.e., hardware, software, and personnel elements) meets performance requirements and supports the plant's safe operation. Human engineering discrepancies (HEDs) are identified if performance criteria are not met. The applicant should provide either an IP (implement plan) or a completed RSR (results summary report) for ISV. If the applicant submits an IP, it should describe the complete methodology for conducting ISV, including: the complete set of detailed scenarios for ISV (and how they were identified through the Sampling of Operational Conditions), performance measures, acceptance criteria, and the methods by which HEDs will be evaluated. Then the applicant will submit the RSR when the work described by the IP is completed. If the applicant submits a completed RSR, at a minimum, the RSR should include details of the results of the ISV, including a statement of how the validation demonstrates the ability to safely operate the plant, and a list of HEDs generated from the V&V, the analyses associated with these HEDs, and their resolutions.

The scenarios for ISV should be performed using a simulator, or other suitable representation of the system, to determine the complete design's adequacy to support safe operations. Validation should be performed after the resolution of all significant HEDs identified in verification reviews.

ISV shall be carried out by the operator on a highly realistic training simulator. According to the relevant laws and regulations, standards and guidelines of NUREG0711, the integrated system validation test will use a specific, full-scope simulator. The simulator should have the following characteristics: interface completeness, interface physical fidelity, interface functional fidelity, environmental fidelity, data completeness fidelity, data content fidelity, data dynamic fidelity. Participants in the applicant's validation tests should be representative of plant personnel who will interact with the HSI (e.g., licensed operators, rather than training personnel or engineers). To properly account for human variability, the applicant should use a sample of participants that reflects the characteristics of the population from which it is drawn. In selecting personnel for participating in the tests, the applicant should consider the minimum shift staffing levels, nominal levels, and maximum levels, including shift supervisors, reactor operators, shift technical advisors, etc. Testing personnel should avoid selection with bias.

The ISV of China AP1000 nuclear power plant is as follows:

The applicant addresses the full-scope simulator will be used for HFE V&V when needed. The simulator includes a representation of the main control room with consoles, panels, large screen displays, operator workstations, and the latest available control logic and operator graphics. In the implement plan for ISV, applicant thinks that in actual operation, the AP1000 MCR and HSI resources will be used only by highly trained and qualified pressurized water reactor (PWR) operating crews. The hypothetical group of qualified crew members is the target user population. The ISV crews are samples taken from this target population (although training will not be completed at the time of ISV, as described above), drawn from the crews of the AP1000 customer utilities.

Up to now, the applicants show that they had carried out four ISV activities:

(1) The first activity was the China AP1000 Standard Plant ISV executed on the China standard plant simulator with Westinghouse Electric Company operations instructors as test subjects.

The results of the China AP1000 Standard Plant ISV can found in "China AP1000 Standard Plant Human Factors Engineering Integrated System Validation Report".

In the report, applicant points out that the Early China ISV is an interim ISV activity, and is incomplete with respect to the requirements for final ISV, thus the need for the subsequent ISV activities. At the same time, the applicant summarizes limitations for this ISV: simulator limitations; procedure limitations; participant limitations and test method limitations.

① simulator limitations.

The simulated plant model used for the Early China ISV test-bed did not include some plant systems, while other plant systems were based on input that was still evolving. Additionally, this software did not satisfy the testing prerequisites.

② procedure limitations.

Plant operating procedures had not been aligned with or validated against the HSI and simulator model used for the Early China ISV, included missing information, were not always aligned with one another, and did not always support the practice of "continuous use." This required the use of verbal prompts and alternate testing methods in order for the crews to progress through the scenario, and led to many of the problems encountered during the Early China ISV.

③ participant limitations.

In summary, only two crews of operators were available for the Early China ISV. These operators were American or Spanish training instructors who were not Chinese AP1000 operators.

④ test method limitations.

The HSI used for the Early China ISV had not undergone design verification or task support verification prior to use for validation. Thus, many findings that would have been identified and resolved as the result of a verification activity were discovered during the Early China ISV.

Given the limitations associated with the plant design as documented above, the applicant thinks that many plant parameters were not available to monitor, which affected the ability to evaluate pass/fail criteria associated with the Technical Specifications and the scenarios that could not be run prevented some RIHAs, also pass/fail criteria, from being evaluated.

(2) The second activity was the China AP1000 Standard Plant ISV executed on the AP1000 Standard Plant Simulator during AP1000 Standard Plant ISV preparation activities with U.S. operator trainees as subjects. This includes re-run of ISV scenarios from early China AP1000 Standard Plant ISV (which contained Priority 1 HEDs) and the execution of ISV scenarios that could not be covered in the earlier China ISV.

(3) The third activity was the observation of China operators during simulator training. The observation of operators during training was undertaken twice. The first time was at the SanMen site, and the second time was at the HaiYang site. There are two reports about operator training observation. But there were some limitations for the China AP1000 observation activities.

The detailed content of the training scenarios was significantly different from that of the ISV scenarios. The training simulator itself was not sufficient to address the full scope of scenarios. In addition, the observation was not permitted to directly collect any subjective data or comments from the trainees or trainers in the operator simulator training. This further limited the results of the observation to meet any ISV objectives.

(4) The fourth activity is the AP1000 Standard Plant ISV executed on the AP1000 Standard Plant simulator, and address remaining open issues and HEDs from the earlier China ISV, as applicable.

In view of the above ISV activities for ISV for China AP1000 nuclear power plant, we believe that:

The state of the simulator during ISV is different from the actual state (the new simulator was handed over in November 2015). At the same time, the Chinese operators ISV did not participate in the test in ISV activity, but only the American or Spanish training instructors. Moreover, relevant performance data of the operators were not collected in the observation of China operators during simulator training, and the task is not the same as that of ISV, and the operator's proficiency is not enough. Also many design change about important system for operate have not been verified and validated sufficiently, and the AP1000 Standard Plant ISV is not applied incompletely for China AP1000 nuclear power plant. So we think it is necessary that Re-ISV test shall be carried out.

4 Conclusions

China Ap1000 nuclear power plant is the first built in the world, and it has no much operating experience. So there are many problems about China AP1000 nuclear power plant and it is necessary for sufficient verification and validation. Because of limitation, integrated system validation should be carried out again by using full scale simulator and the real applicant for participant.

References

O'Hara, J.M., Higgins, J.C., Persensky, J.J., Lewis, P.M., Bongarra, J.P.: NUREG-0711, Human Factors Engineering Program Review Model. Rev. 3. U.S. Nuclear Regulatory Commission, Washington, D.C (2012)

O'Hara, J., Stubler, W., Higgins, J., Brown, W.: NUREG_CR-6393, Integrated System Validation: Methodology and Review Criteria. U.S. Nuclear Regulatory Commission, Washington, D.C (1995)

Risk Analysis of Cyber Security in Nuclear Power Plant

Zhen-Yu Yan[1(✉)], Zeng-Jun Chun[2], Gao-Jun Liu[1], and Lai-Long Zou[2]

[1] State Key Laboratory of Nuclear Power Safety Monitoring Technology and Equipment, Shenzhen China Nuclear Power Design Co., Ltd.,
Shenzhen 518116, Guangdong Province, China
{yan_zhenyu, liugaojun}@cgnpc.com.cn

[2] China Nuclear Power Co. Ltd., Shenzhen 518116, China
{chunzengjun, zoulailong}@cgnpc.com.cn

Abstract. The Cyber Security of Nuclear Power Plants (NPPs) is an important module of NPPs physical protection system (PPS). A potential security risk analysis of NPPs includes attack probability by the adversary, attack purpose and attack ability. Increased security defense advices will reduce the threat of intrusion. While the additional advices will increase the financial burden of the government and enterprises, so that the relevant companies must assess their security capabilities to protect nuclear facilities safety. This paper analyzes the risk of cyber security, including the threat, consequence and system effectiveness, to reduce the cyber intrusion risk of instrument and control system (I&C) and save the defense cost.

Keywords: Cyber security · Risk analysis · Effectiveness

1 Introduction

Nuclear security has become the issue that desperately needs to be solved after “9.11”. The attacks of “9.11” are exactly the type of security event - high consequence and low probability events. Since “9.11”, many agencies and private industries have spent considerable time defining expected threats, especially to critical infrastructures [1]. Nuclear security risk management is playing a more and more important role for the safe operation of Nuclear Power Plants. In order to prevent the nuclear facilities from hostile attack, comprehensive studies have been conducted on security risk management and cyber security within the global nuclear industry. Among them, Sandia National Laboratory is generally accepted as the authoritative institute for nuclear securities.

Cyber security is defined as the ability to protect and defend a computer or computer system against unauthorized access or attack [2]. Information Security is a broader field that is concerned with information and the protection of information whether be it physical or computerized. Cyber security is used for the protection of cyberspace and those that function in cyberspace and any of their assets that can be reached via cyberspace.

Y. Xu et al. (eds.), *Nuclear Power Plants: Innovative Technologies for Instrumentation and Control Systems*, Lecture Notes in Electrical Engineering 455,
https://doi.org/10.1007/978-981-10-7416-5_18

Nowadays cyber-attack matters a lot to the nuclear infrastructure, especially when the analog instrumentation and control systems in nuclear power plants are in the process of being replaced by the digital technologies. In the energy field, examples regarding cyber-attack are not rare. For example, Stuxnet cyber [3] attack occurred in 2010. Also, black energy cyber-attack happened in 2015 and nuclear plant shutdown caused by the malware in Germany in 2016. Stuxnet cyber-attack is reputed to be the advanced and consistent threat to nuclear facilities. Cyber-attack can be triggered once the Stuxnet virus is powered by the terror organizations. In 2014, an event of cyber-attack also occurred in South Korea with the target of KHNP [4].

NPP I&C systems include two categories: safety systems and non-safety systems. The safety systems require higher reliability, functionality, and availability than non-safety systems. Though only some non-critical information were released in that event, it is apparent that the nuclear power plants could be the target of cyber-attack. Failures in the non-safety systems should not cause a loss of safety function. Figure 1 shows the control network (safety systems) of NPPs is isolated from external network.

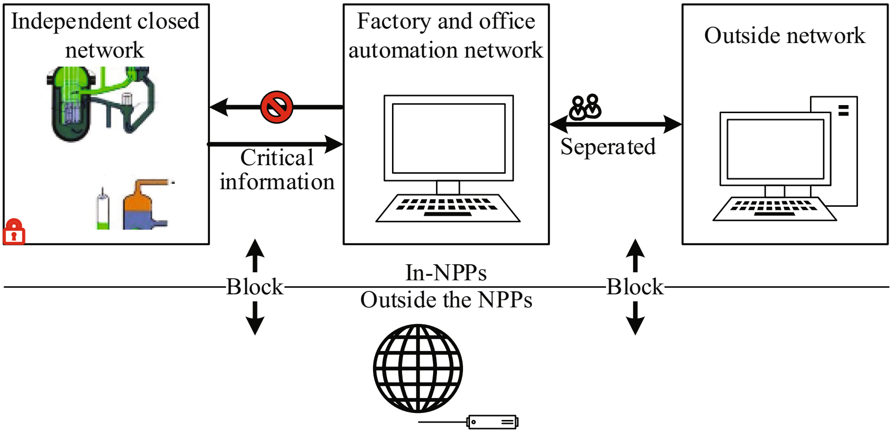


Fig. 1. The network system of NPPs

The paper introduces a classical risk analysis model for the assessment of cyber-security risks. The analytical procedures used to assess the nuclear cyber-security are presented. The cyber-security risks are estimated by going into detail of the risk-assessment impact factors.

2 Assessment of Cyber Security Risks

The classical risk formula [5] used for the assessment of cyber security risks is given by

$$R = P_A \times (1 - P_E) \times C \tag{1}$$

where, R is the risk of hostile cyber-attack.

P_A is the possibility that the hostile cyber-attack incurs.
P_E is the possibility that the cyber security system is about to defend in the attack.
$1 - P_E$ is the failure possibility of cyber security system.
C means the consequences of cyber security attack.

It is difficult to give out a quantitative number for cyber security risks under that assumption that variables are not independent and random. At least the possibility of hostile attack on our nuclear infrastructure is hard to predict. That is because human behaviors are never random events. Human may keep planning, learning and practicing to reach their goals. Therefore, conditional risk is generally applied in nuclear security. The conditional risk assumes that initiating event has already occurred (for security that means a hostile attack is planning to be taken place).

The assumption puts the focus of risk assessment on the probability of a successful hostile attack and its consequences. In general, analyst needs a more specific solution to the risk prediction. It is a fact that in some cases there may be several facilities that are under attack with severe consequences. But they are possible less vulnerable to attacks. It is therefore that priorities should be set appropriately in the security investments, especially when the budget is tighten.

There several methods and techniques have been developed for risk assessment and risk management. Though the focus of each methodology is a little bit different, they are all trying to answering following three questions.

1. The undesired event that facilities are under attack.
2. The possibility of undesired event occurring in an attack.
3. The consequences of undesired event occurring to the facilities.

Qualitative analysis will be conducted on the assessment of security risks based on the three risk factors listed below.

1. The possibility that cyber security attack occurs: to qualitatively predict the possibility of adversary attacks.
2. Consequences imposed upon an attack: to qualitatively assess the consequences.

Possibility of cyber security system fails during an attack: to qualitatively estimate the possibility of cyber security system for not defending in a hostile attack.

3 Cyber Security Risk Assessment

To evaluate the Cyber Security risk, an analytic procedure is used, and Fig. 2 describes the order of the basic steps of the program. The program starts with filter analysis, which is optional, for prioritization of assets in the enterprise, and then describes the features of the subject facilities, including identifying undesired events and their respective critical facilities. The guidelines for defining adversary threats and using threat definitions to estimate the potential threat of a particular facility attack or the probability of an adversary attack are given, and the extent of the corresponding consequences is also estimated. Another optional step is to allow the owner to prioritize the important assets of a given facility and give an effective method for estimating the security system against an adversary attack. Finally, the corresponding risks are evaluated. If the risk value exceeds a predetermined threshold (too high), a strategy procedure for identifying and evaluating risk reduction is given.

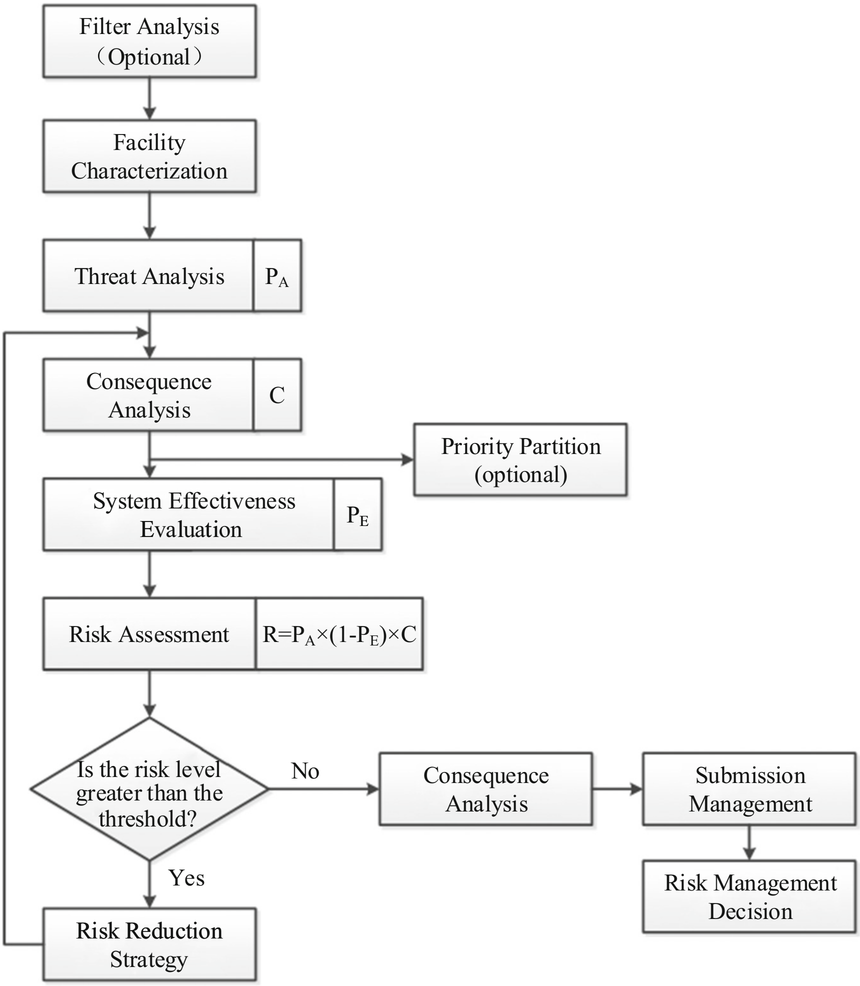

Filter Analysis（Optional）
Facility Characterization
Threat Analysis
P_A
Consequence Analysis
C
Priority Partition (optional)
System Effectiveness Evaluation
P_E
Risk Assessment
$R=P_A\times(1-P_E)\times C$
Is the risk level greater than the threshold?
No
Consequence Analysis
Submission Management
Risk Management Decision
Yes
Risk Reduction Strategy

Fig. 2. Cyber security risk analysis and management

3.1 Description of Cyber Security Facility Characteristics

The first step in the analysis of Cyber Security systems is to describe the characteristics of the facilities being analyzed, the facilities characteristics, and the requirements expressed for a complete understanding of the tasks and operating conditions of the system and equipment, as well as Cyber Security concerns. Cyber Security concerns should be described as undesired events, i.e., special events that should be prevented by security systems in real situations. An extended description of unexpected events is to identify important assets of a nuclear power plant, the assets most likely to be destroyed or acquired by an adversary. Through reasonable inspection, the protected assets can be obtained. But for complex systems, logical analysis is needed to ensure that all important assets are identified and protected. Cyber Security facilities give a characterization facilities protection object of the document, usually protection object is not a desired event or expect a subset of the list of events, as well as an important asset to protect the list [6].

3.2 Analysis of Cyber Security Threats

The first parameter of cyber security risk analysis procedure [7] is the potential for a threat, in other word is the possibility of an adversary attack. Threats analysis means required a description of the threat before the vulnerability analysis and evaluate the possibility and potential of attack, which include the adversary types, strategies and capabilities. The definition of threat is using several paragraphs to describe the number of adversaries, their practice and tool, the type of event or the activity which adversaries might do.

In order to complete the threat analysis, it is necessary to contact some organizations, including local, provincial or national legal enforcement agencies and relevant implementing agencies. The local government should be able to provide information of the type of criminal activity and future activity projections. And also need to research the document of the site historical events report, local newspapers, professional journals and other relevant information.

The potential threat of attack (the possibility of attack) means classified the threat by using the possibility of creating a threat type for an undesired event, historical events statistical data, and cognition of a specific site, after the completion of the description of the threat range. Ideally, the cyber security risk analysis is similar with the security risk assessment, which means forecast the possibility of initiating an incident, and the consequence of the incident. The historical data and statistical data that have been generated by the safety study can help to predict the probability of abnormal events and their responses to the system. But, due to human factors, it is often not possible to correctly anticipate the probability that a group of adversaries will attack against a particular asset.

However, the use of qualitative, relative potential threat parameters can be used to predict the level of non-quantifiable parameters. Conduct threat assessments based on the full potential threat analysis. The parameters are expected based on each undesired event and adversaries. The basic of parameter estimation is the characteristics of the relationship between the protected assets and a group of adversaries and the relative attraction of assets to a group of adversaries.

Figure 3 includes the information that can be used to predict the probability of a given adversary determines the attack on a particular facility.

As threats get more capable or sophisticated, the security system must also perform better. This relationship is shown in Table 1.

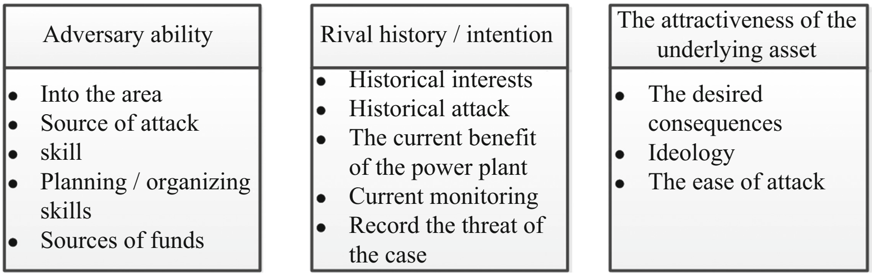


Fig. 3. A prediction of the potential attack risk

Table 1. Threat spectrum

Threat Spectrum		
Low	Medium	High
Single outsider	More outsiders	One insider
No technology	Some technology	More outsider
No weapons	Some tools	Large tools
Non violent	Knowledge	Violent
Low cost	Medium cost	Large cost

3.3 Consequence Analysis

The second parameter of cyber security risk analysis procedure is consequence analysis. Consequence analysis can be performed after the undesired event and its vital assets are identified. The next step is to forecast the consequences of the loss of a particular significant asset to each undesired event belong. Different organizations divide or name consequences into meaningful terms. Some organizations measure the consequences based on loss of income or downtime. Some are measured based on catastrophic or disease. And others are measured according to the credibility or reputation. The consequence criteria must be given qualitative definitions, such as dollar, death, injury, downtime and negative publicity. Table 2 showed an example of consequence criteria which is similar to MIL-STD-882D [8]. The main objective of the consequences analysis is to anticipate the relative consequence of the loss or damage to significant assets caused by each undesirable event.

3.4 Evaluation of Cyber Security Effectiveness

The third factor in the risk evaluation is system failure $(1 - P_E)$ which is got from system effectiveness evaluation process. The failure of security system is complemented with the system effectiveness. That is, the higher the security system, the lower the failure of system effectiveness. The reasonable measure of the effectiveness of security system to prevent the threat is an important factor in the risk evaluation formula.

Table 2. Definition of the consequence

Consequence classification	Consequence level
May cause death, systematically permanent damage, loss of more than $ 1 million, violation of laws and regulations irreversible serious environmental damage	Disastrous
May cause partial damage to the system, personal injury, at least three persons occupational disease hospitalized, more than $ 200,000 but less than $ 1 million in loss, or violation of laws or regulations for reversible environmental damage	Critical
May cause personal injury or occupation disease causes one or more people working on the loss of more than $10 thousand but less than $200 thousand in losses, or not in violation of laws or regulations can relieve the environmental hazards	Marginal
May cause personal injury or illness caused by the loss of working days but not more than $2 thousand, but the loss of less than $10 thousand, or not in violation of environmental laws or regulations of the minor damage	Negligible

The value of evaluating the effectiveness of the cyber system is to identify the specific weaknesses of the physical protection system. If the effectiveness of the security system is low, then the weakness of the plant-specific system is the disadvantages in the low security level and the defect of the protective element. Knowledge of specific weaknesses in power plants is valuable for system upgrades planning for risk reduction and for accident planning to understand where to strengthen system protection under the threat conditions evaluated.

For most applications, the security system consists of physical protection facilities and cyber security facilities. Some undesirable events are always accompanied by physical attacks on the facility, while others are accompanied by information against the system. The complete security system should be able to cope with physical and cyber-attacks. The complete system effectiveness assessment will include physical protection analysis and cyber-security analysis. This paper mainly analyzes the cyber security effectiveness.

It is proved that the high performance of cyber security system is based on three basic cyber-security functions and their integration, according to the detection, delay, response, and the integration of these three functions. The three functions are used to ensure the confidentiality, robustness, and availability of data. Confidentiality requirements information cannot be obtained by unauthorized individuals, entities or processes. Soundness requirements information cannot be altered or destroyed in an unauthorized manner. Availability requirements information is available or unavailable by authorized entity. The three cyber security functions are authentication, authorization, and audit.

(1) Authentication

The validity of the certification statement. User authentication is the ability of individuals to connect with the computer, you can use three mechanisms to complete the personal knowledge, personal ownership and personal.

Once the user is authenticated, a certificate that is associated with the computer in the name of the user is usually issued. User authentication is critical to the overall security of the system or information, since if a user (maliciously or otherwise) obtains another user certificate, who can obtain information that is forbidden.

(2) Authorization

The authorization determines whether an entity's action is permitted to execute a given information object (such as a file, a database record, a web page). Authorized access systems and applications must rely on management assurance that the information on the authorized access system must be controlled so that only authorized users can access specific information objects based on the authorized entity.

(3) Audit

Review the behavior or intent of a recording entity on a computer system or information, and the cyber-attack detection system can support the audit function. The main element of a successful cyber-attack detection system is the continuous review of business data, the detection of any improper scanners (including any suspicious ports and modems), virus protection, and access control monitors.

A simplified table is presented in Table 3 for the evaluation of cyber security effectiveness.

Table 3. Evaluation of cyber security effectiveness

	Low	Medium	High
Authentication	No features	Strong password	Two-factor
Authorization	No features	Permissions based upon project-based groups or roles	Permissions based upon project-based group or roles; other user attributes and authentication trust level
Audit	No features	Required and retained for some months, analyzed if incident occurs	Required and retained for some months, analyzed periodically for evidence of unauthorized activity

The implementation and integration of authentication, authorization and audit must be completed at a high level. The authentication and authorization strategy provides data for auditing capabilities, where the audit analyzes the evidence of malicious conduct.

Access control monitoring ensures complementarity between firewall and intrusion detection systems. The firewall blocks undesired information services and permits the desired business. The cyber-attack detection system needs to be blocked and licensed for the suspicious sample.

4 Conclusions

This paper uses traditional risk evaluation formula to analyze cyber security risks. Cyber security risk is a function of attack probability, successful attack consequences, and security system failure. In order to assess the cyber security risks, the qualitative assessment of the likelihood of the attack, the system failure, and the consequences are logically merged. Describe the characteristics, threats, consequences, system effectiveness, and risks of cyber security facilities for cyber security risk assessment. By the analysis of cyber security, to reduce the level of nuclear power plant risk, and save nuclear power station defense cyber security costs.

References

1. Garcia, M.L.: Design and Evaluation of Physical Protection Systems, 2nd edn. Butterworth-Heinemann, Burlington (2007)
2. Von Solms, R., Van Niekerk, J.: From information security to cyber security. Comput. Secur. **38**, 97–102 (2013)
3. Langner, R.: Stuxnet: dissecting a cyberwarfare weapon. IEEE Secur. Priv. **9**, 49–51 (2011)
4. Chung, M.K., Lim, J.I., Kwon, H.Y.: A study on north korea's cyber attacks and countermeasures. J. Korea Soc. IT Serv. **15**(1), 67–79 (2016)
5. Betty, E.B., Rudolph, V.M., et al.: Security Risk Assessment and Management: A Professional Practice Guide for Protecting Buildings and Infrastructures. Wiley, Hoboken (2001)
6. Cavina, A.: Computer security at nuclear facilities. Int. At. Energy Agency (2011)
7. Veitch, C.K., Wade, S., Michalski, J.T.: Cyber security assessment tools and methodologies for the evaluation of secure network design at nuclear power plants. Sandia National Laboratories (2012)
8. Department of Defense Standard Practice System Safety. Department of Defense, MIL-STD-882D (2000)

Commercial Grade Dedication for Software Life Cycle of Digital Instrument and Control Equipment

Qi Wu, Yun-Bo Zhang(✉), Shi-Xin Li, and Xin-Yu Wang

I&C Department, Nuclear and Radiation Safety Center, Beijing, China
zhangyunbo@Chinansc.cn

Abstract. Commercial grade dedication (CGD) is used to prove that the digital equipment dedicated can be used to perform nuclear safety function. It is a prerequisite for using digital equipment in nuclear power plants. This paper introduces the document architecture, process methods and critical characteristics of digital equipment CGD, discusses the requirements and acceptance criteria of software lifecycle in digital equipment CGD, proposes a method using thread analysis to assess the software lifecycle.

Keywords: Digital equipment · Commercial-grade dedication
Critical characteristics · Software life cycle

1 Introduction

Tian Wan nuclear power plant was the first power plant using digital instrument and control (DI&C) system, since then, DI&C system began to be widely used in China's nuclear power plants including CPR1000, AP1000, EPR etc. Compared with the traditional analog instrument control system and equipment, digital instrument and control system and equipment have some obvious advantages, for example: higher control accuracy and stronger calculating capability, higher reliability of data transmission, easy to expand and configure, easy to maintain and management and high degree of integration, using digital instrumentation equipment can improve the economic benefit of nuclear power plants. Moreover, because of the cost of the spare parts procurement has improved significantly, nuclear power plant needs to use DI&C equipment to replace the original analog equipment.

While most digital instrumentation equipment have broad and mature applications in other areas, purchaser still find the following problems in the procurement of safety-class digital devices that limit the use of digital equipment in nuclear power plants:

1. Most of the digital equipment are mature products, but the supplier's quality assurance system is different from the nuclear quality assurance system, resulting in that the quality assurance measures implemented in digital equipment design and manufacturing process do not fully meet the requirements of nuclear quality assurance;

Y. Xu et al. (eds.), *Nuclear Power Plants: Innovative Technologies for Instrumentation and Control Systems*, Lecture Notes in Electrical Engineering 455,
https://doi.org/10.1007/978-981-10-7416-5_19

2. Due to the small procurement quantity and low value, the supplier do not want to establish a quality assurance system according to the requirements of nuclear quality assurance;
3. The hardware functions and performance of digital equipment, including tolerance to the environment of nuclear power plants, are easy to test and verify, but the software reliability, safety and robustness are difficult to verify and evaluate.

The U.S. nuclear industry faced the same problems in the use of digital equipment to replace analog equipment. In order to solve these problems, the US nuclear industry adopted the "Commercial Grade Dedication" (CGD) way to evaluate the critical characteristic of digital equipment. The equipment which was dedicated successfully can be regarded as safety class equipment, and perform its safety function with adequate reliability. CGD is endorsed by the U.S. NRC [1]. This paper introduces the digital equipment CGD documents architecture, process and method in the United States, and discusses the evaluation problems, methods and criteria about the software life cycle.

2 Documents Architecture of CGD in USA

The US nuclear industry has been implementing CGD for decades, and formed a integrated CGD documents architecture including four levels which are technical report, standard, regulatory document and code of federal regulation.

At the technical report level, since 1988, the American Electric Power Research Institute (EPRI) has published a number of reports about CGD in nuclear safety application, including: EPRI NP-5652, EPRI NP-6406, EPRI TR-102206, EPRI TR-106439, EPRI TR-107339, EPRI 1011710 and so on. EPRI NP-5652 is a principal report on CGD, in which EPRI addresses the background, objectives, basic concepts, overall process, and basic method of CGD, propose the dedication method composed of technical evaluation and acceptance [2]. The EPRI TR-106439 is a report on digital equipment CGD, in which EPRI addresses the critical characteristics, the quality elements and acceptance criteria for digital equipment [3].

At the standard level, IEEE Std.7-4.3.2-2010 is a new and key standard. The terms and provisions of the standard for digital equipment CGD are basically the same as those in the EPRI reports. According to the requirements of this standard, for the digital equipment CGD process is compose of preparation stage, implementation stage, design review and maintain the dedication stage. The standard addresses the requirements for the activities at all stages [4].

At the regulatory document level, the US NRC has approved several EPRI's reports and IEEE standards through a number of generic letters, evaluation reports and regulatory guidelines, including: Generic Letter 89-02 which has conditionally endorsed EPRI NP-5652 and supplemented some requirements for CGD, R.G.1.152 which endorsed IEEE 7-4.3.2, and 《REVIEW OF EPRI TOPICAL REPORT TR-106439, "GUIDELINE ON EVALUATION AND ACCEPTANCE OF COMMERCIAL GRADE DIGITAL EQUIPMENT FOR NUCLEAR SAFETY APPLICATIONS" (TAC NO.M94127)》. US NRC has also developed inspection procedures for CGD, e.g. I.P.

43004, and specifies the review methodology and acceptance criteria for CGD in Standard Review Program (SRP) NUREG 0800 Chap. 7.

At the code of federal regulation level, 10CFR21 and 10CFR50 APP.B states the definitions, concepts and basic principles for CGD. Figure 1 provides the documents architecture of CGD in USA.

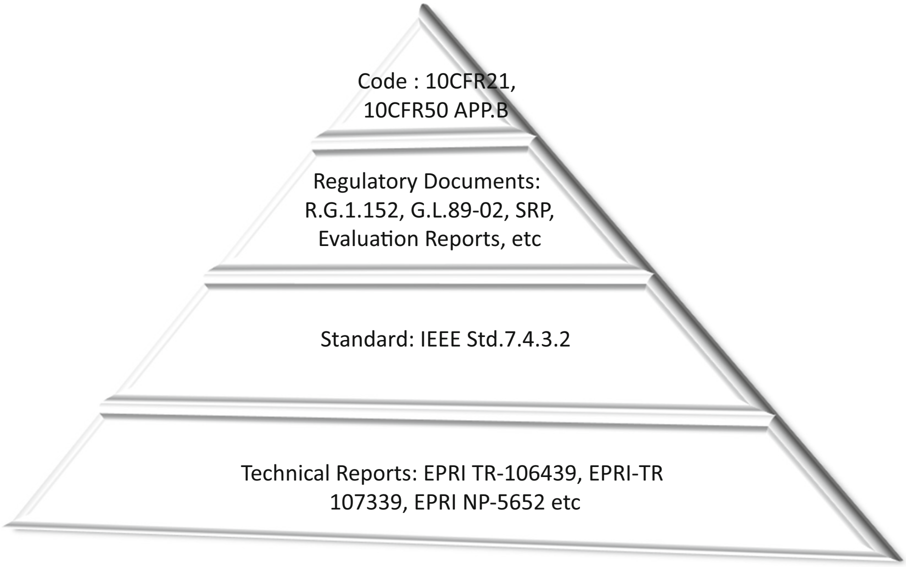


Fig. 1. Documents architecture of CGD in USA.

3 Digital Equipment CGD Process and Method

EPRI NP-5652 presents a common process and method for CGD. Overall, the dedication process includes two steps: technical evaluation and acceptance. The main contents of the technical evaluation include: (1) identify the safety function, (2) failure mode and consequences analysis (FMEA), (3) identify the critical characteristics. Acceptance methods include: (1) special tests and inspections, (2) commercial grade survey, (3) source verification, (4) quality record review and (5) combinations of methods 1–4. The main task of CGD is to verify and evaluate the critical characteristics of the items using appropriate acceptance methods. The critical characteristics depend on the safety functions, environmental conditions and the failure mechanism of the items. The critical characteristics generally include physical and performance characteristic. The process and method of CGD are shown in Fig. 2.

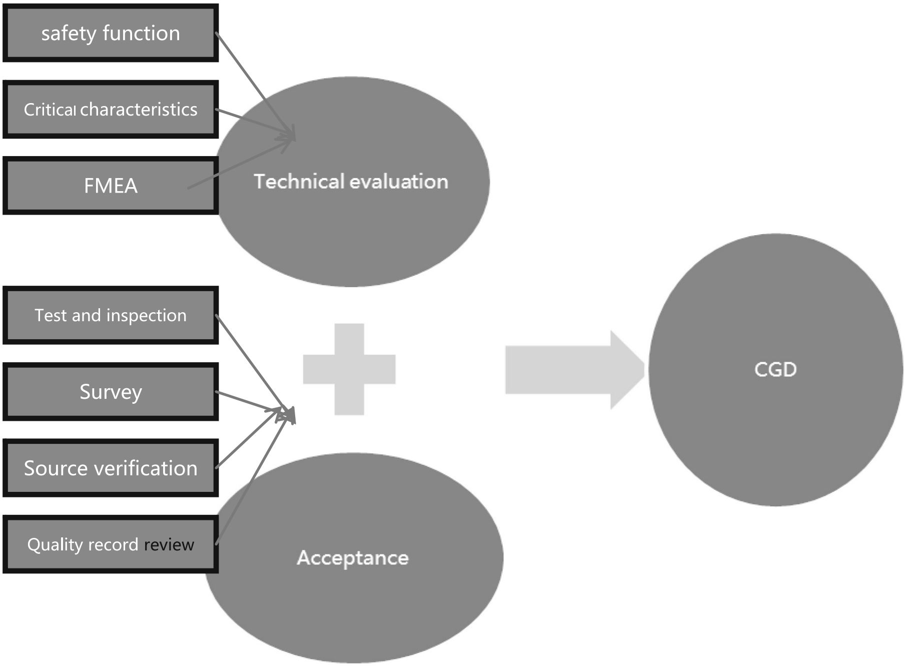


Fig. 2. CGD basic process and methods

The process and method of CGD for digital equipment are basically the same as the above methods and process. But be different from the analog equipment, the digital equipment function depends on the software embedded in the equipment, such as logical calculation, data processing and storage, and the quality of the digital equipment is determined by the quality of the software and hardware. The quality of the software is determined by the quality of a series of process activities such as software development activities, verification and validation activities, configuration management activities, etc. Thus, in EPRI TR-106439, the critical characteristics of commercial digital equipment are classified into three categories, physical characteristics, performance characteristics and dependability characteristics. Dependability characteristics are a set of characteristics related to the digital equipment development process, including reliability, design quality, traceability, etc. Table 1 provides some examples of critical characteristics of digital equipment.

Compared with analog equipment, digital equipment quality and reliability depend on the software quality. Software failure and low reliability is caused by the error and mistake in software design and development activity. Software failures are deterministic, difficult to detect and locate, transitivity and hard to reproduce compared to random hardware failures. Therefore, the evaluation of software dependability characteristics is the key issue of digital equipment CGD.

The software dependability characteristic is a set of characteristic related to the software development process. For most commercial grade digital equipment, the software is not customized for nuclear power plant applications; the development process has been completed. Therefore, the evaluations of the digital equipment dependability characteristics mainly assess the software design and development documents and records. The acceptance method of the digital equipment software dependability characteristics is a combination of commercial grade survey, design review (or critical digital review) and quality record review.

Table 1. Examples of digital equipment critical characteristic

Critical characteristics	Examples
Physical characteristic	Equipment models, materials, sizes, hardware and software version, installation, interface, etc.
Performance characteristic	Safety function, response time, human-machine interface function, the function and performance under the abnormal condition, self-diagnosis, environment qualification, etc.
Dependability characteristic	Functional reliability, design quality, manufacturing quality, fault management, configuration management, operation and maintenance compatibility and traceability, etc.

4 Assessment for Software Lifecycle

The software lifecycle defined by a specific process model is composed of the software development stages, and usually be defined and described in the software development plan, which address the resources, processes, inputs, tasks and outputs of each stage of the software lifecycle. The software lifecycle based on the “V” model is shown in Fig. 3. The objective of implementing the software lifecycle is to control and manage the software development process. The reliability of the nuclear power plant safety software depends largely on the integrity of the software lifecycle, adequacy of software validation and validation, software configuration management and change control activities, and coverage of software testing activities. These activities constitute the software lifecycle, in the process of digital equipment commercial grade dedication, the assessment of the lifecycle is the basis of the software assessment work.

In the process of digital equipment CGD, dedication entity often faces some challenges that equipment vendors do not strictly follow the nuclear safety software standards, e.g., not establish the software development plan, V&V plan and control management plan, and some records is incomplete, etc. To solve the above problems in the dedication process, the dedication entity has to ignore the minor issues but focus on whether the software development process is controlled, that is, the software development process is integrate, traceable and deterministic. Acceptance criterion is shown in Table 2.

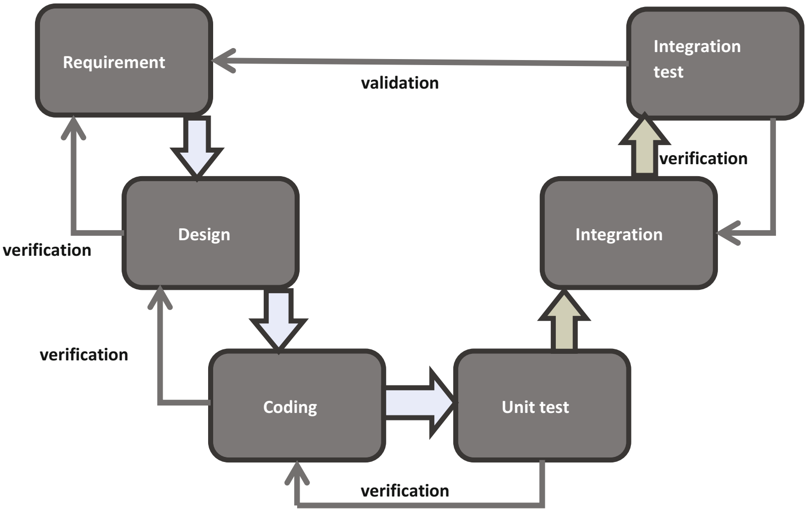


Fig. 3. Software lifecycle based on V model

Table 2. Acceptance criterion of development process

Requirements	Acceptance criterion
Integrity	1. The software development process is a closed-loop which is from the software requirements proposal to final requirements validation. 2. The software development process integrates development activities, validation and validation activities, configuration management activities and quality assurance activities; 3. Performed software FMEA/FTA to identify the risks and effects in the software development process;
Traceability	1. Take measures to trace the implementation of software requirements at each stage of development process (such as the requirements traceability matrix (RTM)); 2. Take measures to trace the change process and the final state of the configuration management items (e.g., documents, code, tools, etc.); 3. Take measures to trace the software risks identified by FMEA/FTA
Determinism	1. There are definite and unambiguous input, task, and output requirements for each stage of the development process; 2. The requirements includes the maximum time for response (e.g., time from data input to calculated output); 3. The criteria for judging software failures are definite; 4. The state and data of the software that recovery from the failures is determined

In the specific dedication process, considering the software lifecycle continuity and iterative process characteristics, dedication entity may do "thread analysis (thread review)" [5] to track some specific requirements and issues to verify whether the software lifecycle is integrate, traceable and deterministic. Thread analysis (review) is not a comprehensive coverage of all software requirements and issues, but rather focus on specific key requirements and issues. A thread begins from a requirement proposal end to the requirement be validated, or begins from an issue occur end to the issue be closed. Dedication entity should track and analyze all of the development, verification and validation, change, configuration management activities and records of the requirement or issue when doing thread analysis. Through the analysis, dedication entity can understand the control of the software development process, discover the shortcomings of the software development process, determine the required compensation measures, and implement the compensation measures in the subsequent dedication work. Examples of software requirements thread analysis and some concerns are shown in Fig. 4.

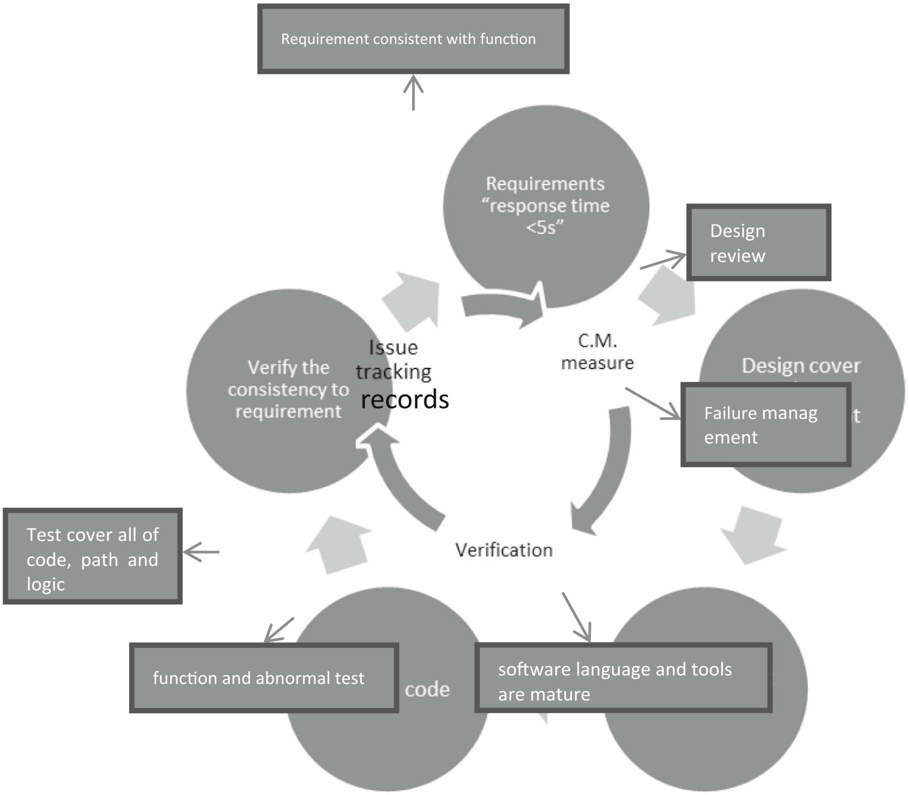

Requirement consistent with function
Requirements "response time <5s"
Design review
Issue tracking records
C.M. measure
Verify the consistency to requirement
Design cover
t
Failure manag ement
Test cover all of code, path and logic
Verification
function and abnormal test
code
software language and tools are mature

Fig. 4. Software requirement thread analysis (example)

5 Conclusion

At present, the safety instrumentation and control system of all the nuclear power plant under construction in China are digital technical, and the analog field meters and controllers are gradually replaced by the digital equipment. Only the digital equipment which has sufficient reliability and quality can be used to perform nuclear safety function.

While the quality assurance measures implemented in the digital equipment design and manufacture process can not satisfy the nuclear quality assurance requirements, it is must to take a "commercial grade dedication" to determine whether the digital equipment can be used for nuclear power plant safety application. This paper introduces the document architecture, process and method of digital equipment CGD in the United States, discusses the requirements and acceptance criteria of software lifecycle of digital equipment CGD, and proposes a method using thread analysis to assess the software lifecycle.

References

1. Title 10 of the Code of Federal Regulations, Part 21, Reporting of Defects and Noncompliance. Nuclear Regulatory Commission (1995)
2. EPRI NP-5652: Guideline for the Utilization of Commercial Grade Items in Nuclear Safety Related Applications. Electric Power Research Institute (1988)
3. EPRI TR-106439: Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications. Electric Power Research Institute (1996)
4. IEEE Std.7-4.3.2: IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations. Institute of Electrical and Electronics Engineers, Inc. (2010)
5. EPRI-1011710: Handbook for Evaluating Critical Digital Equipment and System. Electric Power Research Institute (2005)

Electric Isolation Test Research and Application of Safety Class Equipment Qualification in Nuclear Power Plants

Zhong-Qi Liang, Hua-Ming Zou(✉), Hong-Wei Pei, Guo-Jin Jiang,
and Chun-Ming Liu

China Techenergy Co., Ltd., Beijing 100094, China
zouhuaming@cgnpc.com.cn

Abstract. Electric isolation test is the essential part in equipment qualification. But the lack of electric isolation test standard causes the large diversity in the equipment qualification test. Firstly, this paper analyzes the principle of isolation design of electrical equipment, and then puts forward a set of test requirements, specifies the test level of isolation test to verify whether the electric isolation design can achieve the engineering application. After analyzing the interface character of isolation electrical equipment, combined with the isolation test experience of global DCS platforms in isolation qualification test, this paper gives a whole test method. This method was well practiced in equipment qualification of proprietary intellectual property rights nuclear safety digital I&C platform in China, obtaining good results.

Keywords: Nuclear power plants · Safety class · Equipment qualification
Electric isolation test

1 Introduction

Safety class instrument & control (I&C) system is the nerve center of nuclear power plants, and the reliable and economical operation of nuclear power plant unit depends largely on the performance of I&C system. In order to achieve high reliability and high performance, the redundancy and diversity design in I&C system is necessary. And the isolation design between redundant channels in the same system and between different systems is also effective mean to guarantee the redundancy and diversity. If isolation design is unsatisfied, the faults can be spreaded in the system, which make the design of diversity and redundancy in I&C system become an empty-shell. Section 4.1 in IEC 60709-2004 [1] also clearly puts forward the requirements to isolate about the prevention of the faults from being spreaded.

Therefore, safety class system shall be fully isolation designed to prevent the fault from being spreaded, so as to ensure that the safety class system can perform the required safety functions when any involved basis event occurs during and after.

In general, the physical separation and electrical isolation are adopted in the safety class DCS to realize the isolation within DCS internal system or between systems. Physical separation usually adopts way of using safety class structures, guaranteeing the separation distance among equipments and setting up barriers between equipments.

Y. Xu et al. (eds.), *Nuclear Power Plants: Innovative Technologies for Instrumentation and Control Systems*, Lecture Notes in Electrical Engineering 455,
https://doi.org/10.1007/978-981-10-7416-5_20

And electrical isolation usually adopts way of using these equipments which have the function of isolation, such as using fiber optic coupler, photoelectric coupler, relays, circuit breakers, the power supply device with isolation performance and the signal transmitter with isolation performance.

Physical isolation adopts a relatively intuitive design to prevent the spread of the fault, so adequate verification can be achieved by means of design review to make sure whether the design meets the requirements. For example, checking whether it set up a barrier, measuring the isolation distance among the equipments can verify the design whether meets the application requirements.

However, electrical isolation is achieved by using isolation devices in circuit. The isolation performance of these isolating devices cannot be judged only through the simple way of distance measurement.

2 About the Isolating Test Requirements in Standards

2.1 Overview

There are standards which describe the requirements about isolation design in the series of international standards, such as IEC 60709-2004, which mention the isolation requirements but do not clearly define the specific test method and level of the isolation test.

IEEE 384-1992 [2] also does not clearly specify the requirements of the isolation test. However, among the known standards and specification, the RCC-E-2012 [3] established by *French Society for Design and Construction Rules for Nuclear Island Components* (AFCEN) and EPRI TR-107330-1996 [4] approved by the *Nuclear Regulatory Commission* (NRC) have mentioned the requirements of the isolation test. Some international DCS manufacturers also reference to these two standards when performing this isolation test. Please see the following sections in detail for the related requirements.

2.2 The Requirements in RCC-E-2005

RCC-E-2012 D7600 has specified the features of isolation device which apply to electrical isolation effect. The description includes the following several aspects:

- The requirements of isolation voltage peak between the upstream and downstream;
- The requirements of isolation voltage peak between the upstream and the ground as well as between the downstream and the ground;
- The requirements of insulation resistance between the upstream and downstream.

The standard also stipulates that some circuits, such as CRT screen, the radiation power detectors etc., may have high rated voltage value which shall be taken into consideration. According to RCC-E-2012 D7600, the highest insulation test voltage of the variety of independent circuit is determined by the highest possible voltage of the variety of independent circuit.

The content of above can be interpreted that the device shall be verified whether it meets the requirements of the isolation performance through isolation test instead of design review.

2.3 The Requirements of EPRI TR-107330-1996

The chapters 4.6.4 of EPRI TR-107330-1996 points out the isolation requirements of the isolation equipments between 1E and non-safety, and also points out the following faults which should be prevented from spreading between 1E and non-safety:

- The maximum credible voltage transient applied to the device's non-Class 1E side;
- Shorts, grounds, or open circuits occurring in the non-Class 1E side;
- The maximum credible voltage transient applied to the another device's Class 1E side;
- Shorts, grounds, or open circuits occurring in the another Class 1E side;
- The highest credible direct voltage or power frequency alternating voltage applied to the input and output sides, which leakage current is less than the specified value.

The EPRI TR-107330-1996 also points out that isolation test shall be performed to verify the isolation performance whether meets the requirements of I&C system. However, about the test level, EPRI TR – 107330 only specifies that isolation device should bear at least 600 VAC and 250 VDC, the 30 s duration. And also it specifies that the digital signals of the adjacent channel shall not operate in fault and the changes of analog signal shall be less than 0.05% during high voltage applied.

2.4 The Comparative Analysis of Standard Requirements

The analysis shows that there are some differences between RCC-E-2012 and EPRI TR – 107330-1996 in isolation test. The requirement of RCC-E-2012 is through general method of performing insulation withstand voltage test and insulation resistance test to ensure the isolation performance. The device under test is power off during the test. However, the methods in the EPRI TR–107330 attempt to simulate the fault, such as high voltage, short circuit and grounding etc., during the equipment operation. Therefore, the required test method in the EPRI TR-107330-1996 is that test equipment is power on state during the test.

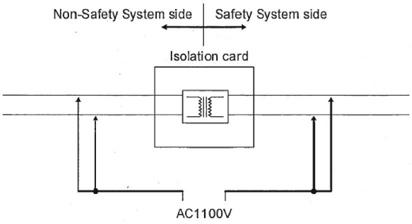
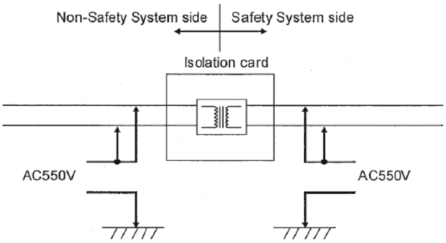
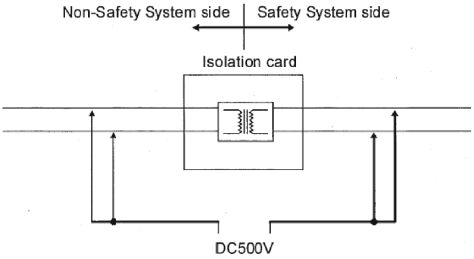
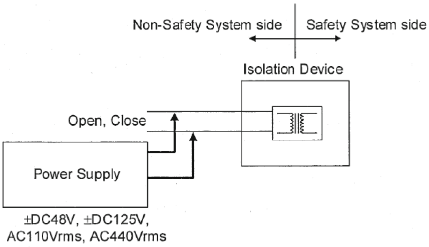
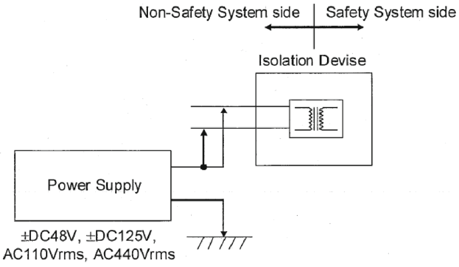
Both two methods can play a role in verifying the isolation performance. Judging from the current international practice, these two methods should be both taken into consideration in some I&C platforms to perform the isolation test.

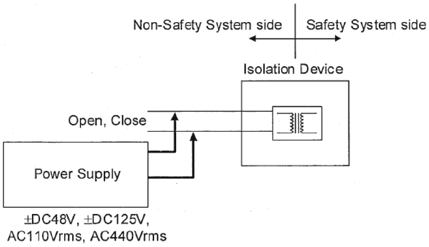
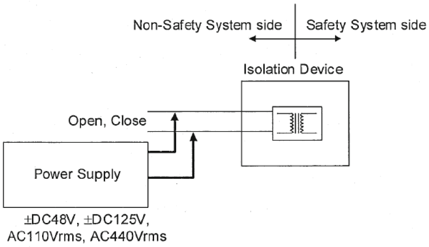
3 The Isolation Test Experience of International DCS Manufacturers

Topical report of international DCS platforms which have been assessed by the NRC can be obtained from the current NRC related web site. From these topical reports, it can be found that all isolated modules have undergone a corresponding isolation test. The following gives an example to illustrate that isolation test approach of an isolation device in I&C platforms. Test items and parameters are listed in Table 1.

From above, these platforms considered not only the RCC-E-2012 isolation test requirements, but also the EPRI TR-107330-1996. This proved the point view

Table 1. Isolation test items and parameters of international DCS platforms

Test item	Test method	Qualified criteria
Isolation withstand voltage between input and output	 Non-Safety System side Safety System side Isolation card AC1100V	Equipment cannot be damaged
Isolation withstand voltage between input and the ground/ between output and the ground.	 Non-Safety System side Safety System side Isolation card AC550V AC550V	Equipment cannot be damaged
Insulation resistance between input and output	 Non-Safety System side Safety System side Isolation card DC500V	More than 10 M Ω
The difference module overvoltage test of non-safety side	 Non-Safety System side Safety System side Isolation Device Open, Close Power Supply ±DC48V, ±DC125V, AC110Vrms, AC440Vrms	The output on the other side should not fluctuate
The common mode overvoltage test of non-safety side	 Non-Safety System side Safety System side Isolation Devise Power Supply ±DC48V, ±DC125V, AC110Vrms, AC440Vrms	The output on the other side should not fluctuate

The open circuit test of non-safety side	 Non-Safety System side Safety System side Isolation Device Open, Close Power Supply ±DC48V, ±DC125V, AC110Vrms, AC440Vrms	The output on the other side should not fluctuate
The short circuit test of non-safety side	 Non-Safety System side Safety System side Isolation Device Open, Close Power Supply ±DC48V, ±DC125V, AC110Vrms, AC440Vrms	The output on the other side should not fluctuate

described in Sect. 1.2.4, which both the requirements in RCC-E-2012 and EPRI TR-107330-1996 should be taken into consideration.

4 The Research and Application of Isolation Test Method

4.1 The Research of Testing Requirements of Isolation Ports

In the safety class DCS system, isolating devices are mainly used for the isolation between analog signals, between digital signals and between the communication signals. The isolation of communication signals is usually realized by using optical fiber which required no isolation test to verify the isolation performance. The digital signals usually use optical coupler components or relays to realize the isolation. The analog signals usually use voltage or current transformers to realize the isolation. Comparing with analog isolation device and the digital signal isolation device, the analog signal isolation device has higher complexity. The constraint of related isolation parameters and isolation performance criteria is higher than digital signal isolation device. So this paper will give the example of the port features about analog isolation device according to the application of general analog isolation device.

Generally, the output signal in analog isolation devices need to go to multiple redundant channels of the redundant system. So the device has multiple outputs. Besides, the input, power supply, grounding, etc. should also be treated as the ports of the device. Power supply ports usually come from safety class power supply network, so the power supply in isolation device can be classified as safety class. Considering the ground loop usually endure interference from the earth, so the ground shall be treated as fault side. And then there exists the isolation between multi-channel outputs because the channel may be distrusted to both safety side and non-safety side, so a general isolation device has the typical port characteristics (see Fig. 1).

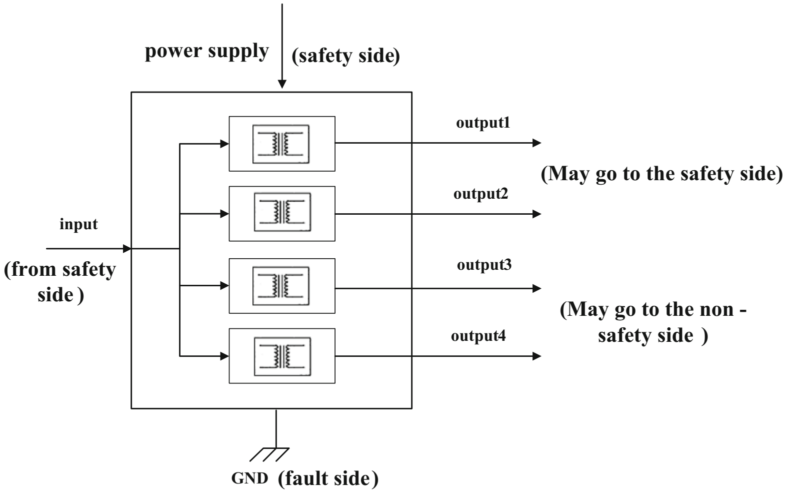


Fig. 1. Isolation ports feature of general analog isolation device

According to the isolation characteristics analysis above, the safety and non-safety isolation requirements between electric ports mainly include:

- Between the input and output
- Between the output and output
- Between the power supply and output
- Between the input and ground
- Between the output and ground

4.2 Test Level and Acceptance Criteria

Based on the requirements of isolation test in RCC-E-2012 D7600 and TR – 107330 and combined with the port feature of isolating device and its fault mode, the isolation test of general analog isolation device can perform according to the test level as Table 2.

Table 2. Recommended isolation test requirements of general analog isolation device

The origin of the test item	Ports	Test item	Test level	Acceptance criteria	Powered status
RCC-E-2012 D7600	Between the input and output	insulation and voltage resistance test	1100 VAC@1 min	Device cannot be damaged after test and device power on.	power off
		insulation resistance test	500 VDC@1 min	More than 10 MΩ or according to the product specification.	Power off
	Between the output	insulation and voltage resistance test	1100 VAC@1 min	Device cannot be damaged after test and device power on.	Power off
		insulation resistance test	500 VDC@1 min	More than 10 MΩ or according to the product specification.	Power off
	Between the power supply and the output of Non - 1E	insulation and voltage resistance test	1100 VAC@1 min	Device cannot be damaged after test and device power on.	Power off
		insulation resistance test	500 VDC@1 min	More than 10 MΩ or according to the product specification.	Power off
	Between the input and protected area	insulation and voltage resistance test	600 VAC@1 min	Device cannot be damaged after test and device power on.	Power off
		insulation resistance test	500 VDC@1 min	More than 10 MΩ or according to the product specification.	Power off

(*continued*)

Table 2. (*continued*)

The origin of the test item	Ports	Test item	Test level	Acceptance criteria	Powered status
	Between output and protected area	insulation and voltage resistance test	600 VAC@1 min	Device cannot be damaged after test and device power on.	Power off
		insulation resistance test	500 VDC@1 min	More than 10 MΩ or according to the product specification.	Power off
EPRI TR-107330-1996	The fault of non-safety side	Common-mode overvoltage test of non-safety side	250 VAC, 60 VDC@30 s (according to the highest voltage inside the equipment)	1. The current changes of input port cannot be more than ± 0.05%F.S. 2. The current changes of other output channel cannot be more than ± 0.05%F.S. 3. The changes of power supply voltage cannot be more than ± 1%.	power on
		Differential mode over voltage test in non-safety side	250 VAC, 60 VDC@30 s (according to the highest voltage inside the equipment)	Same as above	power on
		open-circuit, connect to ground or connect to power in non-safety side	open-circuit, connect to ground or connect to power in non-safety side	Same as above	power on

4.3 The Methods of Test

Voltage withstand and insulation resistance test can be performed according to the requirements of GB - T 15479-1995. And for the isolation test of the non-safety side of the fault can be respectively performed as follows.

4.3.1 Common-Mode Overvoltage Test

The simulation of the common-mode overvoltage test is to verify, when the power supply in non-safety side is short to ground, whether it will impact on the safety side. So the common mode high voltage shall be applied between the non-safety side and the protected area. Test method of schematic diagram is shown as below (Fig. 2).

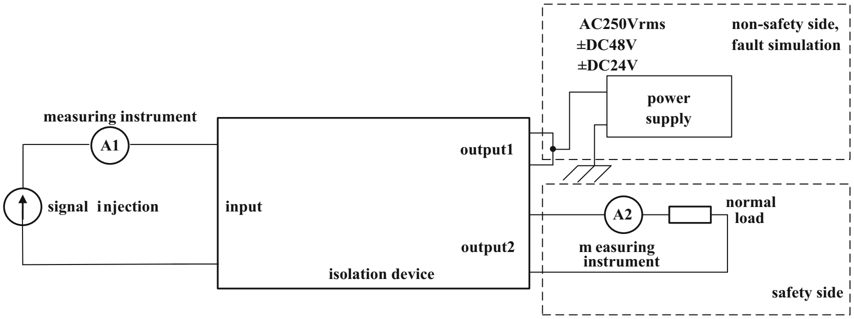


Fig. 2. Test methods diagram of common-mode overvoltage

The change of analog signal of the input and adjacent output channels should be monitored during the test process.

4.3.2 Differential-Mode Overvoltage Test

The method of differential mode overvoltage test is similar with the common mode overvoltage test, but the over voltage is applied to the positive and negative port of non-safety side output ports (Fig. 3).

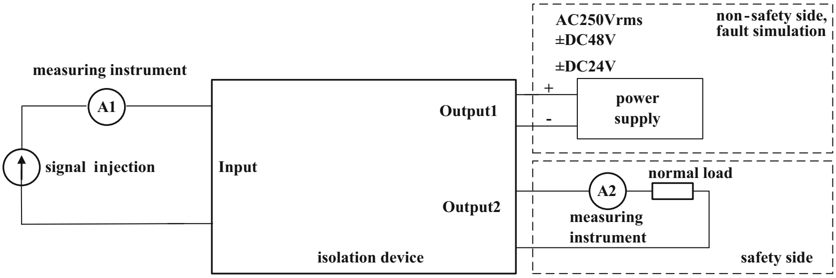


Fig. 3. Test methods diagram of differential-mode overvoltage

4.3.3 Open Circuit, Short Circuit and Ground Connection Test

The fault mode such as open-circuit, short-circuit and connect to ground shall be simulated in the non-safety side, and then the safety side signal shall be monitored to verify the disturbance. The test method of open-circuit, short-circuit and connect to ground as shown in Fig. 4.

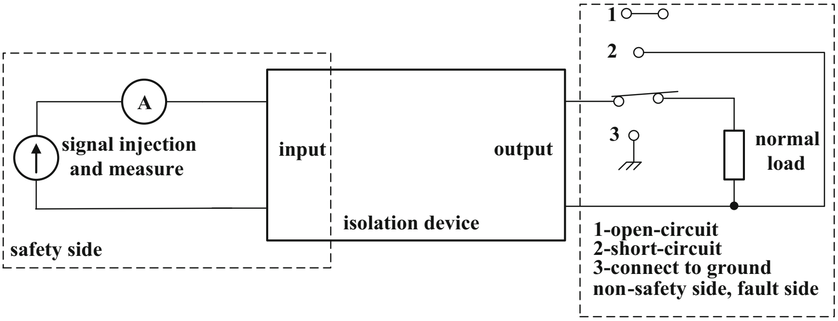


Fig. 4. Test methods diagram of open-circuit, short-circuit, connect to ground

5 Summarize

This article puts forward the test requirements for safety class electronic equipment after analyzing the isolation related standards and technical specifications in nuclear power plant safety class DCS. And after the deep comprehending of the isolation test requirements in equipment qualification standard and technical specifications, this article also puts forward the method for the isolation test port of the general isolation device, and gives the test level, acceptance criterion, combined with the characteristics of isolating device port and the experience in equipment qualification isolation test. The test method can be the complementary requirements about electric test in NB/T 20344-2015 [5]. And it was successfully used in isolation qualification test on the first self-intellectual property I&C platform in China. The method and test result was endorsed by Chinese supervision organization. The test requirements, test level, test method and acceptance put forward in this article can be used to guide the isolation test in the safety class electronic equipment qualification in nuclear power plant.

References

1. IEC 60709: Nuclear Power Plants – Instrumentation and Control Systems Important to Safety – Separation (2004)
2. IEEE 384: IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits (2008)
3. RCC-E: Design and Construction Rules for Electrical Components of Nuclear Islands (2012)

4. EPRI TR 107330: Generic Requirements Specification for Qualifying a Commercial Available PLC for Safety-Related Application in Nuclear Power Plants (1996)
5. NB/T 20344: Qualification Procedure of Safety Class Electronic Equipment in Nuclear Power Plants (2015)

The Appliance of BOP Auxiliary System Centralized Control Network in Nuclear Power Plant

Lei Jiang(✉)

State Key Laboratory of Nuclear Power Safety Monitoring Technology and Equipment,
China Nuclear Power Engineering Co., Ltd., Shenzhen 518172, China
jianglei@cgnpc.com.cn

Abstract. BOP auxiliary system centralized control network is not adopted in nuclear power plant at home and abroad. Local monitoring and control based on PLC is still the main traditional control mode for BOP system, the phenomenon of isolated information island exists in nuclear power plant. The information level of this mode is not only relatively low but also bring a lot of inconveniences for equipment spare part management, maintenance, system operation. With the development of network technology, the BOP centralized control network is a main trend in BOP auxiliary system design. The adaptation of BOP auxiliary system centralized control network is bound to impact the original project schedule, design interface, procurement, cost, and so on. It aims to provide feasible technical reference for the appliance of BOP auxiliary system control network in nuclear power plant.

Keywords: Nuclear power plant · Auxiliary system · Centralized control · BOP

1 Preface

BOP auxiliary system centralized control network (hereinafter referred to as BOP centralized control network) is different from the unit DCS (digital control system). Through the network technology, the centralized monitoring and control function of the auxiliary system or sub-item distributed in different area of nuclear power plant is realized, the whole plant information management level is so improved greatly.

BOP centralized control network is not adopted in nuclear power plant at home and abroad. Local monitoring and control based on PLC (programme logic controller) is still the main traditional control mode for BOP system [1], the phenomenon of isolated information island exists in nuclear power plant. The information level of this mode is not only relatively low but also bring a lot of inconveniences for equipment spare part management, maintenance, system operation. With the development of network technology, the BOP centralized control network not only improves the information level of the whole unit, but also achieves the purpose of reducing the labour intensity.

Y. Xu et al. (eds.), *Nuclear Power Plants: Innovative Technologies for Instrumentation and Control Systems*, Lecture Notes in Electrical Engineering 455,
https://doi.org/10.1007/978-981-10-7416-5_21

2 BOP Auxiliary System Control Scheme

From the perspective of the operation, the relationship between BOP auxiliary system and the unit is not very close. Most BOP auxiliary system operate intermittently, and serve more than one unit, the partial failure or short-term outage of equipment will not immediately affect the normal operation of unit.

The location of each BOP auxiliary system is not centralized, the signal communication between relies on the cable routed in the corridor.

Normally the design and construction cycle of a nuclear power plant is five years, some BOP auxiliary systems need to be put into use in the early stage of the project, such as the demineralized water production system.

2.1 Present Solution

The function of BOP auxiliary system in Nuclear power plant is relatively independent. The design, operation, maintenance experience of process system is relatively mature. These systems are provided as a whole package by the third part supplier, including the process equipment and PLC control device.

At present, most of the BOP auxiliary system has on-site duty room and independent PLC control devices, only some very important information is sent to the unit main control room for indication or alarm. Once perform specific task, site operator is required to check and verify locally.

The control structure of BOP auxiliary system refers to Fig. 1.

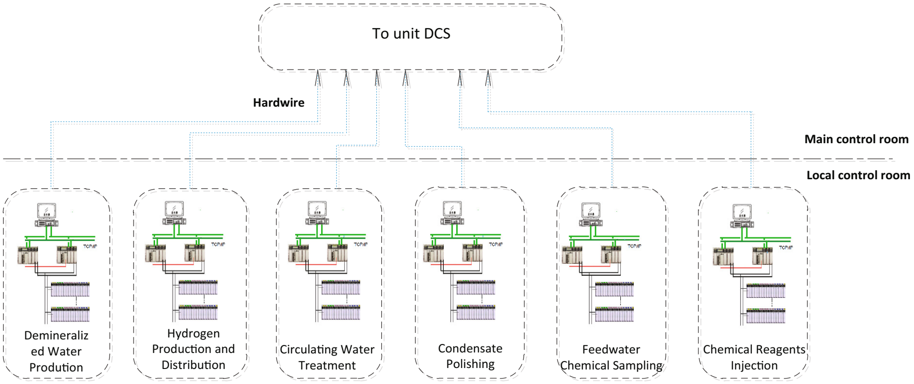

To unit DCS
Hardwire
Main control room
Local control room
Demineralized Water Prodution
Hydrogen Production and Distribution
Circulating Water Treatment
Condensate Polishing
Feedwater Chemical Sampling
Chemical Reagents Injection

Fig. 1. BOP centralized control system structure at present

Each BOP auxiliary system belongs to different procurement package, and the control device is provided by different supplier. Besides, the tending and bidding law make it clear that device is not allowed to specify the brand in the technical specification. The brand uniformity of control device (hardware and software) can't be guaranteed between system in the same project, which brings a lot of trouble for the future maintenance and spare part management.

Actually the BOP auxiliary system is not limited to the system shown in Fig. 1, BOP auxiliary system is geographically dispersed, only few signal exchange exist between main control room and BOP auxiliary system, this control solution is not favorable for the unit operation monitoring and control from the point view of time-response and maintenance convenience.

Each BOP auxiliary system has independent control device, the phenomenon of information island widely exist in nuclear power plant, lot of valuable operation data are not collected to information management system for further application.

2.2 BOP Auxiliary System Control Network

In order to solve the problems mentioned above, BOP auxiliary network solution is proposed.

Refer to the standard DL/T5227-2005 (Technical rule of thermal power automation design for auxiliary system (shop) of fossil fuel power plant) [2], the local control room of BOP auxiliary system could be merged according to the geographical distribution.

Most of BOP auxiliary system is “water” related in nuclear power plant, every two unit set up a BOP centralized control network. The BOP centralized control network structure refers to Fig. 2.

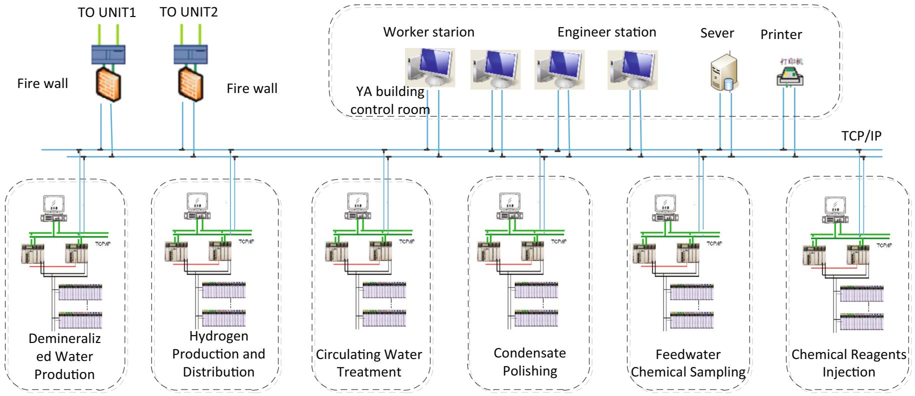

TO UNIT1
TO UNIT2
Fire wall
Fire wall
Worker starion
Engineer station
Sever
Printer
打印机
YA building control room
TCP/IP
TCP/IP
Demineralized Water Prodution
Hydrogen Production and Distribution
Circulating Water Treatment
Condensate Polishing
Feedwater Chemical Sampling
Chemical Reagents Injection

Fig. 2. BOP centralized control network structure

There are two optional schemes for BOP centralized control network, one scheme is to put the “water” related systems together to achieve centralized monitoring and control, this scheme is more in line with operation experience feedback, meanwhile it is also the priority recommended scheme in BOP auxiliary system design. The other scheme is put some other “non-water” related auxiliary system (auxiliary boilers, air compressors, waste collection and discharge etc.,) in BOP centralized control network. In fact, there is no essential difference between two schemes but the scope of system. For the second scheme, higher requirements are raised for ability of staff on duty after integration. Taking into account the first application in the nuclear power project, it is suggested that only put water-related system into the BOP centralized control network, the follow-up project can gradually expand based on operation experience feedback.

After implementing the BOP centralized control network in the nuclear power plant, all the BOP auxiliary system can share the operator station and the engineer station. Meanwhile a BOP auxiliary control room shall be considered. It is recommended to share the control room with demineralized water production system, some other local control room can be cancelled. Taking into account the actual operation needs, the local industry computer of original system can be retained as a supplementary means during start debugging or in case of network failure.

In order to implement the BOP centralized control network and make full use of the performance of network, a basic pre-condition is to realize the uniform of control system brand including hardware and software, and reduce the type of spare part as much as possible. It should be make it clear in technical specification that the design and selection of PLC must meet the BOP overall design requirements of purchaser.

After implementing the BOP centralized control network, the original local control and monitoring responsibility can be transferred to the BOP auxiliary control room operator, it can reduce the frequency of routing check, so as to reduce the work load of site operator.

After implementing the BOP centralized control network, it can further reduce the correlation with the unit DCS. It is favorable to the DCS schedule control.

BOP centralized control network leave the communication interface with unit DCS and plant information management system, all necessary data could be sent to DCS for storage, analysis, indication if need, centralized control network solve the phenomenon of isolated information island completely.

3 Feasibility Analysis

BOP centralized control network scheme is an important part of the overall design of the project, full analysis and demonstration should be done in the early stage of the project from the aspect of progress, interface, procurement, installation, commissioning, operation and so on.

3.1 Impact on Design

After implementing the BOP centralized control network, it will bring the influence of following aspects (Table 1):

Table 1. Design influence evaluation

No.	Item	Description	Evaluation and measurement
1	Operation procedure	Description and requirement of operation procedure	BOP system operation procedure should make adjustment
2	Interface with DCS	Functional and physical interface change with DCS	Thought coordination with DCS supplier, DCS schedule is not affected
3	Cable routing	The number and type of cable change	Replaced by communication cable (optical fiber), it is favorable to the layout of cable tray
4	Auxiliary control room layout	The design for auxiliary control room	It is recommended to share control room with process system, build a individual control room will lead to big civil cost
5	Procurement package	Technical requirement and scope change	Redefine the uniform technical requirement and supply scope
6	Power supply	Add double power supply and UPS	The capacity of supply is less than 5 KW, it make no big differences to electrical design
7	Respond time	Time of process increase	The time process of single direction is less than 1 s, it is in the limit of acceptance

3.2 Impact on Schedule

DCS supplier is normally defied at the first concrete date of nuclear island, but most of BOP system is not finalized at that time. In order to meet the requirements of the manufacturing progress of units DCS, a special schedule is planned to manage and track the system design, the aim is to reduce system design change is as much as possible, so as to minimize the claim of DCS manufacturers caused by system design change and ensure the project general schedule. After implementing the BOP centralized control network, the BOP auxiliary system design progress and DCS are no longer affect each other, it can reduce the impact on DCS to the maximum.

The usage of BOP centralized control network in principle does not break the existing nuclear power plant design and procurement model, it makes no difference to the overall progress of the project.

3.3 Impact on Purchasing

The normal practice in nuclear power plant is that each BOP auxiliary system is supplied as a whole package, including PLC control device. There is no signal exchange interface between auxiliary systems.

A basic requirement for BOP centralized control network is to achieve uniform brand of PLC control device, unified communication interface, data interface, unified screen display style, to maximize the advantages of centralized control network in the system maintenance and spare parts management. In order to achieve the above objectives, the BOP auxiliary system procurement strategy of original nuclear power reference project has to be adjusted. Two optional schemes are available.

Scheme one: the entire BOP centralized control network (large frame) and individual auxiliary system are put in a tender package. A bidder with successful experience undertakes this package and is in charge of integration of other subsystems interface. BOP centralized control network and equipment procurement is recommended to be included in the Demineralized Water Production system procurement package. The Demineralized Water Production system procurement package supplier should ensure the general performance of BOP centralized control network, and define the uniform technical requirements, including data exchange format, content and depth. The biggest advantage of this approach is that it will not have a big impact on the existing procurement model.

Scheme two: take the control device (PLC) out of the each package (each BOP auxiliary system has independent set package), all control devices are supplied and commissioned by the third party supplier. The biggest advantage of this approach is to ensure the unity of design requirements. The disadvantage is that the presentation depth of logic diagram provided by each auxiliary system supplier is not detail enough, the logic diagram of each supplier is only a functional expression due to intellectual property considerations, besides, the third party are not familiar with the operation of all process system, therefore there exist great risk in scheme two 2.

No matter the scheme one or scheme two is chosen, the necessity technical requirements (PLC brands and performance communication interface, screen style, line, color, icon, etc.) should be given clearly in the technical specifications.

3.4 Other Impact

After implementing the BOP centralized control network in the nuclear power plant, the main control room operator no more deal with the monitoring task related to BOP auxiliary system, the responsibility are transferred to the BOP auxiliary control room operator. The operation staff for BOP auxiliary system should be also reconfigured.

Do not consider the cost of adding the building for the new control room, only some network equipment and software need to be purchased on the basis of the original project, a one-time investment increased slightly, but not significant, the total cost of the project is not obvious.

4 Conclusions

BOP auxiliary system centralized control network has been widely adopted in the thermal power plant, nuclear power plant can also learn from the mature application of thermal power plant experience. It can solve the phenomenon of isolated information island exists in nuclear power plant; there are no technical problems and application risks. The adoption of BOP auxiliary system control network can significantly improve the unit information level, reduce staff workload, and bring many other advantages in spare parts management and system maintenance.

References

1. Guangdong nuclear training centre, devices & systems of 900 MW PWR. Atomic Energy Press (2007)
2. Tianhong, Technical rule of thermal power automation design for auxiliary system (shop) of fuel power plant (DL/T 5227-2005)
3. HAF 102: Safety of Nuclear Power Plant Design Regulations (2004)
4. Tao, Y.R., Jiang, M.Y.: Application of Digital Computers to Instrumentation and Control in Nuclear Power Plant (EJ/T 1060) (1998)

Research on New Displacement Sensor Used in Active Magnetic Bearing Systems

Lian-Xiao Xue, Kai Zhang(✉), and Yang Xu

Department of Engineering Physics, Tsinghua University, Beijing 100084, China
zhangkai@mail.tsinghua.edu.cn

Abstract. Active magnetic bearings (AMBs) play an important role in the helium turbine of High Temperature Gas-cooled Reactor (HTR). As one of the main components of the AMB, the displacement sensor influences the performance of the whole AMB system. In this paper, a new radial displacement sensor which characterized by high cost-efficiency, high accuracy, high sensitivity, and compact structure is discussed. Through establishing an equivalent model of the sensor, the theory of the sensor was derived. Then, a finite element model was constructed to analyze various factors that affect the sensor sensitivity and structure. Furthermore, an experimental platform was built to evaluate the sensor. As a result, the sensor exhibited an original sensitivity of 38.94 mV/μm, a good linearity of 1.87% and a low X-Y coupling degree of 2.14%. This sensor was applied to an AMB system and achieved stable suspension at a speed of 12 000 rpm. It is expected to be extended to HTR related applications due to its excellent performance.

Keywords: HTR · AMB · Eddy current sensor · Finite element analysis

1 Introduction

With the advantages of no contact, high cleanliness, high speed, high control precision, low maintenance cost, and extended lifespan [1], AMBs are widely used in clean vacuum system, turbine machinery, etc. The main helium turbine of HTR is also suitable for the use of AMB. In a high-speed AMB system, the sensor requires good bandwidth and high resolution to detect the rotor radial displacements accurately and quickly. Traditional eddy current or inductive sensors could meet the requirements, but they usually need to be manually fabricated, making it difficult to achieve satisfactory uniformity. In addition, in some applications, the space left for the sensor is limited for a rotor with a smaller length-diameter ratio to surpass a critical speed. Therefore, it is necessary to develop compact sensors.

Bühler proposed a new type of radial displacement sensor [2, 6]. In his design, a printed circuit board (PCB) which embedded sensor coils replaced a sensor probe and

This work was supported by National Natural Science Foundation of China (Grant No. 51775292).

Y. Xu et al. (eds.), *Nuclear Power Plants: Innovative Technologies for Instrumentation and Control Systems*, Lecture Notes in Electrical Engineering 455,
https://doi.org/10.1007/978-981-10-7416-5_22

the PCB sensor was used to monitor the central rotor directly. This allowed the sensing coils to be sufficiently close to the rotor. Compared with the conventional sensors, higher sensitivity and smaller axial space occupied were achieved. After that, this sensor was further developed [3, 4, 7] and used in industrial environments, for example, a magnetically levitated 500 krpm permanent magnet machine [8] and a 125 kW waste heat recovery system [5].

PCB design is the focus of the PCB sensors. The width and spacing of PCB copper coils are two key factors related to the sensitivity of the sensor. Andreas MÜSIN chose 150 μm, which was the PCB manufacturer-processing limit, as the track width and track spacing. However, in our opinion, using the manufacturer-processing limit as the track width and spacing is not suitable. Smaller track width and spacing indeed make the rotor closer to the sensor coils, but meanwhile, the coils' resistance also become larger, which leads to sensitivity reduction. Therefore, the specific track width and spacing of the sensor need more elaborate analysis.

This work focused on the optimization of the new PCB sensor. Firstly, the principle of sensor position detection was further deduced. Secondly, the factors that mainly influenced the sensitivity of the sensor were analyzed by finite element simulation, and an optimized PCB sensor was designed for the following experiment. Next, a test platform was built to complete the performance evaluation, including sensitivity, linearity and X-Y coupling degree. Finally, this sensor was applied to an existing AMB system, and a stable suspension was achieved.

2 Sensor Theory

This new position sensor is called transverse flux sensor (TFS). In this section, the structure of TFS is described, and the theory of TFS is derived.

The TFS consists of a central rotor, an excitation coil driven by a high-frequency voltage or current, and four sensing coils surrounding the excitation coil. Figure 1 shows the position detection principle of a TFS. When the rotor is centered, as shown in Fig. 1(a), the mutual inductances between the opposite sensing coils and the excitation coil are identical due to the symmetry of the structure.

As shown in Fig. 2(b), the total magnetic field on the left side is enhanced as the rotor moves towards the left, and the corresponding magnetic flux is increased; on the contrary, the magnetic flux on the right side is decreased. As a result, the mutual inductances between the opposite sensing coils and the excitation coil are no longer equal, and their difference, defined as M_{eff}, is associated with the displacement of the rotor.

The equivalent circuit of the TFS is shown in Fig. 2. Where L_{exc} and L_{sens} are the inductance of the excitation coil and the opposite sensing coils, R_{exc} and R_{sens} are the resistance of copper track inside the PCB (considering the skin effect and the proximity effect), C_{exc} and C_{sens} are capacitors for the excitation coil and the opposite sensing coils in order to achieve resonance respectively.

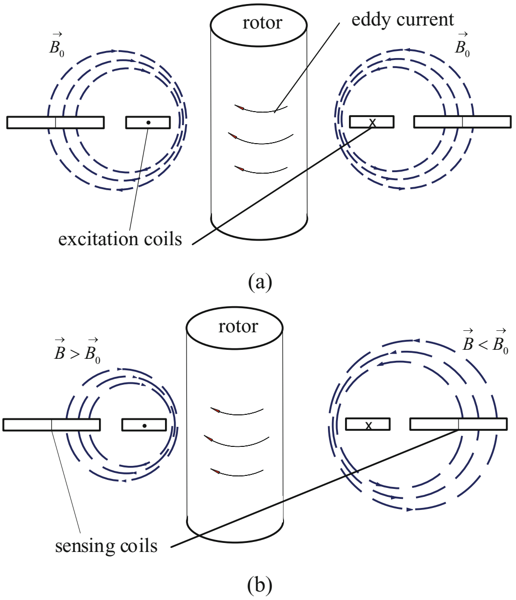


Fig. 1. Illustration of the position detection principle. (a) Centered rotor with the symmetrical magnetic field; (b) eccentric rotor with the asymmetrical magnetic field

When the excitation coil and the sensing coils achieve resonance at the same time, and the resonance frequency equals to the excitation frequency, the TFS works in the best condition. According to [7], the sensor output voltage U_{sens} is given by

$$U_{\text{sens}} = \frac{M_{\text{eff}} I_{\text{exc}}}{C_{\text{sens}} R_{\text{sens}}}. \tag{1}$$

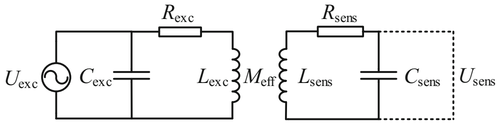


Fig. 2. The equivalent circuit of the TFS

The two coils circuit are RLC parallel circuit with resistance in series with the inductor and the resonant frequency is given by

$$f = \frac{1}{2\pi\sqrt{L_{\text{sens}} C_{\text{sens}}}}. \tag{2}$$

To drive the excitation coil with high-frequency voltage, the AC constant voltage source was chosen. Assuming that the voltage applied to the excitation coil is U_{exc}, the current of the excitation coil I_{exc} is given by

$$I_{\mathrm{exc}} = \frac{U_{\mathrm{exc}}}{2\pi f L_{\mathrm{exc}}}. \tag{3}$$

Substitute (2)–(3) into (1), the voltage of sensing coils is given by

$$U_{\mathrm{sens}} = 2\pi f U_{\mathrm{exc}} \cdot \frac{M_{\mathrm{eff}} L_{\mathrm{sens}}}{L_{\mathrm{exc}} R_{\mathrm{sens}}} \tag{4}$$

Moreover, the sensitivity of the TFS is given by

$$S = \frac{\mathrm{d}U_{\mathrm{sens}}}{\mathrm{d}x} = 2\pi f U_{\mathrm{exc}} \cdot \frac{L_{\mathrm{sens}}}{L_{\mathrm{exc}} R_{\mathrm{sens}}} \cdot \frac{\mathrm{d}M_{\mathrm{eff}}}{\mathrm{d}x}. \tag{5}$$

For convenience, s is defined as

$$S \propto s = \frac{L_{\mathrm{sens}}}{L_{\mathrm{exc}} R_{\mathrm{sens}}} \cdot \frac{\mathrm{d}M_{\mathrm{eff}}}{\mathrm{d}x}. \tag{6}$$

It is concluded that the variables that mainly affect the sensitivity of the TFS are f, U_{exc}, L_{exc}, L_{sens}, R_{sens}, and M_{eff}. The voltage that can be applied to the excitation coil is limited by the device characteristics, and the excitation frequency is restricted by the load capacity of the circuit. The rest of the factors can be attributed to the PCB design on the excitation coil and sensing coils inherent parameters, and an ideal design should achieve an optimal s.

3 Sensor Modeling, Analysis, and Optimization

In this section, a finite element model was established to analyze the influence of several key factors on the sensitivity of the TFS, and an optimized sensor model was obtained considering the sensitivity and the processing cost of the TFS.

3.1 Sensor Modeling

To explore the electrical and structural characteristics of the TFS and achieve an optimized TFS PCB design, as widely used finite element software, *ANSYS Electronics* was selected for modeling and simulation. The eddy current field solver of *ANSYS Electronics* was chosen for calculating the electromagnetic field. Figure 3 shows the structure of a sample simulation model. The model is a four-layer PCB; each layer consists of the two-turn centric excitation coil, five-turn sensing coils surrounding the excitation coil, as well as the rotor in the center. An actual PCB board also contains the dielectric insulator, which owns very high values of resistivity (in the order of $10^{10\sim14}$ Ω·m), and it can be omitted in the simulation due to such large resistivity.

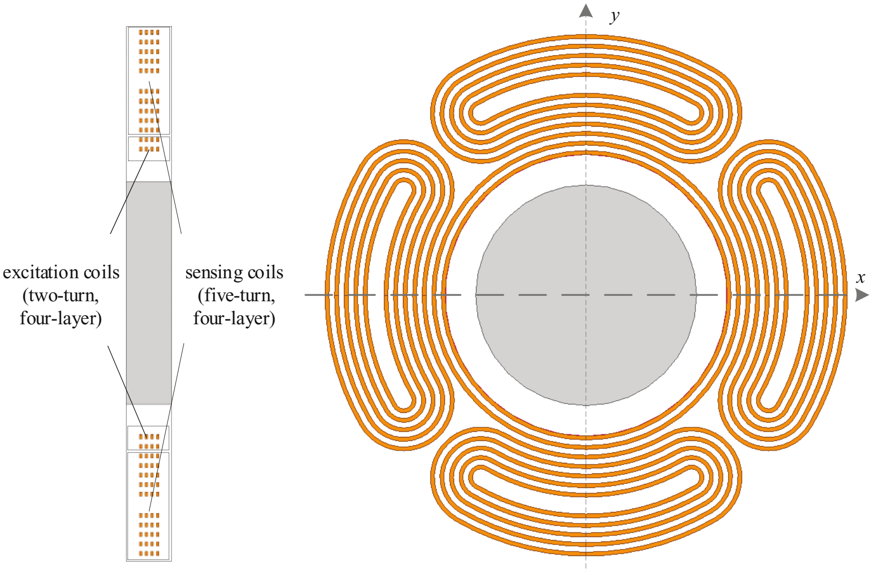


Fig. 3. The structure of a sample simulation model

The actual copper tracks in the PCB are spiral, but in order to simplify the model, the circular coil is used to replace the spiral coil. It is proved that the replacement is valid because of the similar simulation results. The following analysis and optimization work are based on this simulation model with needed adjustments.

3.2 Sensor Analysis

In this section, the influence of the rotor displacement, excitation frequency, rotor material, track width, track spacing, and copper thickness on the sensitivity of the TFS is further calculated and analyzed. It should be noted that all simulation need to consider the skin effect of the rotor and copper tracks.

3.2.1 Rotor Displacement

While the position of the rotor changes, the difference in mutual inductance M_{eff} also changes. Figure 4 shows the simulation results of M_{eff}, L_{exc}, L_{sens} and R_{sens} under a series of displacements at a specific frequency. It can be seen that as rotor moves, the difference between the excitation coil and the sensing coils is predominant, and the other parameters are nearly unchanged.

The inductance and resistance of the coils are inherent in their properties and usually unaffected by the external magnetic field. But as the rotor moves, a good linear relationship between M_{eff} and the displacement x is found. The simulation proves that the TFS is feasible.

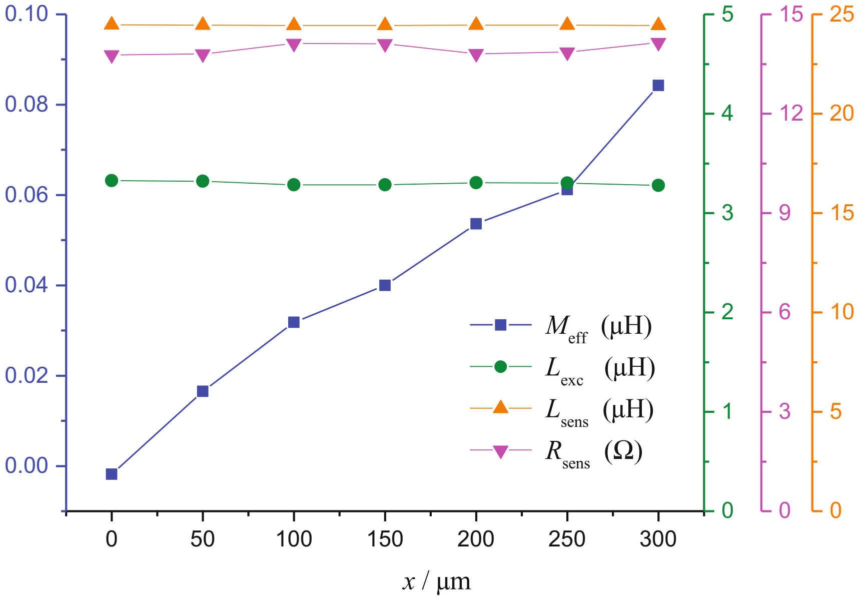


Fig. 4. Coil parameters vs Rotor displacement ($f = 3$ MHz)

3.2.2 Excitation Frequency

The excitation frequency has a significant influence on the parameters of a PCB design. Figure 5 shows the trends of the related parameters when the frequency increases from 10 kHz to 100 MHz. The inductance of the excitation coil and the sensing coils do not change with frequency, while the resistance of the sensing coils has a different trend. The resistance of the sensing coils is almost constant firstly as shown in Fig. 5. However, as the frequency exceeds 1 MHz, the resistance increases rapidly. This is because, in the high-frequency current excitation, the AC impedance of PCB copper tracks substantially increased due to skin effects and proximity effects. For the same reason, the change rate of mutual inductance difference with displacement is also saturated after the frequency exceeds 1 MHz. The higher the frequency, the more concentrated the eddy current on the rotor surface, and finally, when it is considered to be the surface current, $\mathrm{d}M_{\mathrm{eff}}/\mathrm{d}x$ tends to saturation [7].

The trend of s with the frequency could be explained. The higher frequency cannot bring a bigger $\mathrm{d}M_{\mathrm{eff}}/\mathrm{d}x$, but increase the R_{sens} after the frequency exceeds 1 MHz. Finally, this could result in a significant decline in s after the skin effect and the proximity effect became apparent. It should be noted that s is only related to PCB design, and the other factors, such as the excitation frequency and the driving voltage also affect the sensitivity of TFS, so the sensitivity does not begin to drop actually when the excitation frequency exceeds 1 MHz. Considering the simulation results and the actual circuit design, the excitation frequency of 1–8 MHz is recommended.

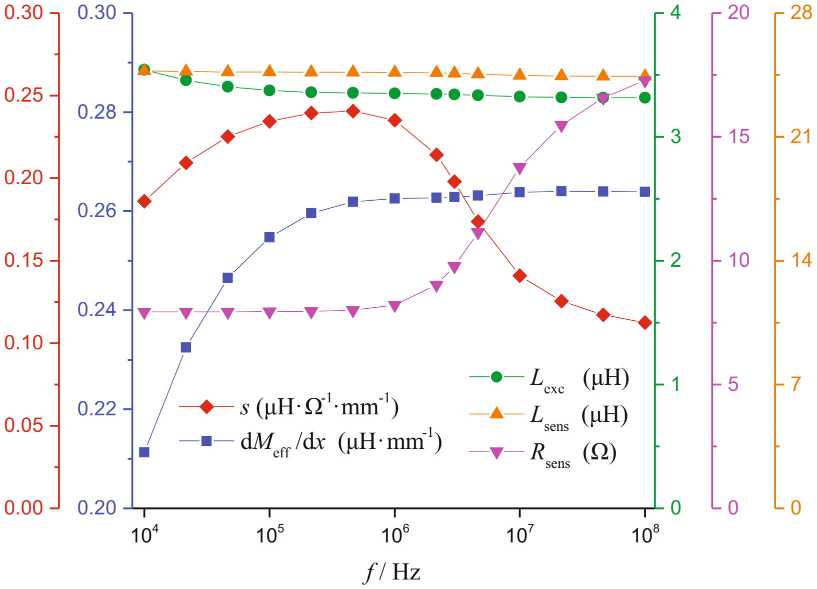


Fig. 5. Coil parameters vs. Excitation frequency

3.2.3 Rotor Material

Since the TFS is dependent on the eddy current generated on the surface of the rotor, the rotor's material also has a certain effect on its sensitivity. In this section, the rotor of different materials with different relative permittivity, relative permeability, and bulk conductivity is studied, and the simulation results are shown in Table 1.

Table 1. Comparison of sensor sensitivity for different rotor materials

Index	#1	#2	#3	#4
Relative permittivity	1	1	1	6
Relative permeability	6	6	1	6
Bulk conductivity (Msiemens·m^{-1})	38	1.1	38	38
L_{exc} (μH)	3.78	3.81	3.30	3.78
L_{sens} (μH)	24.82	24.82	24.56	24.82
R_{sens} (Ω)	9.75	10.29	9.79	9.75
dM_{eff}/dx (μH·mm^{-1})	0.221	0.172	0.283	0.221
s (μH·mm^{-1}·Ω^{-1})	0.149	0.109	0.215	0.149

As shown in Table 1, compared with standard group #1, #2 changed the bulk conductivity, #3 changed the relative permeability, and #4 changed the relative permittivity, the other model parameters are consistent. The following conclusions can be obtained from the analysis of Table 1:

1. The rotor with high bulk conductivity increases the sensitivity (#1 vs. #2).

2. The rotor with high relative permeability weakens the sensitivity (#1 vs. #3).
3. The relative permittivity of the rotor does not affect the sensitivity (#1 vs. #4).

For a TFS, the rotor produces eddy currents on the surface of high-frequency magnetic fields, the higher the bulk conductivity, the greater the intensity of the vortex, resulting in a stronger magnetic field and an excellent sensitivity; on the other hand, if a rotor with high relative permeability, such as a ferromagnetic rotor, was closing to the coil, the L_{exc} increase and the $\mathrm{d}M_{eff}/\mathrm{d}x$ decreases, finally resulting in a reduction in sensor sensitivity.

In comprehensive, the rotor material with high conductivity, low permeability is advisable. Generally, choose aluminum or copper.

3.2.4 Track Width, Track Spacing, and Copper Thickness

Previous researchers have identified the layout optimization as the focus of the TFS, but the combination of manufacturing processes and layout optimization is a better choice. The width and spacing of PCB copper coils have a significant effect on the sensitivity of the TFS. Andreas MÜSIN selected 150 μm as the width and spacing value. However, a larger width and spacing may be more conducive to improving the sensitivity of TFS.

Corresponding to a particular copper thickness, the minimum track width and track spacing have limits. Table 2 lists the manufacturing capabilities of sample orders. It can be seen that for a particular copper thickness, for example, 1 oz, the inner layer copper may have the minimum track spacing of 4 mils, while the outer layer copper can only achieve the minimum track spacing of 5 mils, and this increases the difficulty of PCB design. To obtain the best sensitivity of TFS, it is necessary to carefully select the copper thickness, track width and track spacing of the inner and outer copper.

Table 2. Manufacturing capacity of sample orders

Copper thickness (oz)[a]	Minimum track width (mil)[b]		Minimum track spacing (mil)	
	Inner layer	Out layer	Inner layer	Out layer
0.5	3	4	3	4
1	4	5	4	5
2	5	6	6	8
3	7	7	9	10
4	8	8	12	13
5	10	10	15	16
6	12	12	18	18

[a] Ounces (oz) is the most common unit of measuring the copper thickness on a printed circuit board (PCB), and 1 oz equals to 34.79 μm in SI units.

[b] Mil is most commonly used in manufacturing dimensions and tolerances of PCBs, and 1 mil equals to 25.40 μm in SI units.

A smaller sensing coils resistance requires a thicker copper thickness. But due to cost-efficiency, copper cannot be too thick. On the other hand, affected by the skin effect and the proximity effect, it is not helpful to reduce the resistance of the excitation coil while the thickness is beyond the corresponding skin depth at a certain excitation frequency.

The skin depth is defined as

$$\delta = \sqrt{\frac{1}{\pi f \sigma \mu}} \tag{7}$$

Where δ is the skin depth in meters, μ is the permeability (for copper, $\mu = 1.26 \times 10^{-6}$ H/m), σ is the conductivity (for copper, $\sigma = 5.96 \times 10^{7}$ S/m), f is the excitation frequency in Hz.

The skin depth of copper at a frequency of 3 MHz is given by

$$\delta = \sqrt{\frac{1}{\pi \times 3 \times 10^{6} \times 5.96 \times 10^{7} \times 1.26 \times 10^{-6}}} = 37.6\,\mu\text{m} \tag{8}$$

It can be considered that when the thickness of copper exceeds twice the skin depth, that is, after 75.2 μm, the sensing coils resistance cannot be effectively reduced. Therefore, the thickness of copper should not be more than 105 μm (3 oz) as shown in Table 2.

For a 4-layer PCB, each layer owns a similar shape (which means that the outer layer is limited). At each level of copper thickness, take the smallest track spacing and the proper track width. Then four different PCB designs are shown in Table 3.

Table 3. Comparison of sensor parameters for different PCBs

No of design	#1	#2	#3	#4
Track width (mil)	4	5	6	7
Track spacing (mil)	4	5	8	10
Copper thickness (oz)	0.5	1	2	3
L_{exc} (μH)	3.43	3.41	3.38	3.32
L_{sens} (μH)	25.05	24.73	24.43	24.28
R_{sens} (Ω)	26.79	11.91	7.00	5.44
$\mathrm{d}M_{\text{eff}}/\mathrm{d}x$ (μH·mm^{-1})	0.381	0.342	0.312	0.260
s (μH·mm^{-1}·Ω^{-1})	0.104	0.208	0.322	0.349

Table 3 also lists the simulation results of the four models. It can be concluded that the thicker copper is indeed gain the sensitivity of TFS through reducing the R_{sens} without losing too much $\mathrm{d}M_{\text{eff}}/\mathrm{d}x$.

From a cost-effective aspect, unceasingly increasing the copper thickness to promote the sensitivity yields to the processing cost. So, it is recommended that choosing a 3 oz copper thickness, 7 mil track width and 10 mil track spacing as an optimized TFS design.

3.3 Sensor Optimization

For a rotor with 32.35 mm diameter to be monitored, the optimal TFS design is to get the maximum s. Based on the previous analysis results, the aluminum alloy was selected as the rotor material, and the appropriate track width, track spacing, and copper thickness were set, finally, a TFS with the parameters shown in Table 4 was constructed.

Table 4. Parameters of the optimized TFS model

Parameters	Design value
Track width (mil)	7
Track spacing (mil)	10
Inner layer copper thickness (oz)	0.5
Outer layer copper thickness (oz)	1
Center hole diameter (mm)	34
L_{exc} (μH)	3.34
R_{exc} (Ω)	4.28
Q_{exc}	15.75
L_{sens} (μH)	24.80
R_{sens} (Ω)	13.63
Q_{sens}	36.71
$\mathrm{d}M_{\text{eff}}/\mathrm{d}x$ (μH·mm^{-1})	0.285

Although it is concluded that the optimized copper thickness is 3 oz for a common TFS, it is still worthwhile to reduce the copper thickness to lower the processing cost if the desired sensitivity can be achieved at a thinner copper thickness.

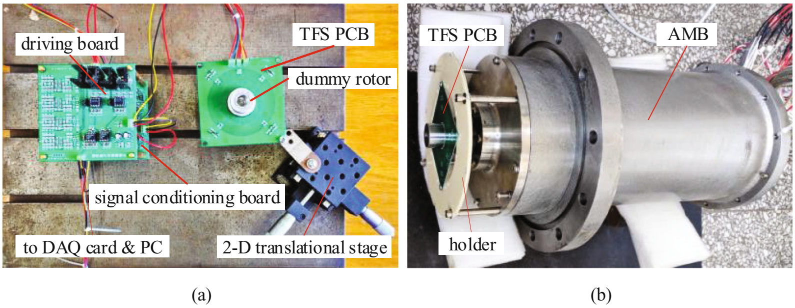
The simulation results showed that the sensitivity of the sensor has reached the target system requirement when choosing 0.5 oz as the inner layer copper thickness and 1 oz as the outer layer copper thickness, which is the default process of the manufacturer, and such a choice greatly reduced the processing costs.

Assuming the RMS value of the driving voltage U_{exc} is 16.3 V and the excitation frequency is 3.211 MHz, theoretically, the sensitivity of this TFS is 51.2 mV/μm according to Eq. (5).

4 Experimental Setup

To test the actual performance of the TFS, an experimental platform, which includes a sensor pre-test system and an active magnetic bearing system, was built to complete several tests. As shown in Fig. 6, the pre-test system consists of the driving board, TFS PCB, two-dimensional translational stage, dummy rotor, signal conditioning board, data acquisition card and computer. A TFS was tested and calibrated firstly; then it was installed on the active magnetic bearing externally for following suspension and rotation experiments.

In the experiment, the driving board generates a 3.211 MHz, 16.3 V RMS sinusoidal voltage signal to drive the excitation coil. The displacement of the dummy rotor can be driven by the two-dimensional translational stage in X and Y directions with a 10 μm step. Then, the voltage signals on the sensing coils are demodulated and filtered by the



(a)

(b)

Fig. 6. Experimental platform. (a) Sensor pre-test system; (b) an active magnetic bearing system with TFS externally installed

signal conditioning board and sampled by the data acquisition card into the computer for subsequent processing.

The key point of the sensor experiment is the resonance of excitation coil and the sensing coils. To tune the TFS, firstly, place the rotor in the center and adjust the capacitor in parallel with the excitation coil to make the excitation coil resonant, the indication of resonance is that the driving current reaches the minimum; then shift the rotor to limiting X+ position, adjust the capacitor in parallel with the X+ sensing coil to reach resonant, the indication of sensing coil resonance is that the output voltage reaches the maximum; in the same way, the sensing coils of X−, Y+, Y− position are adjusted sequentially.

5 Sensor Measurements

The TFS can detect two radial displacements simultaneously. In the experiment, the TFS of the parameters shown in Table 4 was used to monitor the displacements of the aluminum alloy rotor with a diameter of 32.35 mm.

Center the rotor in the X direction and move the rotor in the Y direction, the output of the sensor is shown in Fig. 7. In the Y direction, the sensor has a high sensitivity of 38.94 mV/μm[1], a good linearity of 1.87%, and a measuring range of ±0.7 mm.

When the sensor moves along the Y axis, the sensing voltage fluctuation in the X direction is very small. That means, the X-Y coupling between the two directions is very low (2.14%), the two measurement results are independent.

When the rotor displacement in the Y direction is zero, the output voltage of the TFS in Y direction is lower than 0 V, which is caused by a small mechanical installation and processing bias, as well as some little differences in circuit parameters between the two sensing coils. Therefore, the TFS needs to be carefully zeroed and calibrated during installation.

For TFS, although the outputs of the X-Y direction are independent, the resonant states of the two-directional sensing coils are interdependent during tuning, and in

[1] The sensitivity in this paper is the initial sensitivity without any amplification.

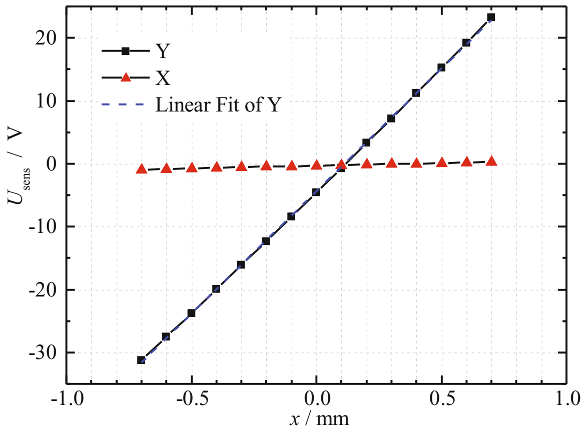


Fig. 7. The outputs of the TFS when the rotor shifts along the Y axis

particular, the resonances weaken each other. But the simulation is based on the symmetric model, considering only a single direction of mutual inductance changes. Therefore, to better compare with the simulation results, we only tuned the two sensing coils in the same direction and got a set of experimental results. Figure 8 shows the comparison of experimental and simulation results.

It can be seen from Fig. 8 that the experimental result for a single dimension is only slightly lower than the simulation result, which proved the correctness of the simulation and TFS design rules. As for the difference between experiment and simulation, it can be attributed to the following factors.

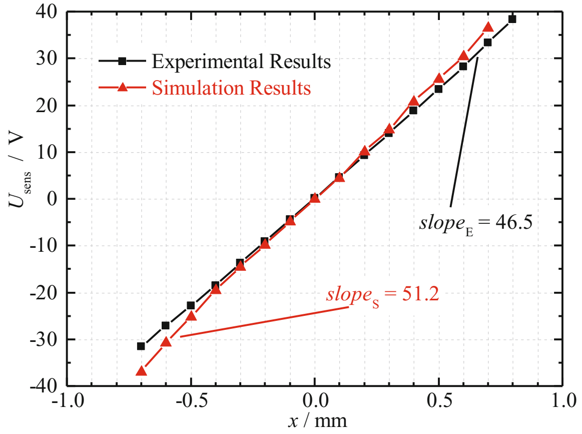


Fig. 8. The comparison of experimental and simulation results when the rotor shifts along a single axis

- The tuning states of the excitation coil and the sensing coil are not perfect, and the simulation results are based on the ideal resonance state, while the experimental process would shift the resonance state.
- The parameter difference between the ideal model and the actual PCB.
- Distribution parameters caused by the wiring.

The sensor was mounted on an AMB system and achieved a stable suspension at a speed of 12 000 rpm successfully. The orbit of the rotor at this speed is shown in Fig. 9. The displacement range of the sensor is ±200 µm. After the AMB system is stable, the rotor orbit radius is not more than ±30.3 µm.

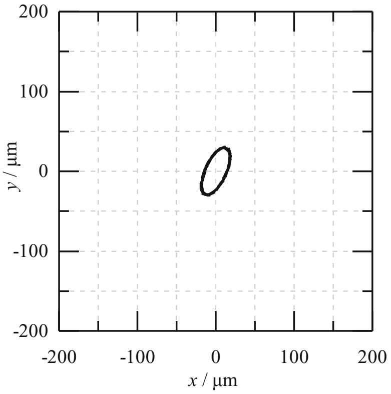


Fig. 9. The orbit of the rotor

6 Conclusions

This work discussed the theory of the TFS which is used to detect the rotor displacement in the field of the magnetic bearings. With the help of *ANSYS Electronics*, several factors that affect TFS performance were analyzed and optimized, and an optimized TFS for detecting an aluminum alloy rotor with 32.35 mm diameter was achieved. An experimental platform was built to evaluate the TFS, and the results showed that the TFS had an ultra-high sensitivity of 38.94 mV/µm, a good linearity of 1.87%, and a low X-Y coupling of 2.14%. In addition, smaller differences between the simulation and the experimental results further confirmed the correctness of the optimization. Finally, an AMB system with TFS installed achieved a stable suspension at a speed of 12 000 rpm with not more than ±30.3 µm rotor orbit radius.

Future work will include optimizing the TFS PCB for higher integration, applying the compact TFS to the main helium turbine of HTR to reduce its length-to-diameter ratio, and developing digitized TFS.

References

1. Bleuler, H., Cole, M., Keogh, P., et al.: Magnetic Bearings: Theory, Design, and Application to Rotating Machinery. Springer Science & Business Media, Heidelberg (2009)
2. Bühler, P.: Device for contact-less measurement of distances in multiple directions. European Patent No. EP 1: 422-492 (2004)
3. Burdet, L.: Active magnetic bearing design and characterization for high temperature applications. École Polytechnique Fédérale de Lausanne, Lausanne (2006)
4. Burdet, L., Maeder, T., Siegwart, R., et al.: Thick-film radial position sensor for high temperature active magnetic bearings. In: 10th International Symposium on Magnetic Bearings, Martigny, Switzerland (2006)
5. Hawkins, L.A., Zhu, L., Blumber, E.J.: Development of a 125 kW AMB expander/generator for waste heat recovery. J. Eng. Gas Turbines Power. 133(7), 072503 (2011)
6. Larsonneur, R., Bühler, P.: New radial sensor for active magnetic bearings. In: 9th International Symposium on Magnetic Bearings, Lexington, USA (2004)
7. Muesing, A., Zingerli, C., Imoberdorf, P., et al.: PEEC-based numerical optimization of compact radial position sensors for active magnetic bearings. In: 5th International Conference on VDE Integrated Power Systems (CIPS), pp. 1–5 (2008)
8. Zingerli, C.M., Imoberdorf, P., Kolar, J.W., et al.: Rotor position measurement for a magnetically levitated 500’000 rpm permanent magnet machine. In: Energy Conversion Congress and Exposition (ECCE), pp. 1778–1784. IEEE (2011)

The R&D of FPGA-Based FitRel Platform in Nuclear Power Plant Diversity Actuation System

Yong-Bin Sun, Chun-Lei Zhang, Yin-Jie Chen(✉), and Tao Bai

China Techenergy Co., Ltd., 5 Yongfeng Road, Haidian District, Beijing 100094, China
chenyinjie@cgnpc.com.cn

Abstract. FitRel platform is developed based on FPGA technology, which is similar to relay technology has intrinsic diversity compared to the micro-processor technology, and also has the advantage of lower complexity, simpler verification and validation processes, etc. This paper presents the architecture, mechanical, function safety and HPD (hardware description language programmed device) design of FitRel platform, and also presents the difficulties and challenges faced during its application. FitRel platform is successfully applied in diversity actuation system (DAS) of ACPR1000 project to handle the common cause failure (CCF) problems of RPS based on micro-processor technology.

Keywords: FPGA · DAS · I&C · NPP

1 Introduction

Diversity Actuation System is applied to handle CCF of RPS, and reduce the influence of Anticipated Transient Without Scram (ATWS) [1]. In order to achieve sufficient diversity to RPS, nowadays there are commonly two kinds of DAS technology in NPP I&C system: the relay-based technology and different micro-processor-based technology. The scale of algorithm processing is limited in the relay-based technology, and it is also not easy to maintain, although it has sufficient diversity to RPS of processor-based, for example, it does not has the function of online self-monitoring and communication. The different microprocessor-based technology does not have sufficient diversity, and it is difficult to be certified in design, equipment, human and software diversity. Field Programmable Gate Array (FPGA) technology, similar to relay technology has intrinsic diversity compared to the processor in architecture, design, and human, and similar to the processor has the advantage of easy-to-use [2, 3].

FPGA technology has been applied in non-nuclear I&C field for a long time, in recently years, more and more countries agreed to introduce the FPGA technology in nuclear I&C field. Compared to the micro-processor technology, FPGA is featured of lower complexity, simpler verification and validation processes, segregation of safety and non-safety functions, reduced vulnerability to cyber security attacks, etc., all of which are quite suitable for nuclear application. This paper introduces the research and development (R&D) of pure FPGA-based (without embedded-microprocessor and controller) FitRel platform, and its application in ACPR1000 project.

Y. Xu et al. (eds.), *Nuclear Power Plants: Innovative Technologies for Instrumentation and Control Systems*, Lecture Notes in Electrical Engineering 455,
https://doi.org/10.1007/978-981-10-7416-5_23

The structure of this paper is as follows; The second part describes FitRel platform development; The third part gives the application of FitRel platform in ACPR1000 project DAS.

2 R&D of FPGA-Based FitRel Platform

As for microprocessor-based I&C platform, which is widely used in NPPs and other industries, FPGA-based system is considered to be featured of simplicity, high performance, long-term support [4]. Firstly, the simplicity feature means without any complicated embedded software, such as the operating system and functional independence which ease the difficulty of verification and validation (V&V) and reduce the cycle of safety certification. Secondly, the high performance feature means that FPGA processes different functions in parallel driven by the high frequency clock, compared to the series cycle scan mode of processor and can be applied in high requirements of response time. The last feature is long-term support, as the FPGA technology allows a significant degree of design portability, i.e. only the final steps (synthesis and place and route) are dependent on the particular FPGA circuit chosen. This mitigates their vulnerability to obsolescence, while the microprocessor-based digital I&C system pays a high price of redesign of hardware and software.

The DAS equipment FitRel platform is base on FPGA without any IP cores or embedded microprocessors to achieve enough diversity. All functions are fulfilled by hardware description language (HDL) with top-down design method, without operating system and complicated interface to achieve simplicity, reliability, and safety.

The FitRel platform design is consists of architecture, mechanical, function safety and HPD design.

2.1 Architecture Design

Figure 1 shows the FitRel platform architecture. The process of Software (HDL) design shall meet the requirements of IEC62138 category B as the DAS is a important safety system [5], while the technical requirements of HDL design are according to the NUREG/CR 7006, EPRI-TR 101918, and the IEC62566 is for reference. In order to decrease the proportion of repeated qualification, the boundary between platform and application portion is defined clearly in the architecture design. The architecture include four kinds of functions: schedule and processing function, physical signal processing, communication and auxiliary function. The modules in solid line is fixed and only the application FPGA (AFPGA) part in dotted line can be modified by users. The qualified FitRel platform is the base of engineering project. The specific engineering project just focuses on the application functions fulfilled by HLD in AFPGA.

To satisfy the general requirement in different project, the four functions are decomposed into different modules.

Schedule and processing function is decomposed into two modules: AFPGA (Application FPGA) and GFPGA (Generic FPGA). GFPGA is the schedule centre just like the operating system. The typical function is as follows: data communication to AFPGA,

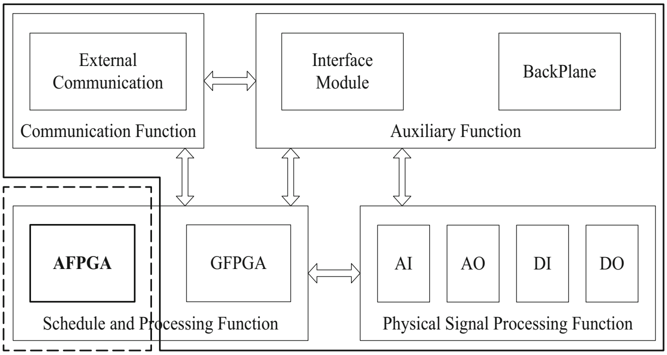


Fig. 1. Architecture of FitRel platform

HMI (Human Machine Interface) and IO modules; Download application function algorithm; Maintenance parameters of application function; Failure diagnosis; Pre-processing the data for AFPGA. AFPGA can be programmed for diffident applications by the dedicated configuration tools.

The physical signal processing function is consists of four parts: analogue output module, analogue input module, digital output module and digital input module. All modules have self-diagnose function. The self-diagnose scope coverage all of the safety critical function, such as availability of channels, power supply, data communication, FPGA, EEPROM, Watchdog and cycle run time. The information of self-diagnose can be sent to HMI, LED or diagnose relay.

The performance of analogue module is as follows: AI (Analog Input) and AO (Analog Output) modules have 8 channels; 4–20 mA input, diagnose scope is 0–25 mA and can be configured trigger in different alarming value; accuracy is better than 99.9% F.S.@25 °C; stability is better than 99.9% F.S.@25 °C; the accuracy drift is less than 0.1% F.S.@25 °C in 18 month; temperature coefficient 50 ppm/ °C; isolation voltage is 1000 VAC@1 min-@5 mA between channel and system ground; over-current protection of ±30 mA and over-voltage protection of ±60 V.

The performance of digital module is as follows: DI (Digital Input) and DO (Digital Output) modules have 16 channels; The digital input signal type is dry contact, support 24 VDC or 48 VDC input; All channels have ability of over-voltage protection of ±30 V/ ±60 V when inquiry voltage is 24 VDC/48 VDC; The digital output signal is 0–3 V in logic "0" and 22–24 V in logic "1", each channel supports 25 mA load, and ±30 mA over-current protection.

Communication function: data exchange between different stations or between station to HMI.

Auxiliary function complete signal connection between modules, power supply interface.

2.2 Mechanical Design

Cabinet and chassis design meet the requirements of 19 inch standard structure, Fig. 2 shows that cabinets afford 40U installation space. The material of frame is 2–3 mm steel to meet the requirements of seismic class I.

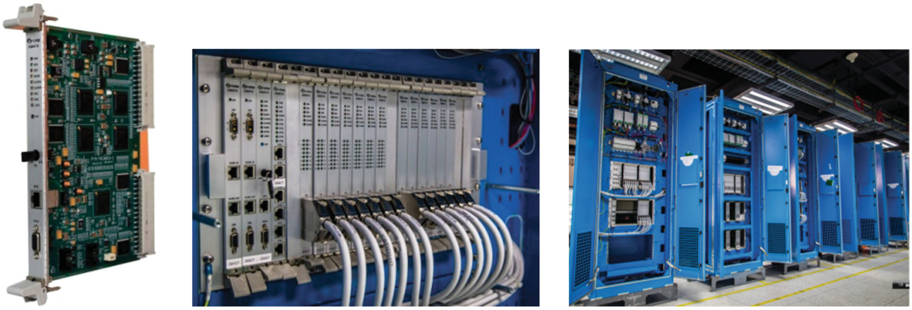


Fig. 2. FitRel platform board, cabinet and chassis

2.3 Function Safety Design

The FitRel platform's safety structure is 2oo3. The main indexes are listed below [6]: HFT = 1; safety target is SIL3; SFF = 90%–99%; DC $\geq$ 90%; $PFD = 1.5 \times 10^{-4}$; $PFH < 1.5 \times 10^{-8}/\mathrm{h}$. FitRel platform completes high self-diagnose coverage to meet the 2oo3 system architecture and the rules are as follows: Danger failure which affects safety function shall be efficiently controlled; self-diagnose design shall not affect the basic safety function; the self-diagnose circuit should be simple, low failure rate and high reliability. Table 1 shows the diagnose requirement and measure.

Table 1. FitRel platform diagnose requirement and measure

Component	Function block	Diagnose measure	DC
FPGA	Clock	Independent time base and time window	H 99%
	Data integrity	CRC32/64	H 99%
	Communication interface	Safety protocol	H 99%
	Application logic block	Built-in self test	M 90%
Clock	Quartz, Oscillator, PLL	WDT of independent time base and time window	H 99%
Digital input		Redundant input signal compare	M 90%
Digital output		Read back & dynamic self-test	M 90%
Analogue input		Dynamic self-test	M 90%
Power supply	Over-voltage Under-voltage	Voltage monitor and compare	H 99%

Safety communication		Transmission errors;
		Repetitions;
		Deletion;
		Insertion;
		Re-sequencing;
		Corruption;
		Delay;
		Masquerade.
			H
			99%

2.4 HPD Design

The life-cycle described in Fig. 3 shows the development life-cycle of HPD. The approach proposed to development is based on the traditional “V cycle” model.

The requirement specification shall include: (a) the functions requirements; (b) state machine and its transition conditions requirements, including power-on and initialization; (c) interactions and interfaces requirements, including the roles, protocols, types, data formats, bit numbering, ranges and constraints of inputs and outputs; (d) maintenance requirements, such as parameters which can be modified manually during operation; (e) performance requirements, in particular response time; (f) environment requirements, e.g. electrical and temporal characteristics of inputs-outputs, power supplies, specific profiles during power-on, cooling.

The objective of the design phase is to develop a detailed description of the processing to be performed by the FPGA circuit (much like software source codes describe the processing to be performed by a microprocessor). The most common detailed design representation used is the RTL. At this level, FPGA functions are

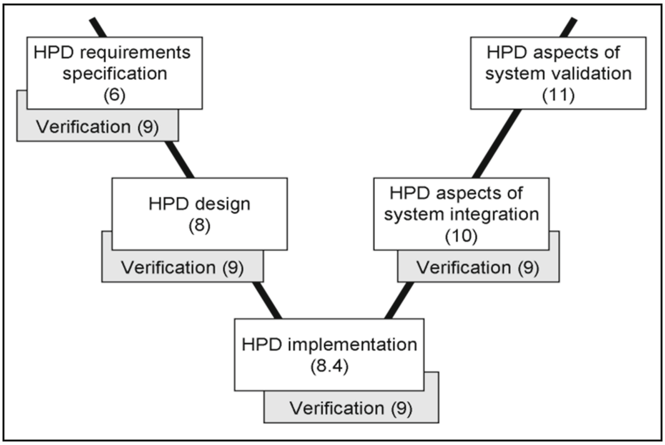

HPD requirements specification (6)
Verification (9)
HPD design (8)
Verification (9)
HPD implementation (8.4)
Verification (9)
HPD aspects of system integration (10)
Verification (9)
HPD aspects of system validation (11)

Fig. 3. HPD life cycle

described in terms of signal flows or data transfers between registers (flip-flops or other memory elements) and operations performed on those signals. The following guidance should be considered when designing the overall circuit: (a) Use a synchronous design approach wherever possible – this makes the design simpler and more deterministic, and it facilitates verification and testing. (b) Use a modular design – use of smaller, simpler modules as opposed to one large, relatively complex design can ease the development burden, facilitate standardization and reuse of common functional designs, and facilitate testing and verification. (c) Consider segregating the primary functions on the circuit as well if they do not need to interact, such as maintenance function like transmitting diagnose information is segregated from the safety function, the signal is unidirectional from the safety to non-safety; (d) avoid use of complex native blocks that have a significant amount of unneeded functionality if the required function can be implemented with a simpler, less burdened custom-developed module, or a simpler pre-developed block. Take the algorithm blocks for example, FitRel platform supplies sufficient application algorithm blocks without any the third party IP, even the basic blocks like addition, multiplication, divisions, etc.

The implementation phase starts upon completion of the design phase. Implementation is usually divided into two main steps: synthesis and place and route. Both steps are normally supported by tools provided by the FPGA vendor. A Static Timing Analysis (STA) is performed and documented for worst and best cases to calculate the margins, taking into account the timing information provided by the technology libraries and all relevant design and implementation tools.

System integration phase includes assembling newly developed and pre-developed components in a whole system and adjustment of all components and connections.

In verification and validation phase for FPGA, simulation is usually performed. RTL simulation is especially suited to the detection of logical and other functional errors. The verification strategy can sometimes be based on the time honored ‘divide et impera’ (divide and conquer) principle, where the design is partitioned into smaller, simpler components, each having well defined interfaces and interactions (structural property) [7].

3 Application in ACPR1000 Project

FitRel platform is used to accomplish DAS to handle the software CCF of RPS which is processor-based in CPR1000 project. DAS aims to relieve the result of ATWS; relieve the probability of reactor core melting by CCF of RPS. The functions are as follows: Afford diverse automotive trigger signal and trigger the reactor trip and Engineering Safety Feature Actuation System (ESFAS) when NPP parameters exceed the setting values; Afford diverse manual trigger to the reactor trip and ESFAS); Afford diverse indication of specific NPP parameter.

DAS is defined 2oo2 structure to satisfy malfunction ratio specification and have the ability of maintenance on-line. The system includes level1 which is diversity activation cabinet (DAC) and level2 which is diversity HMI panel (DHP). FitRel platform fulfills the function of signal acquisition, automatic logic calculation and signal output installed in DAC. DAC includes 2 stations composed by 6 cabinets. Each station fulfills diverse automatic logic and trigger “half-logic”. Relay unit includes 2 relay cabinets and combine the DO signal from each “half-logic” to accomplish 2oo2 logic and send the calculation result to other system. Alarm station is installed in relay cabinet and fulfills the function of different kinds of alarm pre-handling which is sent to DHP. DHP is HMI interface which afford signal indication and manual handling function. The equipments installed in DHP include alarming lamp, display instrument, hardware manual and VDU. The performance values are as follows: input channel accuracy ≤0.1%, system response time ≤0.15 s, malfunction ratio ≤0.02/year, availability ≥99.99%, MTTR ≤4 h, MTBF ≥5 years, high coverage level self-diagnose, supporting hot-swap on running.

As the FPGA technology based digital I&C system is the first time to be applied in nuclear and power plants in China, we faced and solved lots of technical problems, especially the V&V problems and usability problems. We developed the graphical algorithm configuration tools based on FPGA technology, algorithm download technology based on Ethernet technology, and build FitRel simulation platform carried full validation and verification. In 2015, FitRel platform is successfully applied in Yangjiang Unit5 and Unit6.

4 Conclusion

Diversity Actuation System is applied in NPP I&C system to raise the probability of safety. FitRel platform-FPGA technology based, similar to relay technology based device, has intrinsic diversity to the microprocessor-based platform in architecture, design, human, software, etc. FitRel platform is creatively designed in architecture, mechanical, function safety and HPD (hardware description language programmed device), and the HDL design meets the requirements of IEC 62138 category B.

FitRel platform is the first FPGA-based digital I&C platform applied in NPP diversity actuation system in China. As its simplicity, reliability and usability, it is highly appreciated and praised by engineering design teams and owners. It is believed that the FPGA-based I&C platform will be widely applied in safety systems in future.

References

1. NUREG/CR-0800 BTP 7-19: Guidance for Evaluation of Diversity and Defence-in-Depth in Digital Computer-Based Instrumentation and Control Systems (1997)
2. NUREG/CR-6303: Method for Performing Diversity and Defence-in-Depth Analyses of Reactor Protection System (1994)
3. NUREG/CR-7007: Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems (2010)
4. NUREG/CR-6992: Instrumentation and Controls in Nuclear Power Plants: An Emerging Technologies Update (2009)
5. IEC62138: Nuclear power plants -Instrumentation and control important for safety -Software aspects for computer-based systems performing category B or C functions (2004)
6. IEC61508: Functional safety of electrical/electronic/programmable electronic safety-related systems (2011)
7. IAEA Nuclear Energy Series NO NP-T-3.17: Application of Field Programmable Gate Arrays in Instrumentation and Control Systems of Nuclear Power Plants (2016)

Overview of Development of NPP Advanced Main Control Room Console

Qing-Jun Meng, Zhi-Bin Liu(✉), and Yong-Bin Sun

China Techenergy Co. Ltd., 5 Yongfeng Road, Haidian District, Beijing 100094, China
siluhuayu315404@126.com

Abstract. The development of advanced Main Control Room (MCR) console of the Nuclear Power Plant (NPP) in the world is overviewed, and the brief introduction of corresponding techniques used in the various NPP MCR consoles is given. The design input and output of procedure and demands, methods of the design research of advanced main control room are issued in detail, especially for the MCR console, which is to be incorporated in the new generation of Chinese nuclear power plant with computerized reactor, control system, protection system, Cathode Ray Tube (CRT) display and soft operation. The results of the comparison of MCR technology can provide a reference for the MCR console development trend.

Keywords: Main control room console · Nuclear power plant · Advanced digital instrument control

1 Introduction

The 1979 Loss Of Feed Water (LOFW) accident at the US Pressurized Water Reactor (PWR) Three Mile Island (TMI) unit 2 and Chernobyl NPP accident consequences in 1986 offered many lessons about improving nuclear power plant control room Man-Machine Interface (MMI). Post-TMI concerns include reducing operator information overload, improving the human factors of annunciator systems, and monitoring of safety-related information and Engineered Safety Feature (ESF) status.In order to further improve the safety and availability of nuclear power plants, international and domestic have developed and published of a series of new regulations, standards; US and European nuclear power user requirements documents (United States Requirement Documentation (URD) and Europe User Requirement (EUR)), etc., which is an urgent need during the nuclear power plant construction.The use of digital instrumentation and control technology based on the advanced control room console to replace the traditional space operational conceptual, analogue technology-based conventional control room [1–4].

With the rapid development of computer hardware and software technology and the research and implementation of human interface engineering principles, the man-machine interface is further improved. Under the conditions, the NPP designers develop and design an advanced control room based on all-digital control, protection, display

Y. Xu et al. (eds.), *Nuclear Power Plants: Innovative Technologies for Instrumentation and Control Systems*, Lecture Notes in Electrical Engineering 455,
https://doi.org/10.1007/978-981-10-7416-5_24

and operation. This not only improves the reliability, availability and safety of the nuclear power system, but also reduces the operator's work intensity and mental burden due to the fundamental change of the man-machine interface, reduces the probability of judgment and operation error. The main control room console which plays a very important role in the safe and reliable operation of NPP is as the most important control sites. According to the definition of NUREG-0700, the Advanced Control Room (ACR) of a NPP is a control room based on digital technology and a video display unit (VDU) as the main means of human-computer interaction. The development of nuclear power plant control room is divided into three stages: the traditional control room consoles is based on analog plus "hybrid technology" combined with digital technology from 1950s to 1990s [5]; at the end of the 20th century, with the digital technology has been fully applied to the nuclear power plant control room, appeared the French N4, South Korea APR1400, the United States GE ABWR and China Lingao II nuclear power plant as the representative of advanced control room. The Unit 1&2 of Lingao Phase II is a full-featured operator workstation based on plant computer information and control system (KIC) as the main control means, supplemented by conventional technology Back-Up Panel (BUP) as a response to KIC failure of the diversified back-up. While the advanced MCR consoles of AP1000, European pressurized reactor (EPR) and China's HPR1000 reactors combine with the human factor engineering to make the MCR to get a higher level.

2 The Principle and Requirement of Nuclear Power Plant MCR Consoles

In order to reduce the operator's potential operational errors [6], and the mental burden of the operator in the event of an accident, even further to improve the man-machine interface, during the design of NPP control room, a systematic, standardized, mature method should be used to carry out the functional design of the control room and verification. All these follow the following design principles:

- Safe operation guidelines;
- Availability principles;
- Diversity and defense in depth.

The implementation process follows the following HFE design procedures (Fig. 1): Fig. 1 is the flow chart main control room design procedure. During the design process, human factor engineering is complied with throughout the whole process. The green rectangular box is the MCR console position. Combining the projects experience the input and output of NPP MCR console is given.

From the development technology the NPP MCR console design is divided into traditional and digital technology.

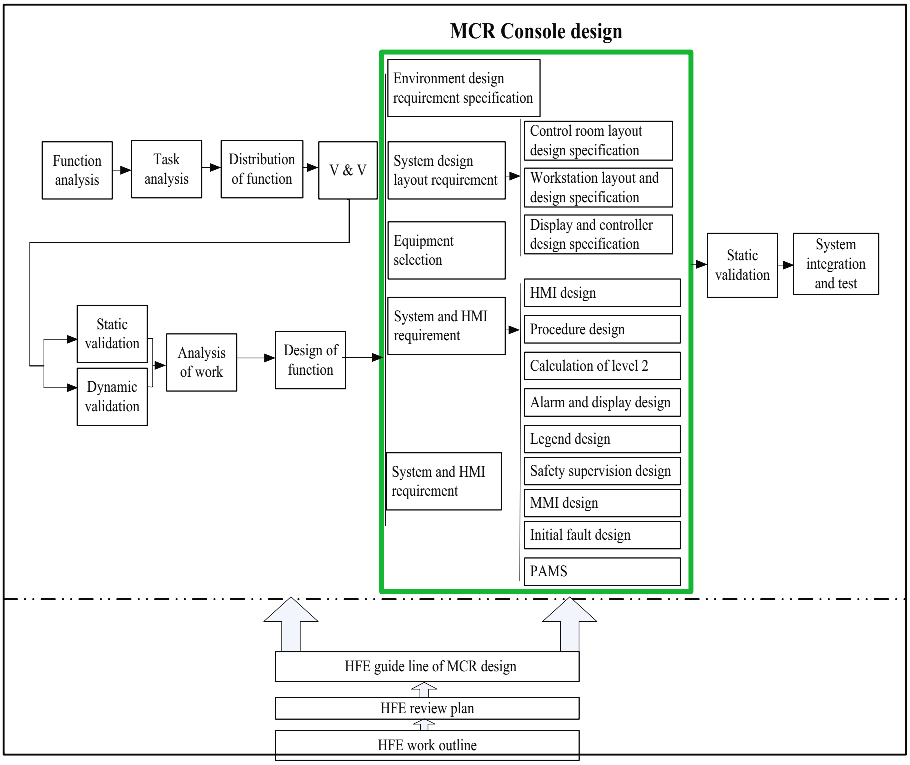

MCR Console design
Function analysis
Task analysis
Distribution of function
V & V
Static validation
Dynamic validation
Analysis of work
Design of function
Environment design requirement specification
System design layout requirement
Equipment selection
System and HMI requirement
System and HMI requirement
Control room layout design specification
Workstation layout and design specification
Display and controller design specification
HMI design
Procedure design
Calculation of level 2
Alarm and display design
Legend design
Safety supervision design
MMI design
Initial fault design
PAMS
Static validation
System integration and test
HFE guide line of MCR design
HFE review plan
HFE work outline

Fig. 1. Flow chart of main control room design

3 The Traditional MCR Console of NPP

The MCR used in the 1960s and 1990s uses a large number of hard-wired recorders, pointer meters, rotary switch, and push-button switches (see Fig. 2). In order to allow the operator to obtain more information, more than 20 m of the control panel is placed in the

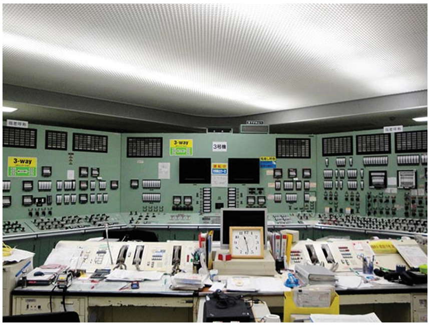


Fig. 2. Chernobyl NPP MCR

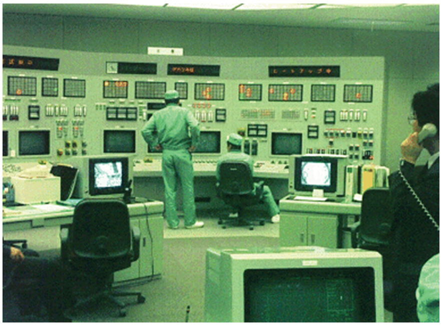


Fig. 3. Japan NPP MCR

control room. The control panel is covered with various monitoring instruments, alarm lights and alarm window. In the event of an accident, the operator needs to move a long distance to monitor and control the manipulation under great psychological pressure.

In the 1980s, cathode-ray tube (CRT) and computer technology were widely used in the human machine interface of MCR. The traditional control room consoles using CRT in auxiliary information display of MCR layout to reduce the burden of the operator. The traditional control room still retains the traditional control panel, but adds a plant display system (PDS) and more use of the CRT display (see Fig. 3). In the event of an accident, the PDS & CRT provides a centralized information display for the operator with the primary goal of "timely and accurate assessment of the status of the nuclear power plant" after the accident. The traditional NPP control room using the analog panel with digital control system combined, which is also known as semi-digital or the hybrid-type MCR.

4 The Digital MCR Consoles of NPP (also Called Advanced MCR Consoles)

With the rapid development of computer and network technology and the continuous accumulation of experience in nuclear power plant operation, the digital of NPP MCR console uses digital instrumentation system instead of the traditional analog instrument console system. Reactor Trip System (RTS) and Engineered Safety Features Actuation System (ESFAS) are included in the full-digital system includes. The operator uses the Plant Overview Panel (POP) system and the Video Display Unit (VDU) to obtain information and control the power plant using computer soft control.

The advanced main control rooms console system of nuclear power plants: N4 (International EDF), APWR-1000 (US Westinghouse, Mitsubishi Corporation), ABWR (American GE, Japan Toshiba and Hitachi), 80+ (ABB CE) have been completed verification. South Korea through the introduction of technology also develop a standard PWR, whose advanced main control room console (similar to the system 80+) design and verification has been completed and used in NPP. The MCRs console of AP1000, EPR and China's HPR1000 reactor combined with human factor, to avoid the occurrence of common mode failure, maintenance and diagnosis have been improved and completed to verify.

4.1 N4 NPP Advanced MCR Consoles

In the history of the development of nuclear power self-created, the French EDF is a pioneer. After the accident in Three Miles Island, they took the lead in using the digital protection system SPIN-1 in the waste heat removal system of P4 1.3 million kW nuclear power plants, which accumulated engineering experience for the realization of all digital protection and control. In the early 80s, EDF started N4 145 million kW main control room design and development. The digital-based advanced main control room was officially put into use in 1996. Despite the constraints of the computer hardware and software technology and the conservative nature of nuclear power, the French power company has creatively developed the prototype of the advanced control room, and verified the operation with the simulator. This computerized control room not only responds to the operator's control commands, but also enables fault diagnosis, alarm classification, and provides the operator with appropriate operating procedures.

4.2 APWR Advanced MCR Consoles

US Westinghouse APWR advanced MCR console is almost consistent with Mitsubishi's APWR advanced main control room console from the overall design ideas. Westinghouse is the founder of the PWR nuclear power plant, whose technology has been at the forefront of the world in a variety of nuclear designs, and has a long time since started the design of advanced PWR nuclear power plants and passive nuclear power plants. But due to the lack of new comprehensive nuclear power plant project, nearly 20 years has been only committed to the local nuclear power plant system transformation. So Westinghouse only completed the prototype verification. Mitsubishi Corporation employed the United States Westinghouse company's system design technology, from the early 90s began the principle of prototype and then the development of engineering prototype. At present, the diagnosis system has been completed, the intelligent alarm system and the operator support system development, the design function verification and validation, the operation procedure verification, has completely finished the integrated main control room upgrading.

The main components of the APWR advanced main control room are as follows:

- POP;
- Console;
- On the console, there are 1E TFT, normal operation CRT, etc.).

4.3 ABWR Advanced MCR Consoles

US GE with Japan's Toshiba, Hitachi jointly developed and built the advanced boiling water reactor and the corresponding advanced control room console, and in 1996 put into commercial operation. Its main control room design pattern, the display is basically the same with the Mitsubishi. The same as the large-screen information display, the same 1E-class TFT security display, display control operator; software development tools are designed for the logic of the POL language, application development is simple, easy to verify, reduce the software on the comprehensive verification and validation the time spent.

The main difference between ABWR and Mitsubishi APWR main control room console is that the former still use more physical alarm windows (arranged in the top of the large screen display), the alarm system classification is also lower than the latter level.

4.4 ABB-CE Corporation System 80+ Consoles

Based on the development of system 80, ABB-CE developed a fully digital system 80+ advanced main control room console system following the computer technology. The main control room console design and prototype has been approval by the NRC.

The MCR console contains the equipment and systems as follows;

- Distributed digital Indication and Alarm System (DIAS);
- Operator control panel, console;
- The main control room is equipped with a main console, safety related operation and auxiliary operation panel, through the control switch or system operator components to perform control actions;
- POP;
- Data Processing System (DPS)

4.5 SIZEWELL B Advanced MCR Consoles

SIZEWELL B is the UK's first PWR nuclear power plant, and earlier (in 1992) fully integrated with advanced control and protection systems. Due to the design and the supplier's changes and the design of the conservative psychological and technical reserves, although Westinghouse provides advanced integrated protection system PPS, integrated control system HICS and centralized data display processing system DCS, but the whole MCR of the design is conservative. The MCR with more control panel, console, retains a variety of digital operation of the display and control equipment, but in the console set up to 23 sets of larger size CRT monitor, used to provide the console system status displayed. So the appearance of the control room is almost the same with analog control room companied with CRT. In addition, the power plant also set up an independent SPS system to meet the requirements of the core logic relay protection system SPS and as a back-up of PPS.

4.6 Korea MCR Consoles of Standard Nuclear Power

The APR1400 MCR console (Fig. 4) which is based on the ABB CE system 80+ is distinguished from Korea Standard Nuclear Power (KSNP) I&C designs by employing fully-digitalized systems and data communications, and primarily computer-based Human Machine Interfaces (MMI). APR1400 MMI advanced design features includes:

- A control room layout with compact workstations;
- A large central display panel;
- A safety console with qualified information and control to perform safe shutdown operation in case of total workstation failure;

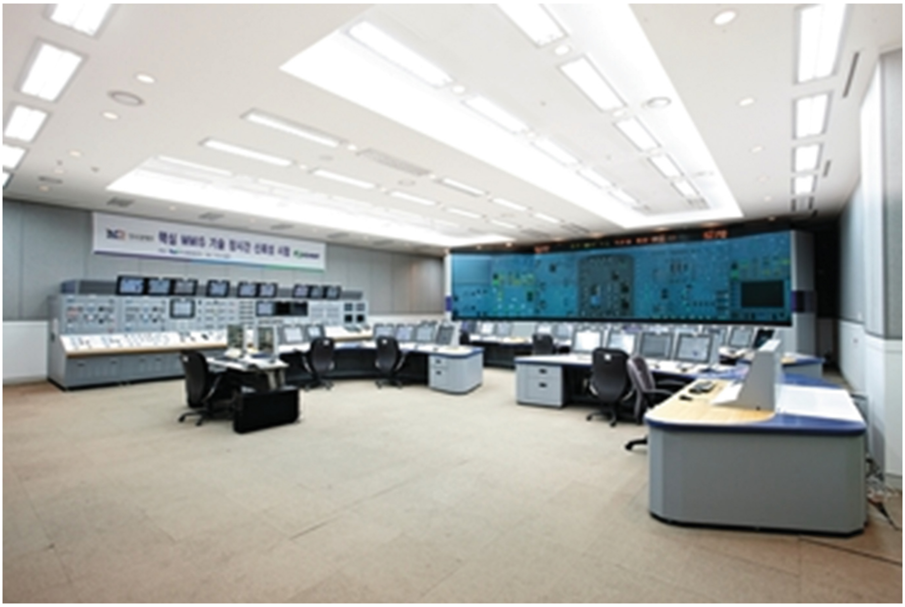


Fig. 4. Korea prototype APR1400 NPP MCR

In the center of the control room are redundant compact workstations. These redundant workstations make plant information, control and procedures available to all of the operators. During dynamic simulations of emergency operations with real KHNP crews for HFE evaluations, there were cases when diagnosis errors by the control room supervisor were detected by another operator. The additional workstations have made a significant improvement in human reliability possible.

4.7 China Advanced MCR Consoles

Lingao II nuclear power plant MCR console is based on KIC full-function operator workstation, supplemented by conventional technology based on the KIC/BUP failure mode as a response to the diverse backup. The configuration of the digital main control room console mainly includes two computerized operator workstations, emergency operation devices, large screen, backup panel, fire detection and fire protection panel, unit workstation and safe engineer workstation. Among them, two computerized operator workstation, unit workstation and safe engineer workstation are four redundant computer workstations, which provide the power station computer information and control system terminal. For the HPR1000 third generation MCR console (Fig. 5), AP1000 MCR console (Fig. 6) and China Taishan EPR MCR console (Fig. 7) are the latest advanced power plant MCR layout, which is an integrated full-digital, HFE system to meet the design principles.

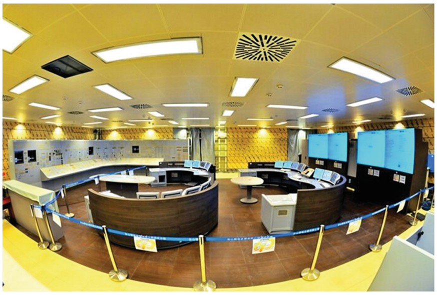


Fig. 5. HPR1000 prototype MCR

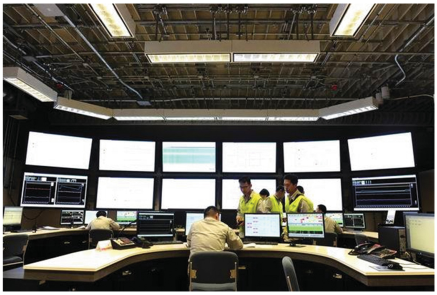


Fig. 6. Haiyang AP1000 MCR

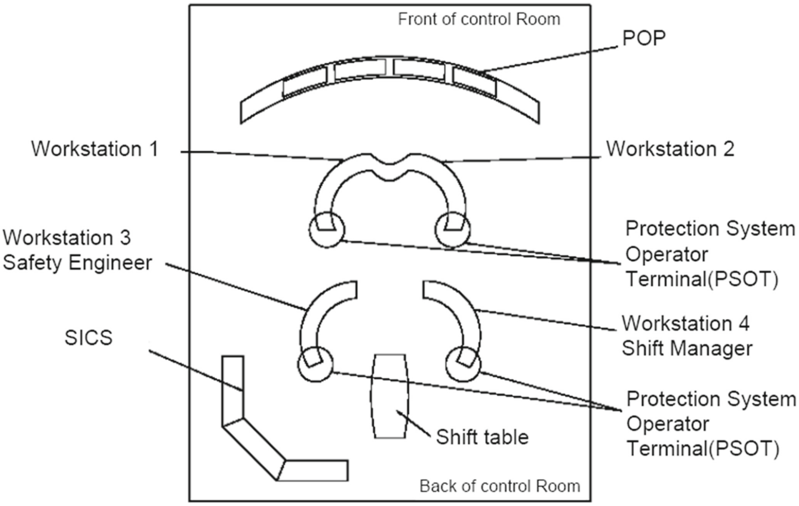

Front of control Room
POP
Workstation 1
Workstation 2
Protection System Operator Terminal(PSOT)
Workstation 3 Safety Engineer
SICS
Workstation 4 Shift Manager
Protection System Operator Terminal(PSOT)
Shift table
Back of control Room

Fig. 7. UK EPR MCR layout

5 Comparison of Traditional and Digital MCR Consoles

From the traditional and advanced development NPP MCR consoles we can see three workstations in front with one behind (China CPR1000 Units) or two workstations in front with two behind (UK EPR MCR layout), equipped with BUP and safety related operation and auxiliary operation panels on both sides to realize alarm and display.

First of all, for the content and method of information display of the nuclear power plant digital control room console system, the operator is mainly through the computer monitor and the central screen directly to access to system information to complete the system monitoring and control tasks. Computer workstations dominate data processing capabilities, but also bring human factor problem. The display screen of the digital control room carries a number of human machine interfaces, but there is not enough space on the screen to display them continuously, and they are seen as virtual workspaces. In addition, the instrument control system display screen may contain thousands of layers of complex interactive interface, in order to effectively complete the power plant monitoring and control tasks, in addition to monitoring, the operator also does status assessment and other conventional tasks, but also in the workstation to complete the interface management tasks.

Second, from the judgment or action response to the displayed information, since the control equipment and the display equipment of the traditional main control room of the nuclear power plant are arranged in a specific position as required, the staff usually needs to travel around the main control room to realize power plant monitoring. During the execution of the task, the operator makes a judgment or action response to the displayed information according to his own experience and knowledge level. In the digital control room of the nuclear power plant, the simulated system running state is quantified as the system operating parameters. Parameters can be visually displayed on the computer screen on the software interface, the operator only needs to operate the central computer, it is easy to make the appropriate action response on a different digital information, equipped with the alarm system to remind the staff to deal with nuclear power plant operation,when the abnormal situation appeared to make sure that the nuclear power plant is in a safe, stable and efficient operation of the state. With the development of the main control room, human factor engineering is tightly applied to the design of the main control room, which is fully complied with the requirements of human factor at the whole design process of main control room.

The comparison between traditional MCR console and advanced MCR console is as follows (Table 1):

From the technical development trend, we can see that except to comply with design principles of NPP, digitalized, diversification, human factors and ergonomics will be the technical center of future, but in order to minimize the mistakes of operator, minimalized, friendly MCR consoles will be needed more to let operator feel comfortable.

Table 1. The comparisons of NPP MCR HMI

Category		Traditional MCR console	Advanced MCR console
Information display	Display medium	Instrument display, LED indicator, CRT et al.	Table, graph, status indicator et al.
	Expression form	Single	Diversification
	Information capacity	Little	More
	Information redundant	Single with little	More
	Method of get information	Mainly upon instrumentation or indicator with CRT	Directly viewing CRT or changeover information between windows
	Information layout method	Inconvenience to modify	Change or switchover at anytime
Control operation	Control method	Control (switch, button)	Software control
	Operation method	Monitoring at console with CRT monitoring	Operation on computer
	Interface operation	Operation at designated location and continues in space	No space limitation, plus interface management task
Human factor engineering	–	Just CRT monitoring	Considering equipment, environment, temperature, people feeling

References

1. Zheng, M.G., Zhang, Q.S., Xu, J.J., et al.: The development of NPP advanced main control room and self-design research objectives. Chin. J. Nucl. Sci. Eng. **20**(4), 207–303 (2000)
2. Zheng, M.G., Zhang, Q.S., Xu, J.J., et al.: Development of NPP advanced main control room. J. Shanghai Tiedao Univ. **21**(6), 99–104 (2000)
3. Sun, Y.B., Jiang, X.H.: Layout design of advanced control room of pressurized water reactor NPP. Nucl. Power Eng. **29**(3), 73–77 (2008)
4. Zheng, M.G., Xu, J.J., Ning, Z.H., et al.: Function analysis and function assignment of NPP advanced main control room. Nucl. Power Eng. **22**(2), 171 (2001)
5. International Electrotechnical Commission: IEC61227: Nuclear Power Plants Control Rooms Operator Controles. International Electrotechnical Commission, Geneva (1993)
6. Dai, L.C.: Analysis on human reliability of control room in semi – digital nuclear power plant. Atomic Press, Beijing (2012)

Implementation of V&V Tasks for Improving Nuclear I&C System Software Safety

Bao-Juan Yin[1], Jing Li[1], Ya-Qi Wang[1], Da-Hu Liu[1](✉),
and You-Yuan Li[2]

[1] Nuclear and Radiation Safety Center,
No. 54, HongLianNanCun, Haidian, Beijing, People's Republic of China
liudahu@chinansc.cn
[2] China Techenergy Co., Ltd.,
Building 5, Yongfeng Road, Haidian, Beijing, People's Republic of China

Abstract. As more computer-based instrumentation and control (I&C) systems are used in nuclear power plants (NPPs), software safety becomes more and more important for safe and reliable operation of NPPs. Based on the hidden nature of software itself, its safety needs to be guaranteed by being strictly verified and validated in the process of software development to eliminate the potential design faults. The tasks performed by verification and validation (V&V) personnel play an important role in improving safety of I&C system software used in NPPs. Three key V&V tasks including traceability analysis, hazard analysis and safety testing are highlighted; their relationship and implementation methods are discussed; the implementation methods can be applied or referenced in future software safety V&V and improving digital I&C system safety.

Keywords: V&V · I&C system · Software safety
Traceability analysis · Hazard analysis · Safety testing

1 Introduction

According to the life cycle of software, software development process can be divided into five stages [1] which are concept stage, requirements stage, design stage, implementation stage and testing stage; software [1] verification activities should cover all these stages to ensure realization of software safety. In the first four stages of software development process, software safety is verified by using selectable analysis techniques and analyzing all outputs of each stage to identify and evaluate all potential hazards; in testing stage, software safety is validated by thoroughly testing software itself, and final safety evaluation of software is performed.

As the outputs of prior stage are inputs of next stage during software development process, in order to better verification results of each stage and ensure the final software products meet requirements of the system, traceability analysis is needed in safety verification during software development process, and its results are used as the basis of application of other verification tasks. Traceability analysis is used to evaluate consistency of outputs of each development stage to system requirements [2]; hazard

Y. Xu et al. (eds.), *Nuclear Power Plants: Innovative Technologies for Instrumentation and Control Systems*, Lecture Notes in Electrical Engineering 455,
https://doi.org/10.1007/978-981-10-7416-5_25

analysis is used to identify and evaluate all potential hazards during realization of system requirements [3]; safety testing is used to validate if the final software products are safe enough; these three verification and validation (V&V) tasks are an organic whole for improving nuclear I&C system software safety, achieving different goals and complementing each other (Fig. 1).

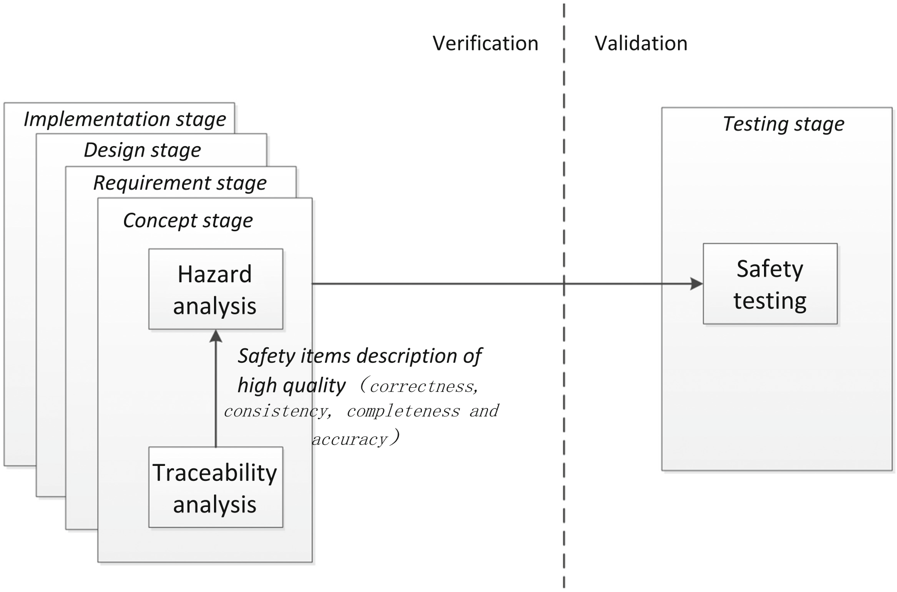


Fig. 1. Relationship of traceability analysis, hazard analysis and safety testing

2 Traceability Analysis

Meeting functional and nonfunctional I&C system requirements is the basis of software safety. Traceability analysis is one verification task which performs two-way traceable analysis between the outputs of one stage in software life cycle and that of its previous stage, and is process of ensuring all outputs of each latter stage could implement correctly the demands of software. Traceability analysis is a verification task that runs through the whole life cycle of software development in parallel with the software development task. Traceability analysis is implemented as follows:

(1) First of all, the tracking matrix of the product outputs in the previous stage and those in current stage of the life cycle should be established to establish the tracking relationship between them.

In order to facilitate tracking, software development documents and test documents should be prepared by using structured methods, supporting automation tools which are capable of handling all software development documents for large-scale tracking should be chosen, and tracking matrix concerning development documents should be associated with configuration management and change control, to ensure that any content changes reflect to the tracking matrix and lay foundation for other safety verification tasks.

(2) Secondly, correctness, consistency, completeness and accuracy [2] of the tracking contents should be analyzed, and complete tracing relationship between them in the contents should be established. It is verified that software completely realizes the needs of users, and no superfluous functions which are outside of user demand are achieved.

Traceability analysis is one basal task which can improve quality of analysis contents, ensure correctness, consistency, completeness and accuracy of safety items, facilitate performance of other analysis tasks, and form objective evidence of software development quality.

3 Hazard Analysis

Hazard analysis is one necessary task for SIL4 software required by IEEE 1012, but this standard only focuses on completeness of process and tasks, no operational guidance is provided. Annex D of IEEE 7-4.3.2 gives a variety of helpful information for hazard analysis. The purpose of hazard analysis is to identify and evaluate factors potentially devastating system; it focuses on system safety-critical functions, failure mechanism affecting implementation of these safety functions which may cause disastrous consequences, and prevention/control measures of these potential factors. After hazard analysis, each hazard item should be determined by the severity level of its impact, the probability of its occurrence [3], and the rating which reflects impact degree of this hazard once occurred. The assessment criteria for the severity and occurrence of the hazard items identified at different stages should be determined before performing hazard analysis.

3.1 Relationship Between Software Hazard Analysis and System Hazard Analysis

Hazard analysis is aimed at the whole I&C system and its safety. All components of the system, its surrounding environment and its external interfaces should be the object of hazard analysis [4]. As an important part of the system, software doesn't fail as time goes by; it fails at some time with specific trigging conditions due to design defects. Function failures of software may lead the system to hazard status and cause the system failure. So the purpose of software hazard analysis is to identify and evaluate software internal potential factors which may cause system fail, so as to ensure that developers can take timely measures to avoid the system hazard caused by software.

Consequently, system hazard analysis should be carried out before software hazard analysis, determine possible software factors which may cause system hazard, as the starting point of software hazard analysis. System hazard analysis needs to be completed in concept stage and by the person who is familiar with I&C application systems. Since then, software hazard analysis needs to be carried out to track the hazard items related to software identified in concept stage, and to ensure that these hazards are eliminated in the process of software design and implementation.

3.2 Software Hazard Analysis Technique

When initial hazard analysis is carried out, the systematic and structured analysis techniques should be selected for the comprehensive identification of hazard items of systems and software. The techniques, FTA [3] using top-down order and FMEA [3] using bottom-up order, are both suitable, one or both can be selected and put in practice.

The choice of whether to use software FTA technique or software FMEA technique should be according to the scale and characteristics of analyzed software and ensure that analyzed object could be completely organized from a perspective or a variety of combination of perspectives. Alternative perspectives include logical perspective, process perspective, physical perspective, development perspective and application perspective.

In addition, according to different features of software products of different stages, as well as software development and verification experience, abnormal conditions and events checklist could be established in advance as a supplement, to facilitate rapid positioning of potential hazard items. Checklist in Table 1 is suggested based on requirements from related standards [2–5] and software project experience.

The structural hazard analysis techniques can ensure hazard items can be fully identified as early as possible, and checklist analysis technique will take full advantage of existing experience, combination of these two types of analysis technique can identify hazards rapidly and comprehensively.

So it is suggested to use FTA and/or FMEA as the main analysis technique and checklist as complementarity.

3.2.1 Hazard Analysis in Software Development Process

Safety critical functions in NPP I&C systems include performing signal acquisition, data transmission, logic processing, control and display outputs, etc.

Hazard analysis in concept stage should cover the potential hazards brought by external factors and from the system itself for implementation above safety critical functions. This task includes identifying potential hazards in the system, assessing the severity and possibility of occurrence of each hazard, and identifying mitigation strategies for each hazard.

The requirements stage should determine software contribution to the system hazards, identify software key requirements related to system hazard items, and confirm whether processing, control or mitigation measures are exist in software for these hazards.

The hazard analysis in design stage and implementation stage should verify the logic and the relevant data elements to design and implement the key needs correctly and not introduce new hazards.

The hazard analysis in test stage should focus on if all identified hazards have been eliminated by proper measures and correct implementation, no new hazards been introduced.

Table 1. Suggested checklist

Stage	Checked items
Concept	(a) Functions related potential initial events of nuclear power plant; (b) Safety critical functions of the I&C system itself; (c) Running environment restrictions; (d) Potential failures caused by hardware; (e) Potential software failures caused by hardware failure; (f) Potential failures caused by operators.
Requirement	(a) Missing or inconsistent software functional execution sequence requirements; (b) Wrong requirements of mismatch of data structure and function; (c) Unreasonable demand about software execution time, I/O transmission rate, memory/storage space allocation and other aspects.
Design	(a) Logic error; (b) Data structure error; (c) Data usage and processing errors, including: data initialization, data access, data range, units and dimensions, etc. (d) Interface errors, including inconsistency between this software and other software, between this software and hardware; (e) Timing errors; (f) Extreme cases that is ignored; (g) Design contents not consistent with software requirements.
Implementation	(a) Logic error; (b) Data definition, usage and processing errors, including: data initialization, data access, data range, units and dimensions, etc. (c) Interface errors, including inconsistent parameter passing, data size, unit, byte order, bit sequence, etc. (d) Code coverage: It should be analyzed that 100% coverage cannot be achieved despite of execution of all test cases; (e) Whether actual software execution time, I/O transmission rate, memory/storage space allocation are satisfied with software requirements.
Testing	(a) Whether software safety critical functions are properly implemented; (b) Whether software performance meets system requirements; (c) Whether interface with other software operates as expected.

3.2.2 Hazard Analysis Procedure

With FTA technique and application perspective, the procedure in Fig. 2 is performed during each stage of software development process. Explanations are given for some nodes of this procedure.

(1) Determining system function module and data flow

If FTA does not exist, V&V staff should analyze the function module and data flow based on the requirements and design documents.

- Function module analysis: the function module should be identified and partitioned based on the requirements and design documents, module name and its function should be recorded.

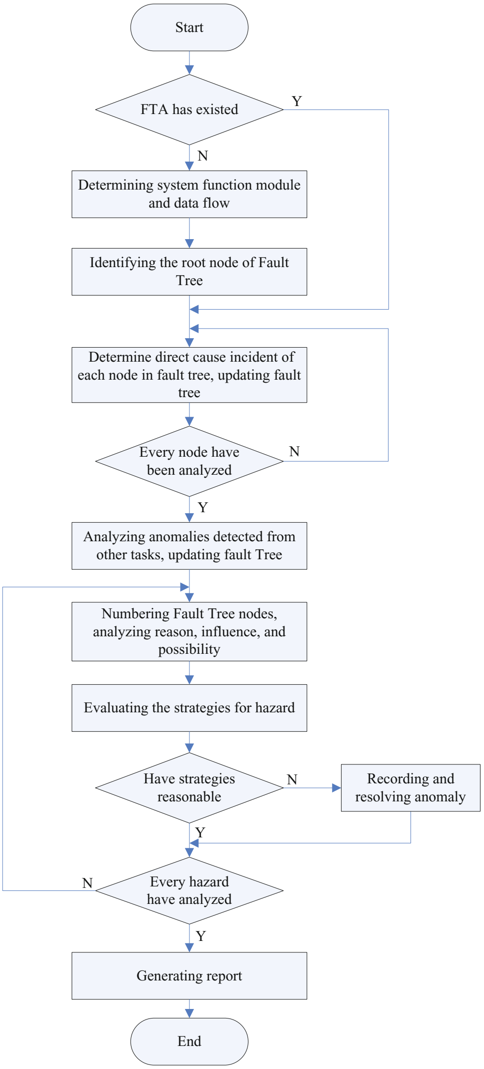

Start
FTA has existed
Y
N
Determining system function module and data flow
Identifying the root node of Fault Tree
Determine direct cause incident of each node in fault tree, updating fault tree
Every node have been analyzed
N
Y
Analyzing anomalies detected from other tasks, updating fault Tree
Numbering Fault Tree nodes, analyzing reason, influence, and possibility
Evaluating the strategies for hazard
Have strategies reasonable
N
Recording and resolving anomaly
Y
N
Every hazard have analyzed
Y
Generating report
End

Fig. 2. Hazard Analysis procedure using FTA technique

- Data flow analysis: with external entities as the inputs and outputs of data flow, input interfaces and output interfaces of data flow, data flow paths, data transferring between function modules, and its function should be recorded.

(2) Identifying the root node of Fault Tree

The root node of Fault Tree should be determined firstly. One unacceptable failure of system safety function should be selected as the root node of Fault Tree, and perhaps more than one Fault Tree are formed.

(3) Determine direct cause event of each node in fault tree, updating fault tree

Direct cause to all the nodes in a fault tree should be analyzed in turn. For each node, analyze its direct causes according to development documents, the depth of analysis should be consistent with detailed level of current development documents. If one analysis result is not identified in fault tree, add it as a new node.

(4) Numbering Fault Tree nodes, analyzing reason, influence, and possibility

Each fault Tree node shall have a unique number, and be recorded on the Fault Tree. Number shall accord to the following:

- Root node is the first level.
- The number of various level is separated with the ".".
- For node in the same level of Fault Tree, the serial number begins from 001.
- The number of each node shall include its father node number.

The reason, influence, and probability of fault for the bottom Fault Tree node should be analysed, the probability of its occurrence and severity level of its impact should be classified according to Table 2.

Table 2. Definition of probability and severity level of faults

Probability	Severity level			
	Fatal	Serious	General	Prompt
Frequent	1	1	2	3
Probable	1	1	2	3
Occasional	1	2	3	4
Infrequent	2	3	3	4
Impossible	3	3	3	4

4 Safety Testing

Through software hazard analysis, we can find the potential software hazard factors as early as possible, and provide the basis for the developer taking measures as soon as possible. Yet analysis is only a static verification means, which cannot replace software dynamic testing. Unless testing which is realized by software actual operation is performed, it cannot be confirmed whether software safety is finally realized.

Based on software safety analysis of the operational profile, the purpose of safety testing is to select and simulate operating environments which impact software safety to find out the potential faults, collect sufficient data for software safety assessment and confirm no defects affect actual software safe operation exist. Safety testing is different from routine function and performance testing whose purpose is to ensure that all software requirements are implemented, which should be a prerequisite for safety testing, and software safety testing is of no significance without achievement of software requirements.

Based on combination of software operational profile and test input coverage, completion of safety testing selects proper test cases. The selected test cases are more close to actual software safety requirement, more conducive to identification and elimination of major faults. In addition, software safety testing should be fully covered with a variety of input conditions and their combination, including the following: legal domain, illegal domain, boundary value and variable input value combination.

The procedure of safety testing is as follows:

(1) First of all, safety testing needs to start with determination of software safety critical functions, and to determine software safe operation profile. This step is the main difference between the safety testing and routine testing, and the content can refer to the result of hazard analysis process.
(2) Secondly, safety test cases which are able to fully cover various input conditions are designed.
(3) Then, according to test cases, test environments are set up, tests are executed, and testing process, all phenomenon and results are recorded in detail.
(4) Finally, based on analysis of the test results, software safety is evaluated.

5 Application

This above implementation method has been applied in one digital I&C System platform which is developed based on microprocessor, although this method is not restricted to any specific technology.

In this project, each design and test item in all documents including system specification, software specification, design description, test designs, test cases and test procedures, was assigned with one unique number which was used to build up the tracking relationship between each other in sequence of development activities. One commercial software tool, namely Rational RequisitePro, was used to output the final tracking matrix which can exhibit tracking connections directly and clearly. Based on these matrixes, V&V staff evaluated accuracy, consistency, completeness and accuracy of each tracking pair to conclude whether the documentation achieve traceability. If not, anomaly would be provided to producer of the documentation. Therefore, strictly speaking, traceability analysis is not software safety verification, yet it is one integral part of software safety verification, just because software safety verification is impossible without excellent traceability.

For design items which achieved traceability, hazard analysis was the next step of safety verification. For a digital I&C system platform, its hazards may come from any dissatisfaction of functional and nonfunctional requirements, so an assumed system which comprises all typical components of this platform was verified. FTA technique was applied in hazard analysis, and the top node of the fault tree was malfunction of this assumed system including unexpected trip and no-trip as required for reactor protection system from application perspective, going through the control and information flow all tree nodes were analyzed and all potential hazards were identified, the bottom-nodes of the fault tree were all possible failures of each typical component relevant to the top-node. The failure-safe criteria was applicable to hazard analysis, that is, all failures of each component were controlled and result in system safety finally. Abnormal conditions and events checklist of each stage were also applied, each component was checked by each check item. The hazards identified in previous stage were verified whether any control or mitigation measure was taken in current stage and whether any change in risk rating if occurred.

With the help of hazard analysis of each stage, all identified potential hazard factors with or without mitigation measures were considered in construction of safety testing operational profile and design of test cases. Possible input combinations were used in test cases to ensure no situation of breaking failure-safe criteria exists. The effect of measures and actual operational result were verified, satisfaction of safety requirements was validated.

6 Summaries

Software safety V&V tasks which cover traceability analysis, hazard analysis and safety testing are needed to verify the output results of different stages in the process of software development; they are mutual support between each other, so as to ensure that software safety is verified and validated comprehensively. Software safety V&V tasks have been applied and proved effective in one digital I&C system platform development project. They have played an important role in improving software safety.

With further application and more experience gained, more appropriate safety V&V techniques, such as probability safety analysis techniques, will be tried, and these three tasks will become more applicable for software V&V of digital I&C system used in nuclear power plants.

References

1. The Institute of Electrical and Electronics Engineers, Inc.: IEEE std 1012 IEEE Standard for Software Verification and Validation. The Institute of Electrical and Electronics Engineers, Inc., New York (2004)
2. International Electro Technical Commission: CEI/IEC 61508-7 Functional safety of electrical/electronic/programmable electronic safety-related systems. International Electro Technical Commission, Switzerland (2010)
3. The Institute of Electrical and Electronics Engineers, Inc.: IEEE std 7-4.3.2 IEEE Standard for Digital Computers in Safety System of Nuclear Power Generating Stations. The Institute of Electrical and Electronics Engineers, Inc., New York (2003)
4. The Institute of Electrical and Electronics Engineers, Inc.: IEEE std 1228 IEEE Standard for Software Safety Plan. The Institute of Electrical and Electronics Engineers, Inc., New York (1994)
5. International Electro Technical Commission: IEC 60880 Nuclear power plants-Instrumentation and control systems important to safety-Software aspects for computer-based systems performing category A functions. International Electro Technical Commission, Switzerland (2006)

Feasibility Analysis and Application Principle of Field Bus Technology in Nuclear Power Plant

Wei Sun(✉), Jin-Na Ma, Chu-Hao Xi, and Long-Qiang Zhang

State Key Laboratory of Nuclear Power Safety Monitoring Technology and Equipment,
China Nuclear Power Engineer Company, Shenzhen, Guangdong, China
sunw@cgnpc.com.cn

Abstract. Smart devices based on the microprocessor compare to the traditional equipment, which can improve the signal accuracy and self diagnosis of equipment. Field bus is used to provide industrial data bus for communication, which not only transfers the site process signal to the Digital Control System (DCS), but also transfers the self diagnostic information and maintenance data to the DCS. The adoption of field bus for Smart devices will change the traditional DCS structure, which means that the input and output modules will be embedded on the site. Field bus can enhance the ability of data acquisition and processing. In the nuclear power plant (NPP), considering the environment is different between the conventional industrial and high reliability requirements, the application of field bus should be carefully analyzed. Based on this, this article analyzes the feasibility of field bus technology in NPP, and gives the application principles, which lays a foundation for the actual project.

Keywords: NPP · DCS · Field bus · Smart device · Feasibility

1 Introduction

According to International Electro-technical Commission, field bus is “a digital multipoint communication data bus” between field devices (smart devices) and DCS installed in the industrial process control area.

According to the definition of the thermal power industrial standard terminology of automation, field bus control system (FCS) using the field bus technology to connect the sensor and mechanism with industrial network. This network is an open and standardized communication protocol which can achieve two-way data transmission and information exchange.

With the development of technology, FCS has become a main scheme in the control system design of large thermal power plant. High precision, remote diagnoses, less cable bridge and adsorption capacity are the main advantages of field bus. In such plant, the field equipment is mainly composed of electric actuators and motor controllers, and the digital signals account for more than 70% of the total I/O. So according to the development trend, the domestic 600 MW power plants gradually have applied the field bus, which has reached more than 40% (3000 sets of field bus devices for per project). And

Y. Xu et al. (eds.), *Nuclear Power Plants: Innovative Technologies for Instrumentation and Control Systems*, Lecture Notes in Electrical Engineering 455,
https://doi.org/10.1007/978-981-10-7416-5_26

then the ability of DCS supplier to provide field bus product becomes an important factor in the 600 MW power plant project.

In NPP, considering the factors of product maturity, application environment and reliability, the use of smart devices and field bus are currently only in some areas. Remote I/O technology uses the field bus network (CPU to IO module) to reduce the hardwire links, and chemical analysis transmitter uses microprocessor as smart devices to acquire the process information. In a specific NPP, ROSEMOUNT's 3051C series transmitter and Conventional Island (CI) are used for about 120 units. This use of instruments is only limited to the configuration of HART manipulator setting and debugging, not network of field bus. So the above applications are only in small area and primary application. Lack of network for field bus, the above application fails to dig the efficiency of smart devices to reduce the workload of power station maintenance people, and cannot acquire the fault diagnosis, calibration and maintenance information remotely. In summary, smart device applications have been started, but field bus technology has not been implemented widely in NPP.

2 Technical Advantages of Field Bus

Smart device is the foundation of large-scale application for field bus, which can put the compensation calculation, parameter modification, display, alarm and other functions scattered in the field. The operation, diagnosis and predictive maintenance of the equipment can be realized remotely by field bus. As a new digital control system, compared with the traditional control method, the technology advantages is as following [1].

2.1 Openness and Compatibility

Traditional control systems have their own closed system and architecture. When data transmission between different control systems, the gateway is used for protocol conversion, this restricts the information exchange among different equipments. Openness and Compatibility of field bus can connect the different equipments into one network which these equipments comply with same protocol. Different manufacturers which obey the same protocol can connect together with no difference.

2.2 Higher Precision

Traditional input/output modules use A/D conversion of input channel and D/A conversion of output channel. Field bus uses communication technology to transmit binary digital signals, this method can reduce the times of signal conversion and then enhance signal transmission accuracy, as shown below Fig. 1.

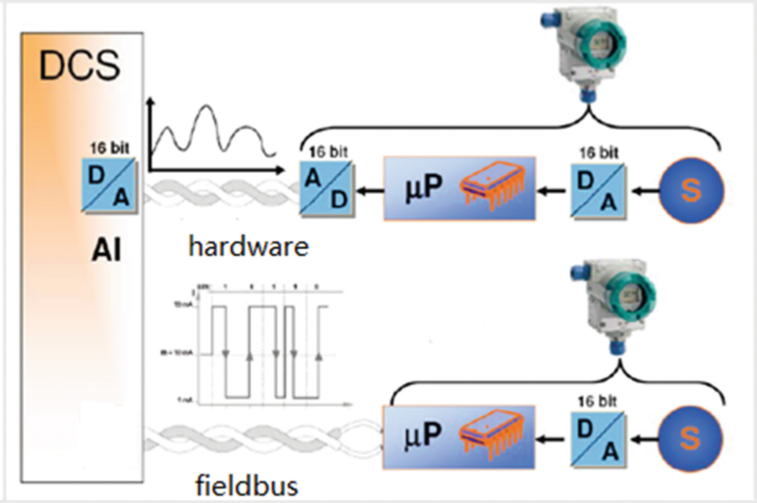


Fig. 1. Signal transmission of field bus

2.3 Higher Capacity of Data Transmission

Conventional signals are transmitted by hard wired, one signal can only represent one physical variable. When a complex process control loop is used, there are a large number of hard wired signals to be used, this induce huge quantity cables and increase complexity of cable trays. By contrast, Field bus data exchange is designed for communication to improve data transmission capability that a bus can transmit many kinds of data for different devices.

2.4 Remote and Predict Diagnosis for Equipment

In theory, all of the smart device information can be collected, including bit number, identification, measuring range, the latest verification records, the number of start and stop, etc. On this basis, field bus can remotely transfer the equipment information and check the operation health status in real time. In addition, field bus control system can store long-term operation data, provide data support of maintenance strategies (e.g., use of factors affecting wear advanced instructions, positioned through frequency tracking to collect stem reciprocating action times and other data, such as with a built-in odometer, thus to predict the decline in performance, due to the increase of seal friction so as to provide support for the operation and maintenance).

2.5 Less Cost of Installation and Operation

Compared to traditional equipment, the price of smart device has increased by 1/3. By contrast, from long-term of operation and maintenance, smart device can enhance self diagnosis and has fast troubleshooting ability. Finally, it can reduce the maintenance workload to save cost. In addition, due to the standardization of field bus it also has the advantages of simple design, flexibility, easy reconfiguration, and so on. Integrating all factors of above, it can effectively reduce the cost during the whole life of NPP.

In the installation phase, cable installation is a simple work that a cable can connect multiple devices and thus save cable installation quantity. Meanwhile, cable terminals, slot box, tray consumption and workload are greatly reduced. In the later stage of engineering, when add a new field control equipment, there is no need to add a new cable and only connect to the original cable nearby, thus this can save investment and reduce the workload for design and installation, as shown below Fig. 2.

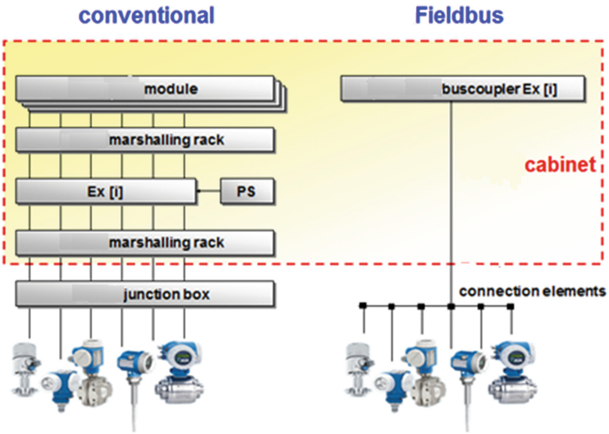


Fig. 2. Field bus link structure

3 Risk of Field Bus and Countermeasures

3.1 Signal Concentrated

Potential risk: since a plurality of sensors and actuators are mounted on the same network, once the network fails, it will lose control of all devices on this network [2].

Response measures: dual-network redundancy configuration is used to meet the requirements of high reliability. Secondly, important signals are not assigned to one single network segment. Finally, the hardware and software should be qualified if necessary. In NPP, RCC-E and IEC61000 are qualification standards and requirements.

3.2 Higher Requirement for Construction and Installation

Potential risks: the field bus is used to control the multi site equipment and collect information, field devices such as power cables, welding, intercom, telephone and lighting power supply can produce signal interference. Thus, mounting position of the bus control box is too close to frequency converter will be interfered. So higher requirements have been put forward for the design and construction of cables [2].

Response measures: the construction and installation should comply with regulations, standards of the field bus. The installation technical requirements of communication cable and grounding should apply design principle, such as different cable lay in separate bridge, communication cable and power cable are avoided to lay parallel. When the cable spacing is not enough, metal cable box should be used. If necessary, optical fiber transmission technology is also a good manner to overcome the interference.

3.3 More Difficult in Initial Debugging

Potential risks: field bus is a new technology in NPP. Debugging requires higher technology, especially communication technology, so in the early stages of engineering and debugging there will encounter difficulties [3].

Response measures: all parties in project should strengthen the technical reserves and extensive exchanges for field bus. Engineering and technical personnel should be trained, accumulate the understanding of field bus, fully learn from the mature debugging experience of thermal power plants.

3.4 Poor Resistance to Radiation

Potential risks: smart device is mainly based on microprocessors for information acquisition, processing and communication. Practice has been proved that the ability of microprocessor devices to resist radiation is poor, so smart device of field bus cannot be used in the containment of NPP.

Response measures: in combination with the current product status, the smart device should be avoided in the radiation area. In a long-term, designers should consider the qualification requirements of application in radiation area of NPP. On this basis, designers actively contact with the manufacturers to take joint research radiation resistance smart device.

3.5 Transmission Time of Field Bus Control

Potential risks: the field bus transmits signals by communication, so the time is delay compared to hard wired signal.

Response measures: For signals which have strict requirements for transmission time, they can be transmitted by hard wired.

4 Nuclear Power Plant Field Bus and Smart Transmitter Application Principle

A typical overall architecture of the field bus in NPP is shown in Fig. 3. The application of smart devices and field bus should be considered to meet the requirements of function, performance requirements, environmental conditions, location and installation/wiring, equipment qualification, operation, maintenance, cost, schedule and interface with other system. According to the characteristics of NPP, field bus control system applications need to be considered as following [4].

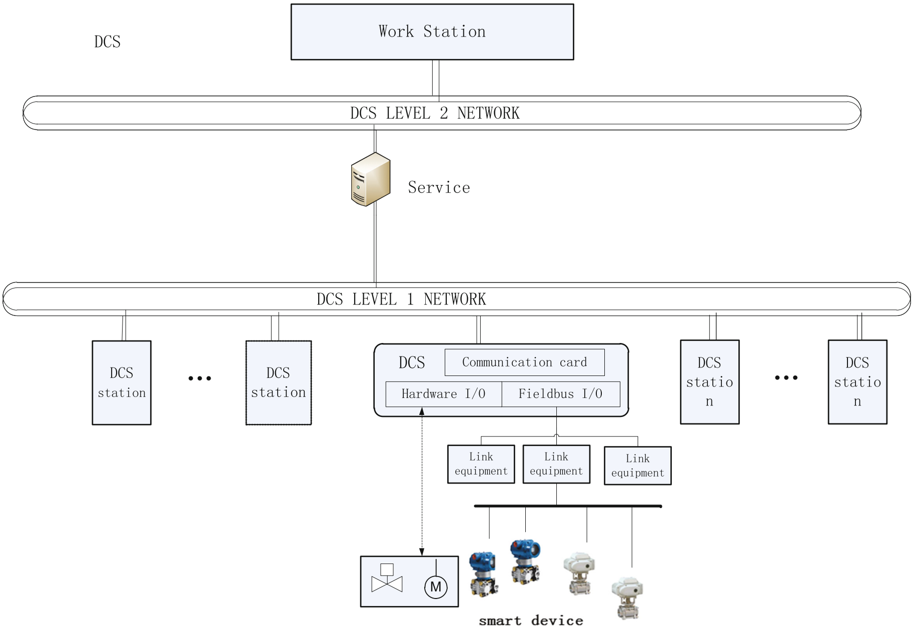


Fig. 3. Typical structure

4.1 Environmental Restrictions

The application of FCS should be based on the location of NPP, which can be divided into nuclear auxiliary building, nuclear fuel building, steam turbine building, and electrical building. Environmental conditions (e.g. temperature, humidity, pressure, etc.) includes:

- Normal environmental conditions;
- Normal and accident environmental conditions outside containment;
- Normal and accident environmental conditions inside containment.

Irradiation is in the inside and outside of the containment, so if the FCS is used in these areas, and the equipment irradiation shall be carried out.

4.2 Operation and Protection Requirements

Considering functional importance, signal distribution requirement the following systems or equipment should be used in conventional DCS rather than FCS (hard wired connection):

- Systems that have a significant impact on safety of reactor and turbine;
- Important control loops, such as nuclear steam supply systems;
- 6 kV motor control;
- Switch signals, including pressure switches, level switches, temperature switches and so on.

For redundant signals that have less impact to the equipment and system can be mixed for field bus and hard wired, this can enhance the diversity of signal.

4.3 System Performance

For signals which have strictly requirements for transmission time, they should be transmitted by hard wired rather than FCS. Considering to reduce the D/A and A/D transfer of data transmission, the transmission precision of field bus is higher to the traditional instrument.

4.4 Installation Requirements

It should follow the DL/T 1212 "guidelines for installation technology of field bus in thermal power plant", including the technical requirements of communication cable/optical fiber and the grounding installation. If site conditions do not meet the following requirements, it should be avoid to use FCS:

- Field bus should be equipped to separate bridge and the communication cable need protect by metal cover plate in complex electromagnetic environment;
- Communication cable and power cable lay in parallel at least more than 200 mm distance. When the distance is not enough, they should be separated by a metal cover plate.

4.5 Equipment Qualification

According to the importance of its performed safety functions, the corresponding equipment qualification procedures such as IEC requirements should be implemented. The key qualification items and the minimum qualification grade are shown in the following Table 1. In actual implementation, the test items can be increased or the test grade increased according to the electromagnetic environment of the equipment.

Table 1. Electromagnetic compatibility test

EMC test project	Test criteria	Application	Criterion
Low frequency conduction	IEC61000-4-16	Power line/signal	A
High frequency conduction	IEC61000-4-6	Power line/signal	A
Magnetic field radiation resistance	IEC61000-4-8	EUT	A
Electric field radiation resistance	IEC61000-4-3	EUT	A
Surge (combined wave)	IEC61000-4-5	Power line/signal	B
Voltage suspension, short interruption and voltage change	IEC61000-4-11	AC power port	B
			C
Electric rapid transient pulse group	IEC61000-4-4	Power line/signal	B
Electrostatic discharge	IEC61000-4-2	EUT	B
High frequency conduction	CISPR 11	Power line	NA
The electric field radiation emits	CISPR 11	Power line	NA

4.6 Interfaces

Based on the high requirement of safety and reliability of NPP, it is not mature to widely adopt FCS technology at the present stage. Therefore, in actual engineering projects, there is a combination of FCS and DCS technology, so equipment that supports these two interfaces should be used simultaneously [5].

4.7 Maintenance

Using smart sensor helps to improve work efficiency, enhance the safety and economy of the unit. For example, using traditional methods for maintenance, pressure test and differential pressure transmitter calibration will take about 1.5 working days. Inspection work of smart sensor will be implemented in the computer without Cut off the cable and inject the test signal in the site, this work only takes an average of 15 min which greatly improves the work efficiency.

In addition, due to the use of communication methods and microprocessor, remote maintenance avoids the high temperature and high pressure in the field environment. This will improve the safety of maintenance personnel.

Based on the above analysis, FCS should be used as much as possible.

4.8 Cost

According to the current research conclusions, the cost of using one system of field bus technology will be relatively high, but the comprehensive of operation and maintenance factors for a long time, there will be less cost than the traditional DCS. The trend of relationship is show in Fig. 4.

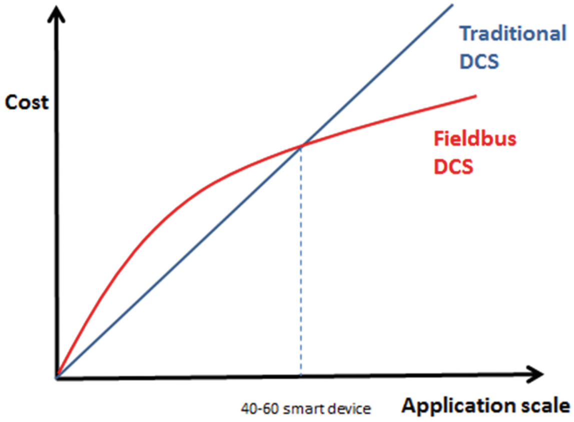


Fig. 4. Cost and application scale

4.9 Equipment Operation and Maintenance Platform

The FCS can obtain the maintenance and operation information of the smart device. If field bus technology is adopted, the Equipment operation and maintenance platform should be build up. Through the platform the operator is easy to acquire the status of equipment and raise the preventive maintenance level of equipment.

4.10 Protocol Compatibility Test

Although smart devices and DCS comply with the same standard of field bus protocols, communication tests are required when the device is firstly connected. The test will ensure compatibility between DCS and smart devices.

4.11 Summary

Considering the development trend of field bus technology, the manufacturing level of smart devices, field bus technology will be gradually applied in the NPP. Early, we can choose 1–2 system and then extend gradually to be whole plant.

5 Conclusions

The application of FCS system in NPP is a gradual step-by-step process, this article analyzes the field bus technology, detailed information of its technical advantages and existing problems, and puts forward some corresponding measures. On the basis of NPP operation, environment, technology, equipment and other requirements, the article put forward the general principles of the application of field bus. This provides a useful exploration and provides the basis for the subsequent large-scale application of field bus technology.

References

1. Yang, X.H.: Field Bus Technology and Its Applications. Tsinghua University Press, Beijing (1998)
2. Wen, L.: The application of field bus in the electric control system of thermal power plants. Technol. Enterp. **16**, 382 (2014)
3. Jin, Q.J.: The application of field bus technology in the auxiliary production system of Huaneng Yuhuan power plant. Power Gener. Equip. (2014)
4. NB/T 20026: The overall requirements for safety and control systems of nuclear power plants (2014)
5. Li, Z.: Field Bus and Its Applications. Mechanical Industry Press, Beijing (2005)

The Analysis of Periodic Test Solution for Main Feedwater Isolation Valve

Zhi-Hong Lv(✉)

State Key Laboratory of Nuclear Power Safety Monitoring Technology and Equipment,
China Nuclear Power Design Co., Ltd., Shenzhen, China
lvzhihong@cgnpc.com.cn

Abstract. This paper relates with the main feedwater isolation valve of nuclear power plant in the periodic test. The article analyzes the requirements of standard and summarizes the series of related standards. The classification, content and method of periodic test have been described. The solutions are proposed according to the problems of the main feedwater isolation valves in T3 test. In the design process of the periodic test solution, not only the design standards should be satisfied, the compatibility of test equipment and field equipment to different types of actuators should also be considered.

Keywords: Periodic test · T3 test · Main feedwater isolation valve

1 Background

Main feedwater isolation valve is one of the most important equipment in nuclear power plant. After the three steps of low heater, deaerator, and high heater, the deaerating and heating water will be delivered to three steam generators by the main feedwater system. To obtain the water level of steam generator secondary side which determined by turbine power, the water supply to the steam generator should be controlled. In this process, the main feedwater isolation valve is for protecting the reactor and the steam turbine unit. Therefore, main feedwater isolation valve needs to be periodically tested on a regular basis, to ensure the function of the instrument and control (I&C) system and the availability of the process equipment in the control loop. Periodical test is required for nuclear power plant equipment in IEEE603/IEEE338/GB/T13284.1. IEEE603 Sect. 5.7 requires clearly that safety system must has the ability of testing and calibration to ensure the reliability of the safety function [1, 2], and can satisfy the requirements of IEEE338 periodic test standard of the nuclear power plant safety system [3]. Section 5.7 of GB/T 13284.1 requests system has the capability of testing and calibration [4]. The design requirements for periodic test of safety systems in GB/T5024 are also specified. Items in design criterions, such as availability, accuracy, response time and set point should be validated periodically. Requirements are mentioned in periodic test functional requirements specification Sect. 3.3.2.2: T3 test should be carried out for the main feedwater isolation valve and bypass feedwater isolation valve, the main isolation valve is under class C test, bypass isolation valve is under class B test. Class C test requires that

Y. Xu et al. (eds.), *Nuclear Power Plants: Innovative Technologies for Instrumentation and Control Systems*, Lecture Notes in Electrical Engineering 455,
https://doi.org/10.1007/978-981-10-7416-5_27

when performs T3 test, the valve actuator cannot be triggered in full power operation condition. However, the actuator controlled by Priority control module (PCM) trigger accidental event successively occur for a number of feedwater isolation valves, leads to T3 test failure.

2 Periodic Test

2.1 T3 Test of a New Nuclear Power Plant

The requirements for periodic test of safety systems in GB/T5024 include channel check, function test, channel calibration and response time validation, and logical system function validation.

Periodic test is a type of safety system monitoring test. The I&C system needs to test the probe and process from the interface to the actuator, as shown in Fig. 1.

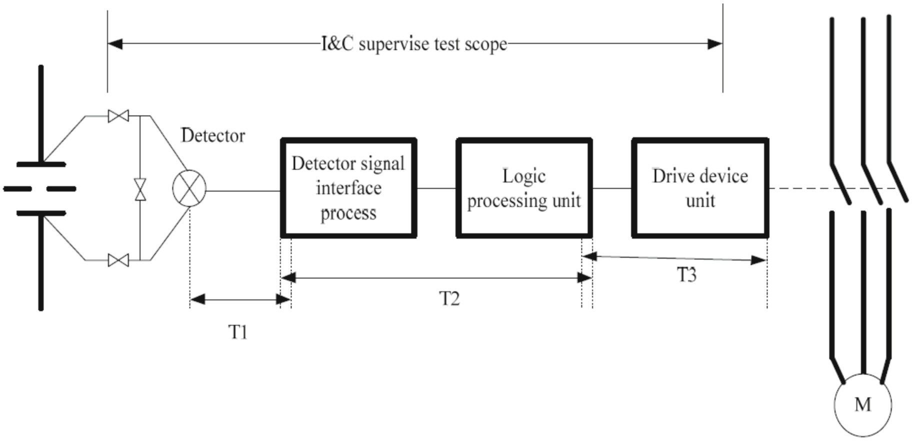


Fig. 1. The test scope of I&C system

According to the characteristics of the I&C platform and the safety of the power plant, the experiment is carried out in several sections, including:

- The T1 test, from sensors to signal collection;
- The T2 test, from the signal to the logical function;
- The T3 test, from logical functional processing (after voting logic) to actuator drive parts (including the driver, based on the technology of the plant).

This paper mainly describes the T3 test problem and analysis of the main feed water isolation valve.

Class C: during the normal operation of the unit, some actuators are unable to operate. They are designed to operate only in the accident, and their actions mean that the reactor's emergency shutdown or equipment is in danger. At this point, the tests against these actuators are limited to the validity of the security signals transmitted to the actuator by the protection logic system. Class C can be carried out only by the actuator, as the continuity test.

The continuity test is mainly aimed at the Class C actuators that can't really trigger the safety movement during the normal operation of the plant. The continuity test can check the function of the driver and the hard connection between the driver and the actuator. The test scope is shown in Fig. 2 [5]:

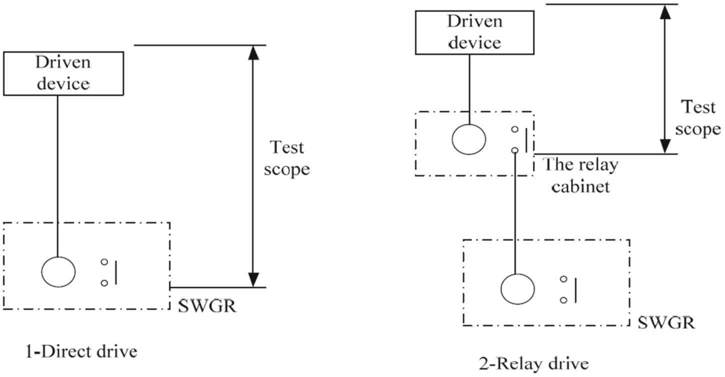


Fig. 2. The scope of continuity test

Continuity test is the testing on the final output of relay contact action, how to prevent real action caused by contact action of the actuator, is the basic points of the design.

2.2 The T3 Test of the Main Feedwater Isolation Valve

Main feedwater isolation valve receives valve close signal from 1E class valve and on-off command signal from the non-safety level of DCS respectively, after the optimization in the PCM module, on-off command will be sent to the smart electric head of valve, and feedback signal will be sent to the DCS, the control logic is shown in Fig. 3:

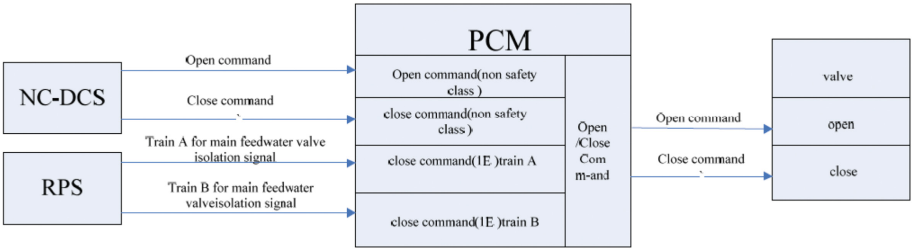

NC-DCS
RPS
Open command
Close command
Train A for main feedwater valve isolation signal
Train B for main feedwater valveisolation signal
PCM
Open command(non safety class)
close command(non safety class)
close command(1E)train A
close command(1E)train B
Open /Close Com m-and
Open command
Close command
valve
open
close

Fig. 3. The logic diagram of feedwater isolate valve

When safety injection occurs, the main feedwater isolation command will be triggered, protective shutoff command will be conducted by the ESF hardwire directly to the PCM driver module, NC on-off command from the DCS and the protective close command from 1E will be optimized within the PCM module, then the command will be sent to the intelligent electric valve head, triggering electric head movements. The implementation is shown in Fig. 4:

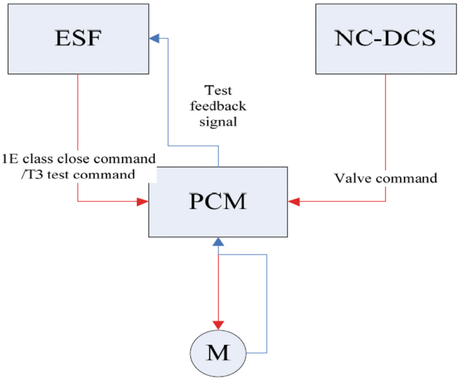


Fig. 4. I&C realization of main feedwater isolation valve

The main feedwater isolation valve (ROTORK manufacturer's intelligent electric head) is for the NC-class actuator class C T3 test range, which is controlled by PCM card. The T3 scope testing is mainly to validate channel integrity and card output from the safety level signal to the PCM and to the actuator and card output. The principle is shown in Fig. 5 (voltage driver, please see Table 1 about the PCM card input/output channel definition) [6].

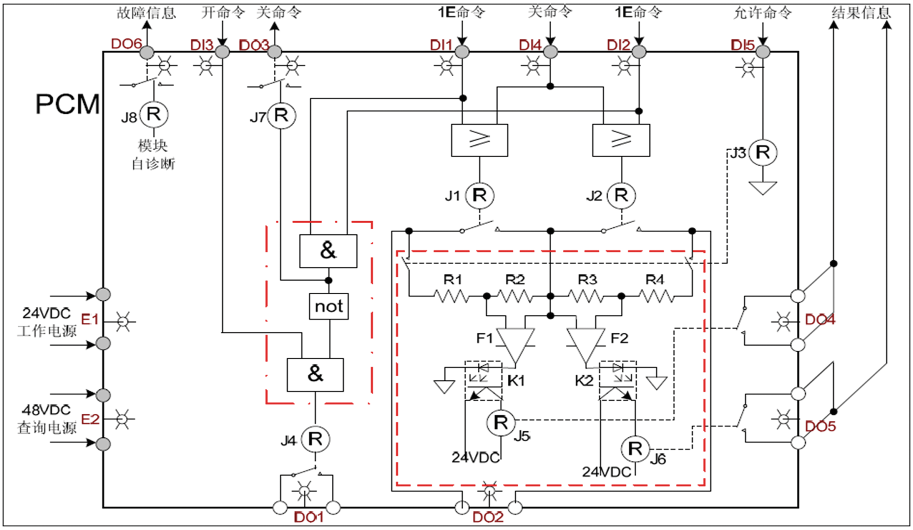


Fig. 5. The test principle of PCM card

Table 1. The illustration of output channel for PCM card

Item	Channel num.	Description
1	DI1	From 1E command, normal work for 1E protection close, T3 test for test command
2	DI2	From 1E command, normal work for 1E protection close, T3 test for test command
3	DI3	Open command from NC - DCS
4	DI4	close command from NC - DCS
5	DI5	The T3 test of 1E allows the command to be valid for the device that does not allow valve to trigger the motion when T3 is tested
6	DO1	open command Output to Level0
7	DO2	close command Output to Level0
8	DO3	Output to the 1E protection close command for NC-DCS
9	DO4	The permission command of T3 test output to 1E that do not allow trigger during T3 tests
10	DO5	The permission command of T3 test output to 1E that do not allow trigger during T3 tests
11	DO6	Self-diagnostic output of the PCM module to NC - DCS
12	E1	Work 24 V power supply
13	E2	Query 48 V power supply

Figure 5 is the schematic diagram of T3 PCM card test, DI1/DI2 are close commands from 1E level, which is the 1E protective shutoff command on the normal operation. Two 1E signals will be sent to PCM card DI1 and DI2 at the same time when the protection command is triggered, and actuators operate. The two 1E signals are test signals in T3 test, which are in turn test and can't be 1 at the same time, preventing the actuator from action by mistake. DI5 is theT3 test enable signal, J3 corresponding contact closes, DI1 sends the test signal, J1 corresponding contact closes. The loop through the internal resistors R3, R4, and the amplifier F2 makes the decoupling K2 conduction, trigger relay J6 and contact acting, lights DO5 to shut the feedback signal to complete the integrity test of the channel for the PCM card, then DI2 continuity is tested, test method is the same whit the DI1 channel test.

But some main feedwater isolation valves are closed in a nuclear power plant project by mistake, lead to T3 test failure.

3 Problem Analysis and Solution

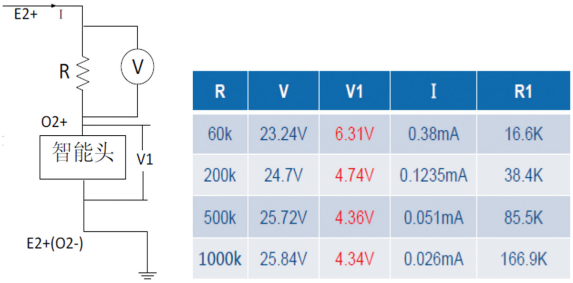
3.1 Problem Analysis

The main feedwater isolation valve controlled by PCM card motion event has occurred in T3 test. The main reason is that the internal resistance of PCM card used in T3 test to drive valve in NC- DCS does not match the resistance of the ROTORK intelligent electric head. Then the resistive subdivision of the PCM card is not high enough. Electric voltage on both sides of the intelligent valve head exceeds the threshold voltage of the valve drive mechanism.

Manufacturer of the intelligent valve head reflects that the intelligent valve head is remote voltage driver. If the remote control signal is higher than 20 V, the command is valid (that is 1), if it is less than 3 V, the command is invalid (that is 0). when it is used, ensure the command is 1 or 0, and the median (20 V and 3 V) might or might not action, therefore, the voltage must be higher than 20 V or less than 3 V to ensure the intelligent head operate appropriately. Other intermediate values may lead to intelligent head to malfunction. The internal circuit of the intelligent head has a diode. Its resistance is infinite when there is no conduction, when the external command voltage is high enough, the diode will conduct. The input circuit of intelligent head is complicated, consisting of resistance, capacitor, and semiconductor equipment, and its impedance characteristic is non-linear, depending on the external voltage.

3.2 Match the PCM Card to the Intelligent Head Resistance

As the mature equipment of ROTORK valve manufacturer, intelligent head has been applied for nuclear power plants many years. Manufacturers modifies the internal circuit is difficult (It needs to consider other project procurement in the future, requires the manufacturer to provide electric head voltage, current action threshold and internal impedance in the valve technical specification). Because the inherent characteristics of intelligent head for ROTORK manufacturers (simulation of intelligent circuit inside the head, adjust the internal resistance of the PCM card, making electric voltage on both sides of the intelligent head less than 3 V, ensure the intelligent motor head in the T3 test) will not be triggered in T3 test. The internal circuit of the PCM is simplified as shown in the Fig. 6, where the resistor R represents the total resistance between E2 + and O2 +. In the site test, the value of the resistance R (sliding rheostat) is tuned during T3 test, V1 is the voltage of the intelligent head on both sides), limit the intelligent head voltage under 3 V.



R	V	V1	I	R1
60k	23.24V	6.31V	0.38mA	16.6K
200k	24.7V	4.74V	0.1235mA	38.4K
500k	25.72V	4.36V	0.051mA	85.5K
1000k	25.84V	4.34V	0.026mA	166.9K

Fig. 6. The test circuit diagram and data of DCS supplier

3.3 Other Solutions

The instrumentation and control platform used relays logic and electromagnetic logic by configuring the resistance bridge in early. The current through the drive relay becomes small enough to allow it to act and judge the functional availability of the relay circuit, teste amplifier to the output relay by measuring the resistance voltage or current on the bridge, the short-term inspection of the field connection isn't implemented.

In some nuclear power plant project T3 test, the Siemens AV42 optimization module is used, because AV42 card is connected with relay, the line connection check is not available, test is only carried on the AV42 drive module, the connection test isn't applied.

In EPR project T3 test, the treatment is same with the project for the actuators cannot be real action in the full power operation. Test is only carried on the AV42E module. The implementation of the actuator of the connection has not been checked.

In the full power operation of the plant, Class C T3 testing requires actuators not to trigger according to RG 1.22 in some ESF systems. The operation of the entire group of equipment performing the safety function may destroy the plant equipment or affect the reactor operation. In this case, acceptable methods that can test the equipment while avoiding the undesirable effects of equipment operation. They include the following aspects.

(1) To test the drive and driven equipment respectively in a reasonable manner;
(2) To test the drive device while prevent some of the driven equipment action;
(3) The operation of the system for each equipment action requires the actuation of a plurality of driven device, so that the drive device can be individually tested.

Certain equipment during normal operation of power station cannot be tested. It is necessary to prove that the probability of trigger is sufficient low to an acceptable level. It dues to the protection system failure. GB/T5024 also indicates that operational trials that cannot be conducted during the reactor operation must be tested during the shutdown of the plant.

The main feedwater isolation valve is real action tested during the outage of the power station, does not do two months of real action test during the normal operation of the power plant. The main feedwater is isolated when the safety injection occurs, even if the valve cannot real act, due to the safety signal trigger the main feed pump and the main feedwater control valve action at the same time, but also to meet the requirements of the main feedwater isolation to ensure that the core is safe. This extends the periodic test cycle of the main feedwater isolation valve, increases its probability of failure, reduces its availability, but also has the main feedwater pump outage and the main feedwater control valve action to ensure the main feedwater isolation requirements.

Based on the above analysis, in view of the T3 test for the referred power plant, even if the actuator wiring continuity of the main feed isolation valves is not implemented. It still satisfies the requirement of the reference station, achieve the PCM card parts exports is also acceptable when do the class C T3 test. The problem is resolved using the first method by making electric voltage on both sides of the intelligent valve head not exceeds the threshold voltage of the valve drive mechanism.

4 Conclusions

This paper begins with the importance of main feedwater isolation valves. The article puts emphasis on the problems of main feedwater isolation valve periodic test. The analysis process has been given. On the premise of meeting the standard requirements, the test equipment and the matching of the field device are taken full account according to the characteristics of the safety level platform. The test equipment is comprehensive and the method is appropriate, which will not cause an impact on the operation and safety of the power plant.

References

1. Solution for Periodic Interface Test. Mitsubishi motors (2014)
2. IEEE 603: Standard criteria for safety systems for nuclear power generating stations (2009)
3. IEEE 338: Standard for criteria for the periodic surveillance of nuclear power generating station safety (2012)
4. GB/T 13284.1: The safety systems for nuclear power plants-Part 1: Design criteria (2008)
5. Zhang, L.Q., Jiang, H., Tian, Y.J.: Periodical test solution for safety I&C system of CPR1000 new project. Chin. J. Nucl. Sci. Eng. **30**, 103–109 (2010)
6. IEC 60671: Nuclear power plants - Instrument and control systems important to safety - Surveillance testing (2007)

Evaluation Measures About Software V&V of the Safety Digital I&C System in Nuclear Power Plant

Peng-Fei Gu[1](✉), Zhe-Ming Liu[2], Hui-Hui Liang[1], Wei-Hua Chen[1], and Feng Gao[1]

[1] State Key Laboratory of Nuclear Power Safety Monitoring Technology and Equipment,
Laboratory of I&C Equipment Qualification and Software V&V,
China Nuclear Power Design CO., LTD., Shenzhen, China
gupengfei@cgnpc.com.cn

[2] Product Information Committee of China Instrument and Control Society, Beijing, China
sssl116688@163.com

Abstract. Since the digital technology is used in the safety system of nuclear power plant (NPP), its safety and reliability are the most important factors to the safety operation of NPP. Software V&V (verification and validation) is a significant method to ensure the safety and reliability of the nuclear power safety I&C (instruments and control) system software, the system to evaluate the efficient of V&V activities needs to further research. An evaluation model of V&V activities has been described in the paper. The anomaly density, V&V effectiveness and V&V efficiency which are to measure the V&V effort, have been included in the model. In the article, the critical point of the anomaly density, V&V effectiveness, and V&V efficiency have been analyzed. Based on the V&V results of nuclear power safety I&C system software, a practice case has been performed to evaluate the V&V activities.

Keywords: NPP · Software V&V · Evaluation measures · I&C

1 Introduction

Computer technology has been quickly taken up in the process to improve and ensure the safety and reliability levels of nuclear power plants. The safety software of nuclear power plant has been divided into categories A, B and C [1]. The IEC 60880 [2] and IEC 62138 [3] together cover the domain of the software aspects of computer based systems used in nuclear power plants to perform functions important to safety. Software verification and validation (V&V) is the key element of evaluating the quality for the software. The verification and validation processes that are applied to the software lifecycle, including software concept V&V, requirements V&V, design V&V, construction V&V, and integration test V&V and so on [4]. TRS 384 [5] is the verification and validation technical report of software related to nuclear power plant instrument. IEEE 1012 [6] is the IEEE standard for system and software verification and Validation. The verification and validation activities are the most efficient method for evaluating the

Y. Xu et al. (eds.), *Nuclear Power Plants: Innovative Technologies for Instrumentation and Control Systems*, Lecture Notes in Electrical Engineering 455,
https://doi.org/10.1007/978-981-10-7416-5_28

software quality. They can help the users to evaluate the completeness, correctness, consistency and accuracy for safety software in nuclear power plant.

The standards and regulations are mature for the software verification and validation in nuclear power plant. The effective and sufficient of verification and validation activities also should be evaluated. The evaluation of verification and validation activities is benefit to improve the V&V processes and to appraise the software development processes and products. Some papers [7] have make the qualitative discussion. The related standards and regulations are less. IEEE 1012 [6] Annex E proposes three categories of measures associated with the V&V effort in brief. The measures are anomaly density, V&V effectiveness, and V&V efficiency. Trends can be identified and addressed by the feedback of V&V activities. But what the insightful information can be provided by the three categories of measures in the project. And how to use the three categories of measures in the practice needs to be considered.

An evaluate model of V&V activities has been described in the paper. The anomaly density, V&V effectiveness and V&V efficiency which are to measure the V&V effort, have been included in the model. This paper executes the quantitative research for evaluating the V&V activities. In the article, the focus opinions for the anomaly density, V&V effectiveness, and V&V efficiency have been analyzed. Based on the V&V results of nuclear power safety I&C system software, an calculate process has been performed for evaluating V&V activities, including the description for evaluating anomaly density, V&V effectiveness and V&V efficiency.

2 V&V Evaluation Model

Software V&V evaluation measures are based on the software V&V processes. Software V&V evaluation includes activities purpose building, data collection, data analysis and trend prediction. So an evaluation model of software V&V has been established in the paper as Fig. 1.

The model has been divided into six levels. The first level is the V&V object. The testers can make the V&V plan based on the object characteristics. The V&V processes, activities, and tasks have been included in the plan. The second level is V&V activities. It may need to execute multiple rounds. But the review items should be divided as the same principle during each round. The reviewed items are the third level. The reviewed items are difference in concept V&V, requirement V&V, design V&V, construction V&V and integration test V&V. The reviewed items are system requirements in the concept V&V for nuclear power plants. The items of other V&V processes are software requirements, design statements, implementation volume and test items. The quantitative information has been collected in the third and fourth levels. The forth level is anomalies. As Fig. 1, the concept anomalies may be found from the review of requirement, design, construction and integration test V&V. The requirements anomalies may be found from the review of design V&V, construction V&V and integration test V&V. It is the key point for calculating the V&V efficiency in the fifth level. The fifth level analyses the information based on the upper information. The anomaly density, V&V

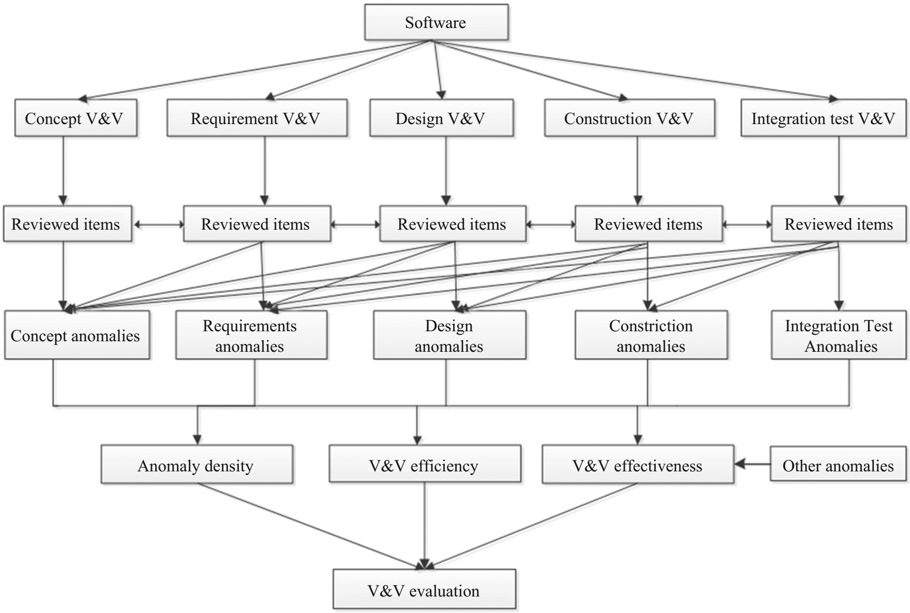


Fig. 1. Evaluation model of software V&V

efficiency and V&V effectiveness are the evaluation measures. The last level is V&V trend prediction.

3 V&V Evaluation Measures

3.1 Anomaly Density

Measures for evaluating anomaly density are used to evaluate the quality of the V&V effort. From IEEE 1012, the anomaly density is equal to anomalies found by V&V effort divide the reviewed items as Eq. (1). The anomalies include the concept anomalies, requirements anomalies, design statement anomalies, implementation anomalies and test anomalies found by V&V effort. So the concept anomaly density, requirements anomaly density, design anomaly density, implementation anomaly density and test anomaly density can be obtained.

$$\text{Anomaly density} = \frac{\text{Anomalies found by V\&V effort}}{\text{Reviewed items}} \tag{1}$$

Anomaly density is influenced by anomalies found by V&V effort and reviewed items for every V&V phase. So if the baseline is changed, the density will is different in the same V&V phase. The principles of reviewed items should be kept uniformity in the same V&V phase.

Anomaly density trends of the same V&V phase can be used to judge the quality of the V&V activities. They also can provide the reference for the similar characteristics. The changing trend of the anomaly density may be caused by the new requirements and the unfound anomalies by V&V in the previous round. If the product increases the new requirements, the program development quality needs to be improved. If the new anomalies have been found in the behind round, the V&V processes should be evaluated.

3.2 V&V Effectiveness

The other category of measures associated with the V&V effort is the measure for assessing V&V effectiveness. From IEEE 1012, the V&V effectiveness is equal to anomalies found by V&V effort divide anomalies found by all sources. The all sources anomalies may come from V&V activities and the development effort. V&V effectiveness is a quantitative indication. The anomaly can be used to evaluate V&V activities separately. So the measure defined by Eq. (2) include the concept V&V effectiveness, requirements V&V effectiveness, design V&V effectiveness, implementation V&V effectiveness and test execution V&V effectiveness.

$$\text{V\&V effectiveness} = \frac{\text{Anomalies found by V\&V effort}}{\text{Anomalies found by all sources}} \tag{2}$$

Anomalies need to be measure in the same baseline between V&V activities and development effort. It's better to execute the V&V activities and development effort in parallelism. The anomalies found by all sources should be in the same reviewed items. So the anomalies found by the development effort need to be mapped in the V&V reviewed items. Then the V&V effectiveness is reasonable and believable.

If the V&V effectiveness is limit to one, then V&V activities is effective. If the V&V effectiveness is limit to zero, then the quality of the development is high. So the V&V effective can also provide the reference for V&V team to elevate the developer. It's benefit to predict the V&V schemes and cost.

3.3 V&V Efficiency

V&V efficiency is an important indication for evaluating the capability of the V&V effort. The requirement V&V efficiency is equal to requirements anomalies found by V&V in requirement activity divide requirements anomalies found by V&V in all activities as Eq. (3).Then the concept V&V efficiency, design V&V efficiency, implementation V&V efficiency and test execution V&V efficiency can be obtained in the same way.

$$\begin{aligned}&\text{Requirement V\&V efficiency}\\&\quad = \frac{\text{requirement anomalies found by V\&V in requirement activity}}{\text{requirement anomalies found by V\&V in all activities}}\end{aligned} \tag{3}$$

As Fig. 1, the requirements anomalies may be found from requirements V&V, design V&V, implementation V&V and test execution V&V activities. The V&V anomalies need to be traced back to the primary causes. So the V&V anomalies should be discovered as early as possible to enhance the V&V efficiency. The quota means that the V&V activities are not separate. The V&V efficiency is related with the software life cycle.

Based on the V&V efficiency, the tester needs to find the factors which prevent the anomalies to be found. Then the V&V plan should be improved. The V&V activities need to be executed repeatedly to find the hidden anomalies and verify the new plan. V&V efficiency can also measure the development product. If the value is high, the factors may be that the development product and processes are inmmature.

4 V&V Evaluation Case

In order to verify the evaluation methods about software, a case has been exhibited. The evaluation measures of concept V&V activities have be performed of the safety digital I&C system in nuclear power plant. In the project, the concept V&V activity has been executed three rounds. The results show as Table 1. The change of reviewed items causes by the change of system requirements in the last round. Four system requirement documents has been became to one.

Table 1. The results of concept V&V activity

	Round I	Round II	Round III
Reviewed items	105	105	54
Anomalies	61	35	0

The baseline is as same as the round I of concept V&V. The anomalies obtained from the other V&V activities are shown as the Table 2.

Table 2. The anomalies of other V&V activities

V&V activities	Requirement V&V	Design V&V	Implementation V&V	Integration test V&V
Anomalies	6	0	0	3

4.1 Anomaly Density

The anomalies found by V&V activities decrease from the round I to round III. The concept anomalies found by V&V effort is seventy in the round I. They include the concept V&V anomalies of requirement V&V and test execution V&V. The round II anomalies are only come from the concept V&V. The anomaly density of the concept V&V activity is higher. The anomaly density has decreased along with the improvement of development process. So quality of the product and development process should be improved. The V&V activity facilitates correction of the anomalies. The quality of the V&V effort to discover anomalies is effective in the concept.

$$\text{Anomaly density I} = \frac{\text{Anomalies found by V\&V effort}}{\text{Reviewed items}} = \frac{70}{105} = 0.67 \tag{4}$$

$$\text{Anomaly density II} = \frac{\text{Anomalies found by V\&V effort}}{\text{Reviewed items}} = \frac{35}{105} = 0.33 \tag{5}$$

$$\text{Anomaly density III} = \frac{\text{Anomalies found by V\&V effort}}{\text{Reviewed items}} = \frac{0}{54} = 0 \tag{6}$$

4.2 V&V Effectiveness

The anomalies which come from the other source is less than V&V activities. The anomalies that have been found by development are included by the V&V activities. So the concept anomalies found by V&V effort is equal to the concept anomalies found by all sources. So the V&V effort is effective. The testers need to consider to incremental changes to the V&V process. The developers should concern to improvement the development process.

$$\text{V\&V effectiveness} = \frac{\text{Anomalies found by V\&V effort}}{\text{Anomalies found by all sources}} = \frac{70}{70} = 1 \tag{7}$$

4.3 V&V Efficiency

The V&V efficiency measure value is high that the V&V effort has discovered anomalies in the earliest concept V&V activities. The concept V&V process can decrease the rework and development costs. Combining the anomaly density with the efficiency, the development products need to further improve, the V&V effort is effective in concept V&V activities.

$$\begin{aligned} &\text{Concept V\&V efficiency} \\ &= \frac{\text{Concept anomalies found by V\&V in concept activity}}{\text{Concept anomalies found by V\&V in all activities}} \\ &= \frac{61}{70} = 0.87 \end{aligned} \tag{8}$$

The concept anomalies found by V&V in requirement V&V activity are caused by the concept documents are not detail. The requirements cannot trace to the concept document. The concept anomalies found by V&V in test V&V activity is that part of the parameter range is not explicit.

5 Conclusions

The evaluation model has been built in the article. The evaluation methods about software V&V of the safety digital system have been discussed in nuclear power plant. The paper has given the critical point of V&V anomaly density, V&V effectiveness and the V&V efficiency. The mapping between the reviewed items of the V&V activities and the anomalies found by all source or all V&V activities is the key point to obtain the exactly evaluation value of V&V activities. The practice case is performed in the last. By the practical case analysis, the evaluation methods are effective to elevate the V&V effort.

References

1. IEC 61226: Nuclear power plants-Instrumentation and control systems important to safety – classification of instrumentation and control functions. International Electrotechnical Commission (2005)
2. IEC 60880: Nuclear power plants - Instrumentation and control systems important to safety – software aspects for computer – based systems performing category a functions. International Electrotechnical Commission (2006)
3. IEC 61138: Nuclear power plants - instrumentation and control important for safety – software aspects for computer – based systems performing category B or C functions. International Electrotechnical Commission (2004)
4. Gu, P., Wang, S.C., Chen, W.H., et al.: A study about safety I&C system software V&V in nuclear power plant. In: Proceedings of the 24th International Conference on Nuclear Engineering (2016)
5. TRS 384: Verification and Validation of Software Related to Nuclear Power Plant Instrumentation and Control. International Atomic Energy Agency, Vienna (1999)
6. IEEE 1012: IEEE Standard for System and Software Verification and validation. The Institute of Electrical and Electronics Engineers (2012)
7. Gu, P.F., Xi, W., Chen, W.H., et al.: Evaluation system of software concept V&V about the safety digital I&C system in nuclear power plant. Lecture Notes in Electrical Engineering (2016)

Software Requirement Evaluation Method for Safety I&C System of Nuclear Power Plant

Jian-Zhong Tang(✉), Peng-Fei Gu, Sheng-Chao Wang, Ya-Nan He, and Wei-Hua Chen

State Key Laboratory of Nuclear Power Safety Monitoring Technology and Equipment, Laboratory of I&C Equipment Qualification and Software V&V, China Nuclear Power Design CO., LTD, Shenzhen, China
tangjianzhong@cgnpc.com.cn

Abstract. Digital technology has been widely used in safety instrument and control (I&C) system of nuclear power plant (NPP). In order to guarantee high quality requirements about the safety I&C system of NPP, software Verification and Validation (V&V) should be implemented according to the standard IEEE 1012-2004. Software requirements evaluation would be done in different activities of software V&V. Even if the main tasks has been given in IEEE 1012-2004, the study about the evaluation methods is necessary to make progress in the implementation. Based on the practice about YangJiang units 5 and 6 projects, which is a Generation II+ pressurized water reactor, this study illustrates the software requirements evaluation methods of safety I&C system related to the laws and regulation standards. The system with evaluation indexes has been established which is also used in the practice of software V&V. Finally the effect has been analyzed from the process of V&V activities in the software development process. As a result, the analysis is also benefit to the design, development, operation and maintenance of safety I&C System as technical references in NPP.

Keywords: Safety I&C system · Software V&V
Documentation evaluation Index

1 Introduction

With the rapid construction of China's nuclear power project, and the promotion of the strategy of localization of nuclear power equipment as well as the "going out" with the nuclear power, the localization of safety digital control system (DCS), as the nerve center of the NPP, has also made a breakthrough. For example, the FirmSys, China's first nuclear safety instrumentation and control I&C system that was independently developed by Chinese Guangdong Nuclear Power Group Co. Ltd has been successfully launched and used in nuclear power project. NicSys8000N developed by CNNC Control Systems Engineering Ltd has also passed the independent engineering review of I&C systems [1]. As one of the necessary technologies to ensure the safety and reliability of the safety I&C systems in NPP, software V&V can effectively guarantee the software to meet the expected requirements of safety function and performance

Y. Xu et al. (eds.), *Nuclear Power Plants: Innovative Technologies for Instrumentation and Control Systems*, Lecture Notes in Electrical Engineering 455,
https://doi.org/10.1007/978-981-10-7416-5_29

completely and correctly, that is to ensure that the software does not appear failure situation, and has received great attention in the field of nuclear power [2, 3]. In addition, it requires the I&C system products that implement safety functions in NPPs must conduct software V&V before launch [4].

The software V&V of digital safety I&C system for NPP runs through the whole process of software life cycle. It is used to conform that the activity output at each stage of the software life cycle can meet the requirements, and verify that the system can perform its expected function. The safety and reliability of software play an important role in ensuring system safety and avoiding heavy casualties and property losses so that there is an urgent need of the application of software safety and reliability analysis in the project [5]. While the independence, integrity and effectiveness of V&V activities are critical to ensure the safety and reliability of the safety digital control system software [6].

The software of safety I&C system in NPP is defined as the classification of safety according to the functional requirements [7]. The software V&V mainly refer to the requirements of IEEE 1012-2004, and perform the V&V tasks in accordance with the integrity Level 4 [8]. The activities of software V&V is divided into six major steps, namely: concept V&V, requirement V&V, design V&V, implementation V&V, integration test V&V, installation and checkout V&V. Because the requirement V&V is in the important position from software development outline design to detailed design, and considering the actual problem of huge amount of V&V activity input files, it is necessary to explore the activity of software requirements V&V, especially the V&V tasks included in the activity.

This article is organized as follows: the first part analyzes the content of the software requirements of safety I&C system of the NPP, combining with actual engineering to analyze the identification methods of software requirements, and proposes the software requirements evaluation method in the software requirements V&V; the second part analyzes the main indexes and key contents of the software requirement evaluation for the safety I&C system of NPP, and worked out the implementation steps for software requirements evaluation; the third part is combined with the software V&V activities of engineering practice, taking the practice of a nuclear power software V&V project as an example to illustrate the effectiveness of the software requirements evaluation method. At the same time, the challenges and directions of software requirements evaluation are summarized.

2 Software Requirement Identification of Safety I&C System in NPP

The software of safety I&C system in NPP is defined as the classification of safety according to the functional requirements. The software development process should meet the corresponding safety software requirements, and follow requirements of its product quality assurance system. According to the requirements of HAF 102-2004 and HAD 102/16-2004, for the safety digital I&C system software of NPP, the software V&V must be performed [9, 10].

According to the requirements of GB/T 13629-2008 and R.G. 1.168-2004, the safety I&C system NPP software should perform V&V in accordance with level 4 of integrity specified in IEEE 1012-2004 to check whether the software meets the requirements of relevant laws and regulations, user requirements and the requirements of I&C system of NPP [11, 12].

The software V&V NPP mainly includes six activities, namely: the concept V&V, the requirement V&V, the design V&V, the implementation V&V, the integration test V&V, the installation and checkout V&V.

The software concept V&V involves the design of system architecture and the analysis of system requirements, and puts forward the concrete solution to solve the users' problems, and the system architecture assigns the corresponding system requirements for hardware, software, and users' interface components. The software concept V&V activity verifies the correctness, accuracy and integrity of system requirements allocation, and make sure that the wrong assumptions are not entered into the program. The output of the software concept V&V activity, that is the system design transformed from system requirements assigned to the software, will be used as the input of software requirements V&V activity.

The software requirement V&V is to analyze the function and performance, the external interface of software, identification requirements, safety and security requirements, human engineering requirements, data definition requirements, the user documentation requirements of software, installation and acceptance requirements, user operations and implementation requirements, and user maintenance requirements, which is involved in the software of safety I&C system of NPP in order to ensure the correctness, integrity, accuracy, testability and consistency of software requirements.

The safety I&C system of NPP is a complex system engineering. For considerations of safety and reliability, the design and development of safety I&C system software in NPP requires to perform complex functional operations with simple program logic. Therefore, it is necessary to identify the software requirements before transforming the software requirements into detailed design and the subsequent code and the database structure. The relevant implementation standards, such as IEEE 1012-2004, only explicit that the software development should select the integrity level and complete the corresponding task according to function performed by the software, but there is no specific technical solution for the effective identification of software requirements. Through the engineering practice of CPR1000 nuclear power project, in order to identify software requirements effectively, it can be encircling the traceability analysis to make the inputs of software requirement V&V activity like requirements documents items and form the process records of software requirement analysis, providing the basis for subsequent analysis and evaluation of V&V tasks (Table 1).

Before the software requirements V&V starts the first is to clear the inputs of the activity, which is including the criterion documents and object documents. The criterion documents are the upstream input for software requirements V&V, that is the output of system concept design document of the concept V&V. While the object documents is the output software requirement analysis document of the requirements V&V. Through the item of requirement item for each input document of the software requirement V&V to perform the requirements of tasks. In the process of implementation of the V&V activity, if there is an anomaly in the input document, the opinion is

Table 1. Software requirements items

Number	Criterion document		Object document		Opinion	Record of anomaly item	Remarks
	Requirement items	Page number	Requirement items	Page number			
1							
2							
3							
……							

"to be discussed", corresponding to record the anomaly and organize the list, anomaly submitting them to the design and development parties for correction.

Through items of the requirement of input document of the software requirement V&V, it can effectively meet the requirements of V&V tasks, which is involving in huge amount of documents, drawings. And it also can identify the software requirements and discover the anomaly, ensure the safety and reliability of safety I&C system in NPP.

3 Software Requirement Evaluation of Safety I&C System in NPP

The software of safety I&C system in NPP is defined as the classification of safety according to the functional requirements NPP. The software requirement V&V need to be performed according to the integrity Level 4 in IEEE 1012-2004. The minimum task V&V involved in requirements V&V mainly includes: traceability analysis, software requirements evaluation, interface analysis, critical analysis, hazard analysis, risk analysis, safety analysis, configuration management evaluation, the generation of system test plan of verification and validation and acceptance test plan of verification and validation. In the software requirements identification of previous chapter, according to traceability analysis and interface analysis, document review and traceability analysis should be carried out firstly for requirement items. The result of identification and analysis of software requirements items can serve as a reference for software requirements evaluation and to evaluate the requirement document of software design and development phase combining with the index of software requirement evaluation.

The software requirement V&V undertakes the system design of the system requirements for the outline design software, and carries on detailed design and program implementation so that software requirements can be correctly identified. After the effective identification of software requirements, the identified software requirements and their analysis results should be evaluated. The purpose of the evaluation is assurance the correctness, consistency, completeness, accuracy, readability and testability of the software requirements. The corresponding evaluation indexes and their evaluation contents are shown in Table 2.

Evaluate the target content through the software requirements listed above, evaluate the requirements items that have been identified by entry division of software

Table 2. Software requirements evaluation indexes and contents

Number	Indexes	Evaluation content
1	Correctness	– Verify and confirm that the software requirements meet the requirements assigned to the software system under system assumptions, constraints, and operating environments; – Verify that software requirements meet the demand of standards, regulations, engineering references, regulations, policies, contracts and other documents; – Verify that data and control streams meet functional and performance requirements; – Confirm data usage and format.
2	Uniformity	– Verify that all the terms and their definitions are consistent; – Verify that the function can meet system requirements and procurement requirements; – Verify that each software requirement has internal consistency and has external consistency with system requirements.
3	Completeness	– Verify that the following elements are specified in the software requirements under system assumptions and constraints: • The software associative function (algorithms, status/mode definitions, input/output validation, exception handling, reports, logs, etc.); • Process definition and schedule; • The description of the hardware, software and user interface; • The performance criteria (such as: time requirements, size, capacity, speed, accuracy, precision, safety and prevention); • The control of system, device, and software (such as initialization, transaction and status monitoring, self-checking). – Verify that the software requirements meet the specified configuration management process.
4	Accuracy	– Verify that logic, computation, and interface accuracy (truncation and rounding) meet the requirements of the system environment; – Verify that the established physical model meets the requirements of system accuracy and natural laws.
5	Readability	– Make sure that the document is clear, understandable and unambiguous; – Verify all abbreviations, breviaries, terms, symbols that have been defined by the document.
6	Testability	– Verify the target acceptance criteria used to identify software requirements.

requirements. In the V&V project of nuclear power engineering software, refer to the exception grading principle of GJB2786A-2009, the identified abnormal items are divided into 5 grades according to the possible severity of the system failure consequences, namely “fatal”, “critical”, “important”, “general” and “suggestion” [13]. The requirement V&V can identify the existing abnormal items and risk items through the process of identification, analysis and grading evaluation, the evaluation results can also provide reference for other V&V tasks, such as hazard risk analysis.

4 The Project Practice of Software V&V

Take the software V&V project of safety of instrument control system prototype of CPR1000 autonomous NPP as an example, using the software requirements identification and evaluation method proposed in this paper to evaluate the requirement of software in the requirement document so as to illustrate the effectiveness of the method. In document review and traceability analysis of requirements V&V, form 585 requirements check entries through the entry division of requirement document, 10 typical exception items are found, 1 of these is the "critical" issues in the software development process, the other 9 are the "important" issues that have not been reflected in the downstream software requirements document that from the upstream requirements of software in system design. Abnormal problems are summarized in Table 3.

Table 3. Software requirements items evaluation

Number	Exception summary	Exception influences	Grading evaluation
1	In the software requirements document, the technical content of the system design document is referenced directly and extensively. The software requirements document should be refinement and design solidification that based on the system design document, therefore, it is inconsistent with the design process	The lack of standardization of design process may lead to the subsequent development of software can̓t meet the relevant standards and regulations requirements, the user requirements and requirements of instrumentation control system of NPP	Critical
2	In the system design document, the related requirements of software can̔t be reflected in the software requirements document	Software requirements have not be identified and analyzed, which may lead to the loss of function or error implementation	Important

What needs to be explained is that, the implementation process and evaluation results described above are not only applicable to the requirements V&V in the software development life cycle, the other five verification and validation mentioned above are also apply. In this way, the whole process of software V&V development from requirement analysis, outline design, detailed design and transformation implementation to final integration test and installation test is formed. The entry analysis of software requirements is beneficial to keep the correctness, consistency, completeness and accuracy in the whole life cycle of software. If software development can be considered from the began of whole life cycle, and achieve the best balance between development cost and the precision of software requirements entry, it will have a significant effect on the improvement of the quality of software.

5 Conclusion

Software requirement evaluation is one of the important V&V tasks of the requirement V&V in the whole life cycle of software development. Because it takes part the system architecture and requirements allocation for software outline design, and carry the detailed design and implementation of the software, in addition, the requirements V&V is in the field of the V&V project of nuclear power software. Therefore, the amount of input files involved has great practical challenges. How to evaluate software requirements efficiently is the key technology problem in the requirement V&V.

In this paper, by referring to the relevant requirements of the implementation standard of safety critical software of IEEE 1012-2004, combined with the engineering practice of V&V project of nuclear power software, summarize and refine the effective method of software requirement evaluation – the entry of software requirement. In the process of requirements V&V, according to the index content of software requirement evaluation, make grading evaluation of the requirement items in input documents, so as to get the design quality of software development from system design to the requirement analysis of software.

The software requirements evaluation method proposed in this paper can be applied to document requirement evaluation of all software V&V during the whole life cycle of software development, it can solve the problem of unclear or messy design of the documents requirement in the process of software development, which is beneficial to the abnormal traceability of the design and development, operation and maintenance of the safety of I&C system in NPPs, it also provides technical reference for the entry of software requirements and the traceability mapping of full life cycle in automation tools.

References

1. Ding, Y.X., Gu, P.F., et al.: Study on standard about safety digital I&C system in NPP. Process Autom. Instrum. **36**(11), 61–64 (2015)
2. Gu, P.F., Xi, W., Chen, W.H., et al.: Evaluation system of software concept V&V about the safety digital I&C system in nuclear power plant. In: International Symposium on Software Reliability, Industrial Safety, Cyber Security and Physical Protection for Nuclear Power Plant, vol. 400, pp. 125–132. Springer, Singapore (2016)
3. Liang, H.H., Gu, P.F., Tang, J.Z., et al.: A study of implementation V&V activities for safety software in the nuclear power plant. In: International Symposium on Software Reliability, Industrial Safety, Cyber Security and Physical Protection for Nuclear Power Plant, vol. 400, pp. 23–31. Springer, Singapore (2016)
4. Ye, W.P., Tang, J.Z., Chen, W.H.: Software V&V methods for safety digital I&C system of nuclear power plant. At. Energy Sci. Technol. **49**, 378–381 (2015)

5. Zhao, J., He, Y.-N., Gu, P.-F., et al.: Reliability of digital reactor protection system based on extenics. Springer Plus **5**(1), 1953 (2016)
6. Gu, P.F., Wang, S.C., Chen, W.H., et al.: A study about safety I&C system software V&V in nuclear power plant. In: The 24th International Conference on Nuclear Engineering, vol. 1, p. 005. American Society of Mechanical Engineers (2016)
7. International Electro Technical Commission: IEC 60880 Nuclear power plants-Instrumentation and control systems important to safety-Software aspects for computer-based systems performing category A functions. International Electro Technical Commission, Switzerland (2006)
8. Software Engineering Standards Committee of the IEEE Computer Society: IEEE 1012 IEEE Standard for Software Verification and Validation. Institute of Electrical and Electronics Engineer, New York (2004)
9. HAF 102: Safety of Nuclear Power Plant Design Regulations. Doctoral dissertation (2012)
10. HAD 102/16: Safety of Nuclear Power Plant Design Regulations Guides. Doctoral dissertation (2004)
11. GB/T 13629: Applicable standards for digital computer in safety system of nuclear power plant. Doctoral dissertation (2008)
12. R.G.1.168: Verification, validation, reviews, and audits for digital computer software used in safety systems of nuclear power plants. U.S Nuclear Regulatory Commission (2004)
13. GJB2786A: Military software General Development Requirement. Doctoral dissertation (2009)

Discussion on Multi-dimensional Security System of See-Air-Land in Nuclear Power Plant

Shuang Li[1](✉), Wei-Dong Liu[2], Zhe-Ming Liu[3], Peng-Fei Gu[1], and Wei-Hua Chen[1]

[1] State Key Laboratory of Nuclear Power Safety Monitoring Technology and Equipment,
China Nuclear Power Design CO., LTD., Shenzhen, China
lishuang@cgnpc.com.cn

[2] National Nuclear Security Technology Center, Beijing, China

[3] Product Information Committee of China Instrument and Control Society, Beijing, China
sssl116688@163.com

Abstract. With the rise of global terrorist forces, nuclear facilities have been targeted by some terrorist groups for their extreme purposes, and carried out targeted training. In modern society, the rapid development of Internet information intrusion, unmanned aerial vehicles and unmanned submersibles has made it easy for terrorist forces and anti-nuclear organizations to obtain relevant technical equipment. Therefore, these factors and related threats have brought new challenges to nuclear security. In an increasingly complex security environment, the design that only has been taken from the ground intrusion to prevent benchmark could unable to adapt to the current security requirements. How to build a nuclear security system that can jointly cope with air intrusion, ground intrusion, underground intrusion, sea intrusion, cyber intrusion, etc., is the key point we must pay attention to. This paper focuses on the demand of multidimensional and protection system, integrate the existing available means of nuclear security technology, using big data fusion thinking, through information intelligent processing means such as identifying, behavior analysis, to explore the construction of multi-dimensional integration of a new generation of security system.

Keywords: Nuclear security · Information security · Airspace security
Sea security · Multi-dimensional integrated security system

1 Introduction

On September 11, 2001, an airliner hijacked by terrorists crashed into the world trade center and the US department of defense pentagon in the United States, causing fateful consequences. In February 2012, the "stuxnet" virus struck Iran's nuclear power plant, leaving a fifth of its centrifuges scrapped. In October 2015, the British Think Tank reported that, with the large use of commercial software and the increasing reliance on digital technologies, the cyber security threat of the global civilian nuclear facilities is getting worse [1].

The constant development of new technologies, the growing threat of anti-terrorism situation and the rising threat of nuclear terrorism have led to the increasingly serious

Y. Xu et al. (eds.), *Nuclear Power Plants: Innovative Technologies for Instrumentation and Control Systems*, Lecture Notes in Electrical Engineering 455,
https://doi.org/10.1007/978-981-10-7416-5_30

situation of international nuclear security. China is not only the country that has the largest number of power plant units under construction in the world, but also one of the few countries with complete nuclear industry chain in the world. There are many nuclear materials and radioactive sources that need to be protected. At the same time, the situation of nuclear security in China is very complicated. The construction of the Domestic nuclear facilities have developed rapidly and the number of nuclear radioactive materials huge, resulting in an active international nuclear black market in the surrounding area, which leading to a more serious threat of domestic and international terrorism [2]. Meanwhile, the construction of the nuclear security system also needs to reposition the new challenges posed by emerging technologies.

2 The Situation of Nuclear Security

Prevent, detect and respond to nuclear materials and other radioactive substances or other related facilities are stolen, sabotage, unauthorized contact, illegal transfer or other malicious behavior is an important goal of nuclear security [3], which can maximize the protection of personnel, property, society and the environment from the radiation hazards.

With the popularity of unmanned aerial vehicle (uav) technology and the rapid development of cyber intrusion technology information, intrusion means will gradually show the characteristics of the diversification and specialization, and intrusion pattern will also extend from a single ground intrusion to the water, the air, the cyber, the internal and external collusion, etc. The defense targets will also be diverse, such as terrorists, underwater frogmen and automatic submersible, surface ships, drones, hackers, and internally defectors.

The targets mentioned above actually have gone far beyond the design basis threat for physical protection system of nuclear facilities. Due to the deteriorating situation of security, the nuclear facilities have to deal with the super-design threats.

3 Analysis of Intrusion and Penetration

The threat of nuclear security mainly comes from internal penetration and external intrusion. Internal penetration mainly considers the dangerous behavior from the internal staff. External intrusion mainly considers physical intrusions from the ground, underground, low-altitude and water, and virtual intrusions from the network.

3.1 Analysis of Ground Intrusion

Ground intrusion can be divided into single point intrusion and multi-point invasion. Ground incursions need to consider in response to organized and planned multipoint invasions, as well as need to consider in response to the complex intrusion that use feint to attract response forces.

The forms of ground intrusion are complex and changeable, and the common forms of intrusion are as follows:

a. Abnormal conditions outside the defense boundary: Focus on early warning and control of individuals or groups of individuals who behave in unusual ways.
b. The intrusion of the fake staff: The need to deal with the intrusion behavior that the personnel and the authorization card are not consistent.
c. The intrusion of modified the authorized vehicles: The need to deal with the risk behaviors of vehicle refitting and concealing.
d. The intrusion of carrying objects: The need to deal with the Risk behaviors such as package carrying and body carrying.

3.2 Analysis of Underground Intrusion

Underground intrusion has very strong concealment characteristic. Considering the possible mining behavior, monitoring the vibration of the areas that have not been hardened needs to be mainly considered, as well using technology methods to monitor the pipe rack which has external interface.

3.3 Analysis of Low-Altitude Intrusion

In recent years, with the explosive growth of the global civil uav market, there has been a constant occurrence of uav attacks on sensitive facilities. In May 2017, a foreign media reporter used an UAV to aerial photography a domestic NPP without permission. The uav flied over the reactor building and fuel storage facilities, which brought security hidden danger to NPP and the negative impact on society.

Low-altitude slow small uav with low cost, easy to carry, easy to obtain, launch sudden strong, not easily found by reconnaissance and other advantages, and has the functions of photoelectric reconnaissance, explosive material release and chemical release.

Therefore, it is necessary to deal with unmanned aerial vehicles, especially unmanned aerial vehicles which have the capacity of loading. In addition, the early warning mechanism should be designed according to the ability of the disposal personnel to respond, and the ability of multi-target tracking should be considered. In the case of technical conditions, it is necessary to configure the function of positioning the uav operators.

3.4 Analysis of Water Intrusion

In recent years, under the background of the frequent terrorist forces activities and the variety of attack means, the ability of waters security for NPP needs to be increased. It is necessary to consider the risk of the safe operation of the unit by the attack, intrusion or direct destruction of the enemy.

The intrusion prevention of water intrusion is mainly concerned with the intrusion of water surface rapid impact type. Meanwhile, it also needs to consider the underwater covert intrusion, including the frogman intrusion and the intrusion of unmanned submersible.

3.5 Analysis of Cyber Intrusion

With the rapid development of information technology, the digital industrial control system has been widely used, which leads to the security of the information system itself is becoming more and more important to NPP unit security, and the problem of information intrusion is becoming more and more serious.

It is necessary to consider viruses, trojans, and networks to make the network out of control, and then make the system fail in many forms of network intrusion.

3.6 Analysis of Internal Penetration

The international atomic energy agency (IAEA) points out that insiders can bypass the physical protection system of measures or other regulations by their access, by having some operation license and a certain degree of understanding of the facilities, such as security measures, material control and balance, and running measures and procedures. In addition, insiders are able to enter various work areas, and in the face of protective factors and in and out of control, they can also implement the "win" method that outsiders can't use. At the same time, insiders have more opportunities to choose the weakest targets and the best time to carry out malicious behavior, and the chances of success are higher. Therefore, it is necessary to consider effective identification and intervention measures to deal with the dangerous behavior of internal personnel (Fig. 1).

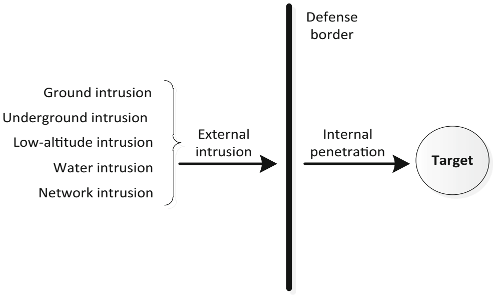


Fig. 1. Intrusion and penetration

4 Response to Threat

With the upgrading of security technology, especially mature application of Internet technology in recent years, the breakthrough of video transmission technology and the rapid development of intelligent recognition technology, there have more solutions to deal with the threats. The security system is a comprehensive system of detecting, delaying and responding to a series of elements. The ability to accurately detect and effectively identify are core functions. As long as these two points are done, the conditions can be provided for the response to the intrusion [4]. An accurate view of intrusion behavior is shown in Table 1.

Table 1. Response measures for intrusion and penetration in NPP

Intrusion area	Intrusion type	Response measures
Ground	Multipoint intrusion	1. Accurate positioning technique for accurate position judgment 2. The intelligent identification of gun ball linkage camera 3. Check the scene screen of the alarm check camera
	Fake staff	Using face recognition and vein identification in the entrances and entrances can identify that the human and card are consistency
	Modified authorized vehicle	The technology of car base photography, license plate recognition, personnel authorization analysis, vehicle appearance comparison, etc
Underground	Unhardened area	Through embedded vibration sensor, the abnormal vibration data of underground can be monitored continuously. The data is transferred to the software for processing, which can accurately identify the source of the vibration
	Pipe rack	Set up physical barrier and combine with the compound recognition function of special camera
Low-altitude	uav	Unmanned aerial vehicle defense system
Water	Quick ship	Set up the physical fence and combine with the space detection equipment
	Frogman, unsubmersible	Small sonar technology
Network	Viruses and trojans	Hierarchical control Personnel authorization and supervision Antivirus software Software verification and validation
Inside	Penetration	Through personnel positioning system, personnel abnormal behavior supervision technology and combining with big data fusion and mining technology, the abnormal behavior of internal personnel is checked

5 Construction of Multi-dimensional Security System

Through the analysis of the various forms of threats, this paper provides a basis for the construction of multi-dimensional security system. In the construction of multidimensional security system, the defense zone on the ground will be divided into early warning area, alarm region, delay area and response area. It is divided into low-altitude defense, ground (surface) prevention, underground (underwater) prevention from space; In the form of protection form, it is divided into physical impact type, information intrusion type and internal personnel infiltration, thus forming a multi-dimensional three-dimensional security system, as shown in Fig. 2.

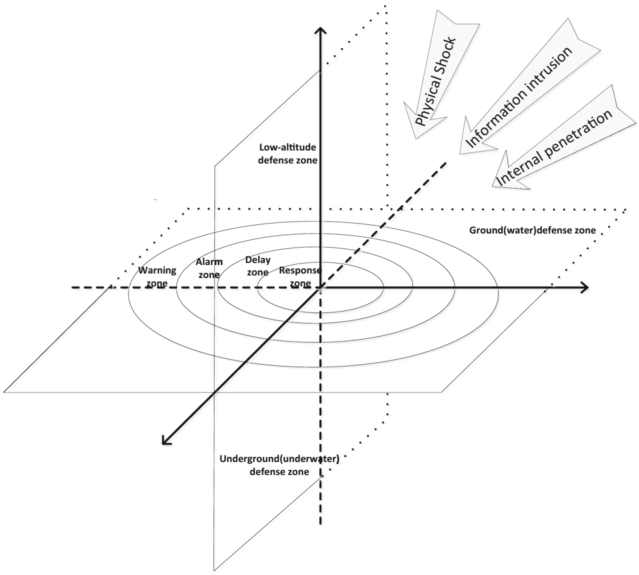


Fig. 2. Multi-dimensional Security System of See-air-Land

In this system, the integration and processing of information is the core link, whether it can effectively dispose and integrate a large number of multi-dimensional information or not will be the key point to the operation of the system. In order to make intelligent analysis through mathematical model, the overall goal of multi-dimensional three-dimensional security system is studied through the system's self-learning of specific project situation.

6 Summary

In this paper, the form and characteristic of external intrusion and internal penetration has been carried on the system analysis. Meanwhile, the new form of intrusion of integrated security system has been put forward that combining with the original security system of NPP. The proposed system not only improves the capability of nuclear power plants to deal with all kinds of external intrusion and internal penetration, but also provides reference for the new generation safety system of NPP. It is believed that with the rapid development of security technology and data processing technology, the system can realize engineering application in the near future. And it has more in-depth research on the function of situational awareness and event decision making.

References

1. Yan, M., Feng, L.F., Yan, M.: Research on nuclear security and nuclear security measures. China Sci. Technol. Expo. 300–301 (2013)
2. Liu, C.: The situation and policy of China's nuclear security. Contemp. Int. Relat. **3**, 4–9 (2016)
3. Mao, Y.Z., Wang, S.Q., Zhou, Y.L.: Numerous issues about nuclear safety construction and nuclear security system. J. Southwest Univ. Sci. Technol. **27**(4), 1–10 (2012)
4. Li, X.F., Ye, L., Wu, W.F.: Discussion on planning of physical protection system for maritime nuclear facilities. Electron. Instrum. Cust. **23**(9), 81–83 (2016)

Author Index

Y. Xu et al. (eds.), *Nuclear Power Plants: Innovative Technologies for Instrumentation and Control Systems*, Lecture Notes in Electrical Engineering 455,
https://doi.org/10.1007/978-981-10-7416-5