Springer Series in Advanced Manufacturing

Lane Thames
Dirk Schaefer *Editors*

Cybersecurity for Industry 4.0

Analysis for Design and Manufacturing

Springer

Springer Series in Advanced Manufacturing

Series editor

Duc Truong Pham, Birmingham, UK

More information about this series at http://www.springer.com/series/7113

Lane Thames · Dirk Schaefer
Editors

Cybersecurity for Industry 4.0

Analysis for Design and Manufacturing

Springer

Editors
Lane Thames
Research and Development Department
Tripwire, Inc.
Atlanta, GA
USA

Dirk Schaefer
Department of Mechanical Engineering
University of Bath
Bath, Bath and North East Somerset
UK

ISSN 1860-5168 ISSN 2196-1735 (electronic)
Springer Series in Advanced Manufacturing
ISBN 978-3-319-50659-3 ISBN 978-3-319-50660-9 (eBook)
DOI 10.1007/978-3-319-50660-9

Library of Congress Control Number: 2017932776

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

A transformative event known as Industry 4.0 is occurring where countless elements comprising industrial systems are being interfaced with internet communication technologies to form the smart factories and manufacturing organizations of the future. Industry 4.0 and its associated technologies, such as cloud-based design and manufacturing systems and the Industrial Internet of Things, are currently being driven by disruptive innovation that promises to bring countless new value creation opportunities across all major market sectors. However, existing internet technologies are plagued by cybersecurity and data privacy issues that will present major challenges and roadblocks for adopters of Industry 4.0 technologies. Industry 4.0 will face traditional cybersecurity issues along with its very own unique security and privacy challenges. If these challenges are not appropriately addressed, the true potential of Industry 4.0 may never be achieved.

The objective of this book is to provide an overview of cybersecurity for the Industry 4.0 landscape with an emphasis on Design and Manufacturing applications. It covers the technological foundations of cybersecurity within this domain and addresses existing threats faced by Industry 4.0 sectors along with existing state-of-the-art solutions. To provide a holistic perspective, the topic is discussed from the perspectives of both practical implementations in industry and cutting-edge academic research. This way, it benefits practicing engineers and decision makers in industry as well as researchers and educators in the design and manufacturing communities.

In Chapter "Industry 4.0: An Overview of Key Benefits, Technologies, and Challenges", Thames and Schaefer provide details of Industry 4.0 technologies and paradigms in order to provide the reader with a good background of Industry 4.0 basics. The purpose of this chapter is to give the reader a better understanding of the cybersecurity aspects of the remaining chapters in the book.

In Chapter "Customized Encryption of CAD Models for Cloud-Enabled Collaborative Product Development", Cai, Wang, Lu, and Li introduce an innovative and customized encryption approach to support secure product development collaboration. Their goal is to maintain the security of the sensitive information in

CAD models while sharing other information of the models in the cloud for effective collaboration.

Wegner, Graham, and Ribble introduce in Chapter "A New Approach To Cyberphysical Security in Industry 4.0", titled a new paradigm using a direct-to-machine communication approach that limits and protects information flows to internal and subcontracted factory floor devices to complement perimeter security. The authors believe this to be an essential first step in creating secure manufacturing for Industry 4.0.

Chapter "SCADA System Forensic Analysis Within IIoT" introduces the reader to Forensic Analysis within the Industrial Internet of Things (IIoT). In this chapter titled "SCADA System Forensic Analysis within IIoT", Eden et al. focus on the need for incident response when incidents occur within Industry 4.0 environments. The chapter focusses on the forensic challenges and analysis within an IIoT and its physical infrastructure.

In Chapter "Big Data Security Intelligence for Healthcare Industry 4.0", Manogaran et al. provide an overview of how the healthcare industry can be viewed as an Industry 4.0 paradigm. The healthcare industry has started using many types of Internet of Things (IoT) and Industrial Internet of Things (IIoT) technologies. The data generated by healthcare 'things' should be managed with security and privacy in mind. The authors introduce their Meta Cloud-Redirection architecture and describe the security and privacy aspects of it.

In Chapter "Decentralized Cyber-Physical Systems: A Paradigm for Cloud-Based Smart Factory of Industry 4.0" Zhang et al. introduce the conceptual model and operation mechanism of decentralized cyber-physical systems (CPS), which enables manufacturers to utilize a cloud-based agent approach to create an intelligent collaborative environment for product creation. Similar to Chapter "Industry 4.0: An Overview of Key Benefits, Technologies, and Challenges", Chapter "Decentralized Cyber-Physical Systems: A Paradigm for Cloud-Based Smart Factory of Industry 4.0" details many key underlying technologies of Industry 4.0.

Chapter "Applying and Assessing Cybersecurity Controls for Direct Digital Manufacturing (DDM) Systems" introduces the reader to direct digital manufacturing and its cybersecurity needs. In this chapter, Glavach, LaSalle-DeSantis, and Zimmerman address cybersecurity threats to the DDM community. They provide a case study detailing a security assessment performed on an additive manufacturing system and present protocols and recommendations for security best practices for DDM systems.

In Chapter "The Resource Usage Viewpoint of Industrial Control System Security: An Inference-Based Intrusion Detection System", Nair et al. introduce cybersecurity mechanisms for Industrial Control Systems. Their premise is that one can infer CPU load by remotely profiling the network traffic emitted by an ICS device and use that inference to detect potentially malicious modifications to the behavior of the ICS device.

In Chapter "Practical Security Aspects of the Internet of Things", Mehnen et al. introduce a set of key security issues related to the implementation of the Internet of

Things (IoT) in an industrial mechanical engineering context. The authors provide a real-world example concerning remote maintenance of CNC machine tools, which illustrates the different threat scenarios related to IoT in practice. The authors detail various aspects of Big Data and Cloud Manufacturing but focus on improving security at the Edge of IoT, which is where data is collected, transmitted and eventually transferred back to the physical actuators. The authors' aim is to introduce a generic overview of real-world IoT security issues as well as giving a deeper technical example-supported insight into practical considerations for designing IoT systems for practical use in business.

Finally, the book concludes with Chapter "Cybersecurity for Industry 4.0 and Advanced Manufacturing Environments with Ensemble Intelligence". In this final chapter, Thames and Schaefer discuss how machine learning approaches using ensemble intelligence can be achieved. Particularly, the authors describe how cyberattack detection and response mechanisms were integrated into a Software-Defined Cloud Manufacturing architecture. The cyberattack detection algorithm described in this chapter is based on ensemble intelligence with neural networks whose outputs are fed into a neuro-evolved neural network oracle. The oracle produces an optimized classification output that is used to provide feedback to active attack response mechanisms within the software-defined cloud manufacturing system. The underlying goal of this chapter is to show how computational intelligence approaches can be used to defend critical Industry 4.0 systems as well as other Internet-driven systems.

This book is one of the first collections of works related to various aspects of Industry 4.0 and its cybersecurity needs. We hope you find it to be informative and useful for your cybersecurity and Industry 4.0 research efforts.

Atlanta, USA — Lane Thames, Ph.D.
Bath, UK — Prof. Dirk Schaefer
Winter 2016/2017

Contents

Contributors

Andrew Blyth Information Security Research Group, Faculty of Computing, Engineering and Science, University of South Wales, Wales, UK

Pete Burnap School of Computer Science and Informatics, Cardiff University, Cardiff, UK

X.T. Cai School of Computer Science and Technology, Wuhan University, Wuhan, China

Hui Cheng Shanghai Spaceflight Manufacture (Group) Co., Ltd., Shanghai, China

Yulia Cherdantseva School of Computer Science and Informatics, Cardiff University, Cardiff, UK

Peter Eden Information Security Research Group, Faculty of Computing, Engineering and Science, University of South Wales, Wales, UK

Kevin D. Fairbanks Unaffiliated Contributor, Laurel, MD, USA

Dominick Glavach Concurrent Technologies Corporation, Johnstown, PA, USA

James Graham True Secure SCADA, Goshen, KY, USA; Professor Emeritus (Electrical and Computer Engineering) for the University of Louisville, Louisville, KY, USA

Hongmei He Cranfield University, Bedfordshire, UK

Kevin Jones Cyber Operations, Airbus Group Innovations, Cyber, UK

Julia LaSalle-DeSantis Concurrent Technologies Corporation, Johnstown, PA, USA

W.D. Li Faculty of Engineering and Computing, Coventry University, Coventry, UK

Xiang Li Beijing Sysware Technology Co., Ltd., Beijing, China

Daphne Lopez School of Information Technology and Engineering, VIT University, Vellore, Tamil Nadu, India

X. Lu Faculty of Engineering and Computing, Coventry University, Coventry, UK

Gunasekaran Manogaran School of Information Technology and Engineering, VIT University, Vellore, Tamil Nadu, India

Jörn Mehnen University of Strathclyde, Glasgow, UK

Kashif Memon Information Security Institute, Johns Hopkins University, Baltimore, MD, USA

Rahul Nair Information Security Institute, Johns Hopkins University, Baltimore, MD, USA

Chinmohan Nayak Information Security Institute, Johns Hopkins University, Baltimore, MD, USA

Eli Ribble Authentise Inc., Sandy, UT, USA

William H. Robinson Security and Fault Tolerance (SAF-T) Research Group, Vanderbilt University, Nashville, TN, USA

Dirk Schaefer University of Bath, Bath, UK

Hugh Soulsby Cyber Operations, Airbus Group Innovations, Cyber, UK

Kristan Stoddart Department of International Politics, Aberystwyth University, Aberystwyth, UK

Revathi Sundarasekar Priyadarshini Engineering College, Vellore, Tamil Nadu, India

Nikolaos Tapoglou AMRC with Boeing University of Sheffield, Rotherham, UK

Stefano Tedeschi Cranfield University, Bedfordshire, UK

Lane Thames Tripwire Inc., Atlanta, GA, USA

Chandu Thota Albert Einstein Lab, Infosys Ltd, Hyderabad, India

Pengyuan Wang ECpE PowerCyber Lab, Iowa State University, Ames, IA, USA

S. Wang Faculty of Engineering and Computing, Coventry University, Coventry, UK

Xin Wang Department of Industrial and Manufacturing Systems Engineering, The University of Hong Kong, Hong Kong, China

Lanier Watkins Information Security Institute, Johns Hopkins University, Baltimore, MD, USA

Andre Wegner Core Digital Manufacturing Faculty for Singularity University, Nasa Research Park, Moffett Field, CA, USA; Authentise Inc., Sandy, UT, USA

Zhinan Zhang School of Mechanical Engineering, Shanghai Jiao Tong University, Shanghai, China

Scott Zimmerman Concurrent Technologies Corporation, Johnstown, PA, USA

Industry 4.0: An Overview of Key Benefits, Technologies, and Challenges

Lane Thames and Dirk Schaefer

Abstract A new revolution known as Industry 4.0 is occurring where countless elements comprising industrial systems are being interfaced with internet communication technologies to form the smart factories and manufacturing organizations of the future. Industry 4.0 and its associated technologies are currently being driven by disruptive innovation that promises to bring countless new value creation opportunities across all major market sectors. However, existing Internet technologies are plagued by cybersecurity and data privacy issues that will present major challenges and roadblocks for adopters of Industry 4.0 technologies. Industry 4.0 will face traditional cybersecurity issues along with its very own unique security and privacy challenges. If these challenges are not appropriately addressed, the true potential of Industry 4.0 may never be achieved. This chapter provides a brief overview of several key Industry 4.0 technologies and paradigms in order to give the reader a better understanding of the cybersecurity aspects of the remaining chapters in the book.

1 Introduction: Background and Motivation

A transformative event known as Industry 4.0 is occurring where countless elements comprising industrial systems are being interfaced with internet communication technologies to form the smart factories and manufacturing organizations of the future. Industry 4.0 and its associated technologies such as cloud-based design and manufacturing systems, the Internet of Things, the Industrial Internet of Things, and Social-Product Development are currently being driven by disruptive innovation that promises to bring countless new value creation opportunities across all major market sectors. However, existing Internet technologies are plagued by cybersecurity and data privacy issues that will present major challenges and roadblocks for

L. Thames (✉)
Tripwire, Inc., Atlanta, GA, USA
e-mail: lthames@tripwire.com

D. Schaefer
University of Bath, Bath, UK
e-mail: d.schaefer@bath.ac.uk

L. Thames and D. Schaefer (eds.), *Cybersecurity for Industry 4.0*,
Springer Series in Advanced Manufacturing, DOI 10.1007/978-3-319-50660-9_1

adopters of Industry 4.0 technologies. Industry 4.0 will face traditional cybersecurity issues along with its very own unique security and privacy challenges. If these challenges are not appropriately addressed, the true potential of Industry 4.0 may never be achieved.

A significant obstacle faced by those in Industry 4.0 related to cybersecurity is that of integration and cooperation amongst the stakeholders of any given Industry 4.0 organization. The core of this obstacle is that of language. Particularly, Industry 4.0 environments are made of diverse technologies spread across many disciplines with many different types of subject matter experts, but there are few standards and processes designed to assist each entity to speak a "common language" that appropriately aligns necessary objectives related to cybersecurity. For example, on the manufacturing side we have control engineers working with Operational Technology (OT). Similarly, on the Information Technology (IT) side we have system administrators working with traditional IT assets such as servers and software. On the one hand, a control engineer when dealing with securing OT assets is mostly concerned with 'mission assurance'. On the other hand, an IT system administrator is concerned with 'information assurance'. These objectives rarely align with one another. For example, a control engineer doesn't care about data loss over human life or machinery loss whereas a system administrator would never think about air gapping his battery backup units (UPS) for his servers. The drivers underlying these cybersecurity objects are vast and very different across domains. However, Industry 4.0 demands that these systems be integrated across all dimensions.

A primary goal of this book is to shed light on these aforementioned types of obstacles, needs, technologies and such as related to Industry 4.0 and cybersecurity. As alluded to in the previous paragraph, when approaching this subject, stakeholders need to understand the bigger picture. As such, the purpose of this chapter is to provide the reader with an overview of key technologies and paradigms related to Industry 4.0. The remainder of the book will emphasize cybersecurity aspects of Industry 4.0.

2 Industry 4.0 and Smart Manufacturing

Industry 4.0 is sometimes referred to as the 4th industrial revolution, and it is a vision of smart factories built with intelligent cyber-physical systems. It will enable manufacturing ecosystems driven by smart systems that have autonomic self-properties, for examples self-configuration, self-monitoring, and self-healing. Industry 4.0 will allow us to achieve unprecedented levels of operational efficiencies and accelerated growth in productivity. New types of advanced manufacturing and industrial processes revolving around machine-to-human collaboration and symbiotic product realization will emerge.

Industry 4.0 will encompass numerous technologies and associated paradigms. A few of these emerging paradigms include the Industrial Internet and the Industrial Internet of Things along with new 21st century product development paradigms such as cloud-based design, cloud-based manufacturing, crowd sourcing, and open innovation to name a few. A brief overview of these paradigms is provided in the following sections.

2.1 Industrial Internet and the Industrial Internet of Things

A new revolution is occurring within industry. It is a revolution resulting from the convergence of industrial systems with advanced computing, sensors and ubiquitous communication systems. It is a transformative event where countless industrial devices, both old and new, are beginning to use Internet Protocol (IP) communication technologies. We refer to this new revolution as the Industrial Internet of Things. The Industrial Internet of Things is a subset of what we have come to know as the Internet of Things (IoT). The IoT is an abstract idea that captures a movement that started when we began integrating computing and communication technology into many of the "things" that we use at home and work. It started with the idea of tagging and tracking "things" with low cost sensor technologies such as radio frequency identification (RFID) devices. However, the paradigm shifted as the market began delivering low-cost computing and Internet-based communication technologies, simultaneously with the rise of the ubiquitous smartphone.

This perfect storm of low cost computing and pervasive broadband networking has allowed the IoT to evolve. Now, the IoT includes all types of devices ranging from home appliances, light bulbs, automation systems, watches, to even our cars and trucks. Technically speaking, the IoT is a collection of physical artifacts that contain embedded systems of electrical, mechanical, computing and communication mechanisms that enable Internet-based communication and data exchange.

The Industrial IoT follows the same core definition of the IoT, but the things and goals of the Industrial IoT are usually different (see Fig. 1). Some examples of the things of the Industrial IoT include devices such as sensors, actuators, robots, manufacturing devices such as milling machines, 3D-printers, and assembly line components, chemical mixing tanks, engines, healthcare devices such as insulin and infusion pumps, and even planes, trains, and automobiles. Indeed, it is a vast spectrum of devices.

One interesting aspect of Industrial IoT devices is system complexity. In particular, Industrial IoT devices can contain systems of IoT systems. For example, an industrial robot as a whole might contain multiple sensors working both independently and as a group, and one or more of these sensors could control one or more actuators that, in turn, control the robots movement. Further, the sensors, actuators, and other parts of the robot can connect independently to an IP network with some centralized server that governs the overall control of the robot. Another term commonly used when discussing the Industrial IoT, and in particular, the Industrial Internet, is operation technology. Operation technology (OT) refers to the traditional hardware and software systems found within industrial environments. Some examples include programmable logic controllers (PLC), distributed control systems (DCS),

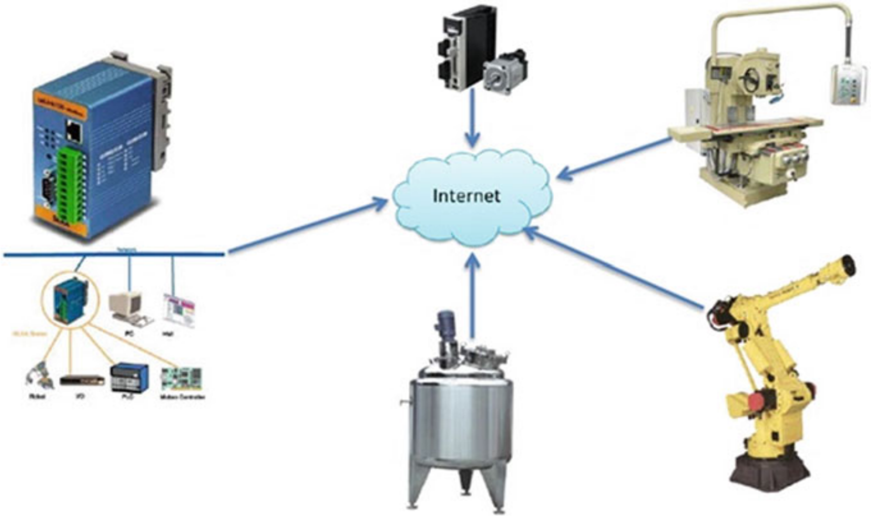


Fig. 1 Abstract idea of the industrial IoT

and human-machine interfaces (HMI). These systems are also known as Industrial Control Systems (ICS) because they control the various processes that occur within an industrial environment.

The Industrial IoT is a subset of the more general IoT. Hence, some of their characteristics are similar. The most common characteristic is that they all contain embedded computing and communication technology. These systems are largely focused on sensor technology along with the collection, transmission, and processing of sensory data. Communication is obviously a key component of the Industrial IoT. As illustrated by Fig. 2, the Industrial IoT can use both wired and wireless

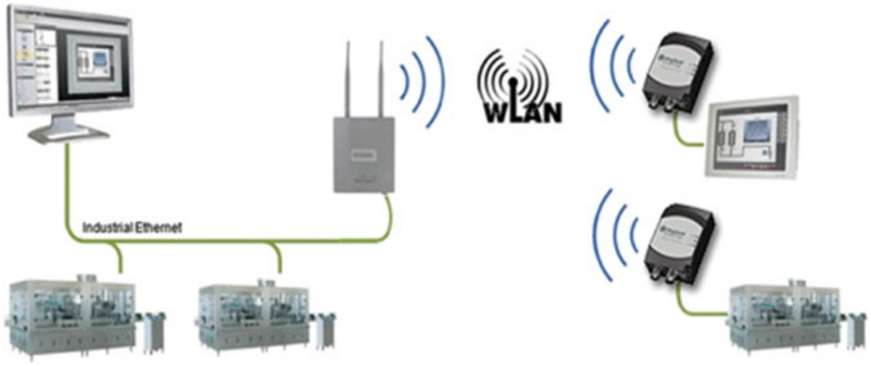


Fig. 2 An example of industrial IoT communication architecture

communication. Some of the protocols used by Industrial IoT devices include Ethernet, Wi-Fi, WiMax, LR-WPAN, 2G/3G/4G telephony, IPv4, IPv6, 6LoWPAN, HTTP, CoAP, MQTT, XMPP, DDS, and AMQP, Profinet, ModBus, and DNP. There are different protocols for different use cases, commonly driven by environmental factors and resource constraints. For example, HTTP and MQTT are application layer protocols. HTTP, the hyper-text transport protocol, is a text-based protocol commonly used by web-based systems, i.e., web servers. It is a good protocol for client-server communications when there is more of a need to do only one-way data pulling. Although multiple sets of data packets moving in both directions are required for a client to pull down a web page from a server, the protocol is designed for pure client-server architectures. However, it is common for IoT devices to act as both client and servers. In these cases, HTTP is more difficult to implement, although it can be done using a polling methodology. MQTT was designed specifically for industrial network environments. It is a publish-subscribe messaging protocol, which eases the pain in terms of two-way communications where a device might act as both a client and server. Further, it is a light weight protocol in terms of transmission overhead, and it was designed to support lossy data transmission networks.

The Industrial Internet of Things will drastically change the future, not just for industrial systems, but also for the many people involved. If we can achieve the full potential of the Industrial IoT vision, many people will have an opportunity to better their careers and standards of living because the full potential of this vision will lead to countless value creation opportunities. This always happens when new revolutions get set into motion. The full potential of the Industrial IoT will lead to smart power grids, smart healthcare, smart logistics, smart diagnostics, and numerous other smart paradigms. For example, the Industrial IoT is at the heart of a related movement called Industry 4.0. Industry 4.0 is sometimes referred to as the 4th industrial revolution, and it is a vision of smart factories built with intelligent cyber-physical systems. It will enable manufacturing ecosystems driven by smart systems that have autonomic self-* properties such as self-configuration, self-monitoring, and self-healing. This is technology that will allow us to achieve unprecedented levels of operational efficiencies and accelerated growth in productivity. New types of advanced manufacturing and industrial processes revolving around machine-to-human collaboration and symbiotic product realization will emerge. It will truly be amazing to see all of the many benefits and technological advances that can be gained if we can achieve the full potential of this technology.

The Industrial Internet of Things can have a bright and shiny future. However, the devil is in the details. The number one challenge faced by the Industrial IoT is security and privacy. Cybersecurity and data privacy issues present major hurdles and roadblocks for adopters of Industrial IoT technologies. If we cannot alleviate many of the security and privacy issues that impact the Industrial IoT, we will not be able to achieve its full potential.

2.2 New 21st Century Product Development Paradigms

The force of globalization has served to instantaneously connect people from all across the globe, bringing with it game-changing opportunities to share knowledge and expertise to benefit in a collective manner (sometimes called share-to-gain). Friedman (2005) explains that the latest globalization phase, which he coins Globalization 3.0, began around the year 2000 and was enabled by the expansion of the internet on a global basis during the dot-com boom. According to Friedman, Globalization 3.0 is defined by individuals and small groups from across the globe collaborating in areas once dominated by less-connected western economies.

Tapscott and Williams (2008) explain that the advent of the internet has led to the development of cooperative collaboration networks, resulting in a power-shift from the once mighty hierarchical business model. These traditional business models, according to the authors, can no longer sustain successful innovation: "In an age where mass collaboration can reshape an industry overnight, the old hierarchical ways of organizing work and innovation do not afford the level of agility, creativity, and connectivity that companies require to remain competitive in todays environment." Simply put, industry is going to have to rethink the traditional models of business operation, as the amount of internal expertise they hold is dwarfed by that held by the global mass of peoples connected through globalization.

In academia and industry, the Pahl and Beitzs (1988) systematic design approach and Suhs (2001) Axiomatic Design theory are two of the most widely accepted design methodologies. Pahl and Beitz describe the product development process as a series of core transformations, from problem description to requirements list, to principal solutions and working structures, to preliminary design, to detailed layouts, and to final layout, form/dimensions, and manufacturing specifications. The design activities are classified into: product planning, conceptual design, embodiment design, and detail design. Suhs Axiomatic Design is a systematic design methodology based on matrix methods to analyze the transformation of customer needs into functional requirements, design parameters, and process variables.

However, neither Pahl and Beitzs design method nor Suhs Axiomatic Design theory offers a framework that facilitates seamless information, knowledge, and resource sharing, or aids participants of global value co-creation networks in identifying potential collaboration partners or resource providers (Franke et al. 2006). For example, value can be co-created when the participants of such networks identify information, knowledge, and manufacturing resources that are more cost effective than existing ones. The motivation of the research presented in this chapter is to bridge the gap between traditional product development methods and new methods that are required in the globalized world in which paradigms such as crowd-sourcing, mass collaboration and social product development are the order of the day. We begin by giving an overview of these paradigms.

In light of a continuing globalization alluded to above, product development is not only becoming increasingly complex and dynamic but also significantly more competitive. More and more of the skills and industries that traditionally fueled the economic prosperity of our nation are becoming the commodities of today and tomorrow. In addition, new product development paradigms and associated competencies required to successfully compete in the “flat” world are emerging at a mind-boggling rate of speed. Some of these new paradigms can be considered real game changers and are worth a closer look.

Complex social networks, consisting of millions of individuals, have formed over the Internet through emerging Web 2.0 technologies such as blogs, discussion boards, wikis, and collaboration networks such as Facebook or LinkedIn, video networks such as YouTube, and countless others. Information on almost anything is readily available to everyone through the Web, anytime and anywhere. Individuals, who have never met physically, are already collaborating on the development of complex products and services for major companies, collectively solving challenging problems that are openly “crowd sourced” to a community of interested engineers, scientists, and even hobbyists. While this may sound weird to some of us, for the next generation of engineers, it will be the norm. Their number one material to work with will be information, their final product(s) will be intellectual property and innovation, and their generation is already becoming known as the generation of knowledge workers.

Globalization 3 has led to the emergence of various game-changing paradigms anticipated to foster breakthrough innovation. These paradigms are characterized by the self-organization of individuals into loose networks of peers to produce goods and services in a very tangible and ongoing way. These paradigms include, among others, crowd-sourcing, mass collaboration, and open innovation. Enabling technologies for these paradigms include first and foremost the Internet, social networking platforms for business, cloud computing, as well as new business philosophies, such as “share to gain”. New organizational structures based on self-organizing communities are emerging to complement traditional hierarchies. According to Tapscott and Williams (2008), new principles for success in the globalized world are (a) openness to external ideas, (b) individuals as peers, (c) sharing of intellectual property, and (d) global action. In such emerging organizations, individual success is defined by the recognition gained through contributions towards a common goal rather than by following the directions from the top management. An organization’s success is determined by its ability to integrate talents of dispersed individuals and other organizations.

Crowd sourcing is defined as “the act of sourcing tasks traditionally performed by specific individuals to a group of people or community (crowd) through an open call” (Wikipedia 2017). Because it is an open call to a group of people, it attracts those who are most fit to perform tasks or solve problems, and provide fresh and innovative ideas. This way, a significantly higher talent pool than the one any company could possibly have can be tapped. Procter & Gamble, for example, created their own platform for this, called Connect + Develop, years ago.

Closely related to crowd sourcing is the paradigm of mass collaboration. Here, the idea is to harness the intelligence and ideas of many (or the crowd), to find innovative solutions to complex problems. Mass collaboration can be defined as “a form of collective action that occurs when large numbers of people work independently on a single project, often modular in its nature. Such projects typically take place on the Internet using social software and computer-supported collaboration tools such as wiki technologies, which provide a potentially infinite hyper-textual substrate within which the collaboration may be situated" (Wikipedia 2017). While the online encyclopedia Wikipedia may be one of the most prominent examples for a mass-collaborative project, there are many other examples of projects related to the development of real world products in this fashion.

The two preceding paradigms are considered to foster Open Innovation, a term coined by Henry Chesbrough (2003). According to his definition, open innovation is "a paradigm that assumes that firms can and should use external ideas as well as internal ideas, and internal and external paths to market, as the firms look to advance their technology". He also states that "...the central idea behind open innovation is that in a world of widely distributed knowledge, companies cannot afford to rely entirely on their own research, but should instead buy or license processes or inventions (i.e. patents) from other companies. In addition, internal inventions not being used in a firms business should be taken outside the company (e.g. through licensing, joint ventures or spin-offs)". This is closely related to what others refer to as share-to-gain. Crowd sourcing, mass collaboration and open innovation certainly have a number of appealing characteristics. However, there are two major issues that currently make companies shy away from these new paradigms. One is intellectual property (IP), which can be tricky waters to navigate, especially on a global level. The second one is a lack of new business models to go along with the new paradigms. Companies still need to make money, and while everyone will agree that putting together an online encyclopedia in a share-to-gain fashion is a neat thing to do, designing and manufacturing, for example, cars and airplanes that way isnt quite that straight forward.

The technical and enabling backbones for these new paradigms are the Web and the Internet, which has grown into a huge "supercomputer" that is continuously getting smarter, i.e., capable of responding to its semantic surroundings, for the world to share. Today, a myriad of software packages to facilitate all sorts of online collaboration, both for professional as well as personal purposes, are available. They range from simple video communication tools such as Skype to more complex collaboration suits like Wiggio, up to full-blown product design solutions, such as Dassault Systems CATIA V6 in concert with their cloud-based collaboration platform SwYm.

Cloud computing, originally conceptualized in the 1960s, is a fancy marketing term for networked computers that provide services (or resources) through the Internet to a network of clients who utilize them, usually on a pay-as-you-go cost model. The three most prominent cloud computing application areas are Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). Clouds can be public, private, or a hybrid in nature. In other words, companies may choose to implement their own internal cloud as a Local Area Network (private cloud), use the cloud-infrastructure from a third-party provider (public cloud), or opt for a hybrid for example, to rent and run software as a service in the public cloud and store application data in a local, private cloud.

Recently, cloud computing has made its advent to the domain of computer-aided product development. In addition to running CAD systems as a service in the cloud, other business-related everything-as-a-service models have started to emerge. One such model relates to manufacturing and aims at utilizing physical resources, for example, 3D printers for additive manufacturing, mills, lathes, and other manufacturing-related equipment, through the cloud. Long-term, computer-aided product development in general (including design, analysis and simulation, as well as manufacturing) is anticipated to become predominantly cloud-based. It is a promising new model to facilitate globally distributed design and manufacture processes that seamlessly integrate both virtual and physical resources. In the next section, we provide a discussion of cloud-based design and manufacturing (CBCM) that seeks to enhance the Industry 4.0 paradigm by harnessing the power of crowdsourcing, open innovation, and mass collaboration along with technologies such as cloud computing, the Internet, and the web as a new 21st Century Product Development Paradigm.

3 Cloud-Based Design and Manufacturing

Before introducing CBDM and identifying its key characteristics, we first review some of the existing definitions of cloud computing:

- Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction (NIST 2011).
- Cloud computing refers to both the applications delivered as services over the internet and the hardware and systems software in the datacenters that provide those services. The services themselves have long been referred to as Software as a Service (SaaS). The datacenter hardware and software is what we will call a Cloud (Armbrust et al. 2010).
- Clouds are a large pool of easily usable and accessible virtualized resources (such as hardware, development platforms, and/or services). These resources can be dynamically reconfigured to adjust to a variable load (scale), allowing also for an optimum resource utilization. This pool of resources is typically exploited by a pay-per-use model in which guarantees are offered by the infrastructure provider by means of customized SLAs (Vaquero et al. 2009).
- A cloud is a type of parallel and distributed system consisting of a collection of interconnected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resources based on service-level agreements established through negotiation between the service provider and consumers (Buyya et al. 2008).
- Cloud computing is both a UX and a business model. It is an emerging style of computing in which applications, data and IT resources are provided to users as services delivered over the network. It enables self-service, economies of scale

> and flexible sourcing options an infrastructure management methodology—a way of managing large numbers of highly virtualized resources, which can reside in multiple locations...(IBM 2010).

From above, a number of well-known and widely cited definitions of cloud computing are presented. Here, we put these ideas in a historical perspective in order to understand the origin of cloud computing, where it comes from, and its evolution. While the term cloud computing was only coined in 2007, the concept behind cloud computing, delivering computing resources through a global network, was rooted in 1960s (Licklider 2010). The term "Cloud" is often used as a metaphor for the Internet, and refers to both hardware and software that deliver applications as services over the Internet (Armbrust et al. 2010). When looking backward, one realizes that cloud computing is based on a set of pre-existing and well researched concepts such as utility computing, grid computing, virtualization, service oriented architecture, and software-as-a-service (Bohm 2010). One milestone is utility computing, proposed by John McCarthy in 1966. The idea of utility computing is that "computation may someday be organized as a public utility". Due to a wide range of computing related services and networked organizations, utility computing facilitates integration of IT infrastructure and services within and across virtual companies (Parkhill 1966). Another milestone is that Ian Foster and Carl Kesselman proposed the concept of grid computing in 1999. A computational grid refers to a hardware and software infrastructure that provides dependable, consistent, pervasive, and inexpensive access to high-end computational capabilities (Foster and Kesselman 1999). Since cloud and grid computing share a similar vision, Foster et al. (2008) identified the main differences between grid computing and cloud computing. The greatest difference is that cloud computing addresses Internet-scale computing problems, utilizing a large pool of computing and storing resources, whereby grid computing is aimed at large-scale computing problems by harnessing a network of resource-sharing commodity computers, dedicating resources to a single computing problem.

Compared to grid computing, we envision that cloud computing would be the most promising underlying concept that can be borrowed in the fields of design and manufacturing due to the advantages of greater flexibility, ubiquitous availability of high capacity networks, low cost computers and storage devices as well as service-oriented architecture. Thus, before exploring CBDM in more detail, it is worthwhile to take a close look at what make cloud computing unique and how it is being leveraged in design and manufacturing fields.

Cloud computing can be seen as an innovation from different perspectives. From a technical perspective, it is an advancement of computing history that evolved from calculating machines with binary digit systems, to mainframe computers with floating-point arithmetic, to personal computers with graphical user interfaces and mobility, to the Internet that offers computing resources via distributed and decentralized client-server architectures, and eventually to utility, grid, and cloud computing (Boem et al. 2010). From a business perspective, it is a breakthrough which is changing the mode of IT deployment and potentially creating new business models.

In order to leverage cloud computing in existing manufacturing business models and enterprise information systems, cloud manufacturing, based on cloud computing and service-oriented technologies, is proposed (Tao et al. 2011). The architecture, core enabling technologies, typical characteristics for cloud manufacturing, and the difference and relationship between cloud computing and cloud manufacturing has been discussed. Xu (2012) discusses the potential of cloud computing that can transform the traditional manufacturing business models by creating intelligent factory networks. Two types of cloud computing adoptions in the manufacturing sector have been suggested, direct adoption of cloud computing technology in the IT area and cloud manufacturing where distributed resources are encapsulated into cloud services and managed in a centralized manner.

4 Defining Cloud-Based Design and Manufacturing (CBDM)

Based on the concept of cloud computing, we propose a definition of CBDM as follows (Wu et al. 2012):

Cloud-Based Design and Manufacturing refers to a product realization model that enables collective open innovation and rapid product development with minimum costs through a social networking and negotiation platform between service providers and consumers. It is a type of parallel and distributed system consisting of a collection of inter-connected physical and virtualized service pools of design and manufacturing resources (e.g., parts, assemblies, CAD/CAM tools) as well as intelligent search capabilities for design and manufacturing solutions.

Figure 3 illustrates the concepts underlying the foundations and principles of CBDM systems aligned with our proposed definition thereof. At this point, it is noteworthy to explain the use of the term Cloud. Communication and network engineers have traditionally encapsulated the inherent interconnection complexity of networks with cloud diagrams. In essence, a network of any reasonable size is too complex to draw on a diagram. Consequently, cloud diagrams are used to hide the interconnect complexity while simultaneously revealing the primary details of a particular network diagram. As seen from Fig. 3, the Internet communication cloud forms the basic and required underlay network for any CBDM system in general. As stated previously, CBDM technologies are enabled by Internet-based information and communication technologies. This dependency is represented by illustrating CBDM as an overlay in Fig. 3. Moreover, Fig. 3 seeks to illustrate the overall and basic interconnectivity of the primary elements of a CBDM system. For example, the human resources of a CBDM system form their own human-centric network, which is represented by design teams, social networks, and students, just to name a few. Likewise, the cloud resources, which include human, virtual, and physical resources, are

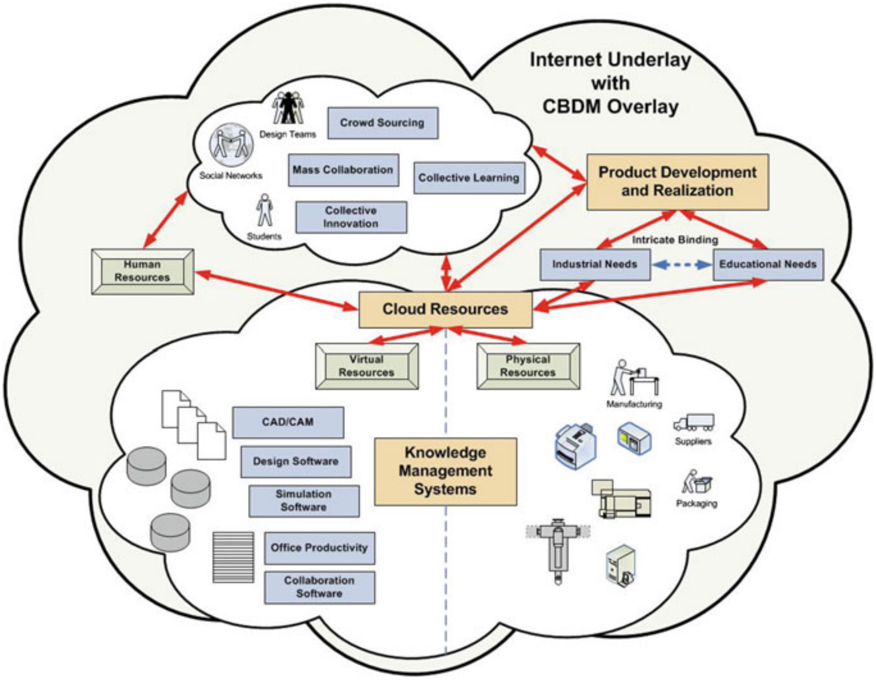


Fig. 3 The CBDM concept

illustrated along with their appropriate partitions. One of the primary goals of CBDM is to enable efficient product development and realization processes. Hence, appropriate interconnections are established between this goal and the basic partitions of the diagram. Further, one should observe the needs of the product development and realization process: namely, industrial needs and educational needs. These two sectors comprise the basic categories of entities that need the CBDM functionality. Moreover, industrial needs and educational needs are, in general, intricately bound. Industry will use CBDM technology to produce raw goods and services. Obviously, industry depends on educational entities for the following: (1) to educate students on the basic principles and foundations of CBDM systems in order to accomplish their economic goals and (2) to conduct cutting-edge research and development on the underlying details of CBDM systems. Hence, the educational and industrial entities are intricately bound.

In addition, the essential characteristics of CBDM, including on-demand self-service, ubiquitous network access, rapid scalability, resource pooling, and virtualization are emphasized as prerequisites to enable CBDM as follows:

- On-demand self-service: A customer or any other individual participating in the cloud can provide and release engineering resources, such as design software, manufacturing hardware, as needed on demand. It provides a platform and intuitive, user-friendly interfaces that allow users (e.g., designers) to interact with other users (e.g., manufacturers) on the self-service basis.

- Ubiquitous network access: There is an increasing need for a so-called customer co-creation paradigm, which enables designers to proactively interact with customers, as well as customers to share different thoughts and insights with designers. In order to easily reach such a communication media, it requires a capability of broad and global network access. The CBDM systems can provide such access to the network where cloud consumers reside through multiple tools, e.g., mobile phones and personal digital assistants. CBDM allows various stakeholders (e.g., customers, designers, managers) to participate actively throughout the entire product realization process.
- Rapid scalability: The CBDM systems allow enterprises to quickly scale up and down, where manufacturing cells, general purpose machine tools, machine components (e.g., standardized parts and assembly), material handling units, as well as personnel (e.g., designers, managers, and manufacturers) can be added, removed, and modified as needed to respond quickly to changing requirements. It helps to better handle transient demand and dynamic capacity planning under emergency situations incurred by unpredictable customer needs and reliability issues. For example, the cloud system allows the cloud service consumers to quickly search for and fully utilize resources, such as idle and/or redundant machines and hard tools, in another organization to scale up their manufacturing capacity.
- Resource pooling: The cloud providers design and manufacturing resources are pooled to serve cloud consumers in a pay-per-use fashion. Resources include engineering hardware (e.g., fixtures, molds, and material handling equipment) and software (e.g., computer-aided design and Finite Element Analysis (FEA) program packages). The CBDM model enables convenient and on demand network access to such a shared pool of configurable manufacturing resources. The real time sensor inputs, capturing the status and availability of manufacturing resources, ensures effective and efficient cloud resource allocation.
- Virtualization: The CBDM systems provide a virtual environment through the simulation of the software and/or hardware upon which other software runs. It enables enterprises to separate engineering software packages, computing and data storage resources from physical hardware, as well as to support time and resource sharing.

4.1 Cloud Based Design

Cloud Based Design (CBD) is a part of the CBDM concept with a focus on design aspects. CBD refers to a design model that leverages Web 2.0 (i.e., social network sites, wikis, online reviews, and recommender systems) and Web 3.0 to support the gathering, representation, processing, and use of product design-related information that is distributed across social media and the Internet (Wu et al. 2013).

Traditionally, it has been assumed that generating design ideas and implementing them was the exclusive task of design teams. However, CBD has the potential to enable customers, engineers, and other participants to share information through social media by integrating Web 2.0 tools into product design processes. For example, a Web 2.0 site provides service providers and consumers a vehicle to communicate and interact with each other through online product reviews. In this way, designers can easily get feedback on their customers user experience.

In addition, due to the vast amount of product design-related data in social media, engineers are facing a significant challenge in quickly find the information they need. Web 3.0 allows the information to be precisely described in terms of ontology that can be understood by machines. Web 3.0 will support effective and efficient discovery, automation, and reuse of data for CBD.

4.2 Cloud Based Manufacturing

Cloud based manufacturing (CBM) is the other part of the CBDM concept with a focus on the manufacturing aspect. CBM refers to "a customer-centric manufacturing model that exploits on-demand access to a shared collection of diversified and distributed manufacturing resources to form temporary, reconfigurable production lines which enhance efficiency, reduce product lifecycle costs, and allow for optimal resource loading in response to variable-demand customer generated tasking". (Wu et al. 2013) the motivation for introducing CBM is based on the belief that CBM can lead to important advances in new ways of conducting manufacturing activities from the following perspectives.

First, one of the main reasons for the adoption of CBM by manufacturing enterprises is the emerging outsourcing and crowd sourcing models in manufacturing. CBM may (1) facilitate Small and Medium-Sized Enterprises (SMEs) run manufacturing operations more cost effectively by utilizing excessive manufacturing resources owned by large enterprises; and (2) enable large sized enterprises to develop and enhance their core competencies and innovation capabilities by crowd-sourcing labor-intensive tasks.

Second, one of the distinguishing characteristics of CBM is that CBM allows enterprises to quickly scale up and down, where manufacturing cells, general purpose machine tools, machine components (e.g., standardized parts and assembly), material handling units, as well as personnel (e.g., designers, managers, and manufacturers) can be added, removed, and modified as needed to respond quickly to changing requirements.

4.3 CBDM Services

Figure 4 presents some example CBDM cloud services available to a cloud consumer.

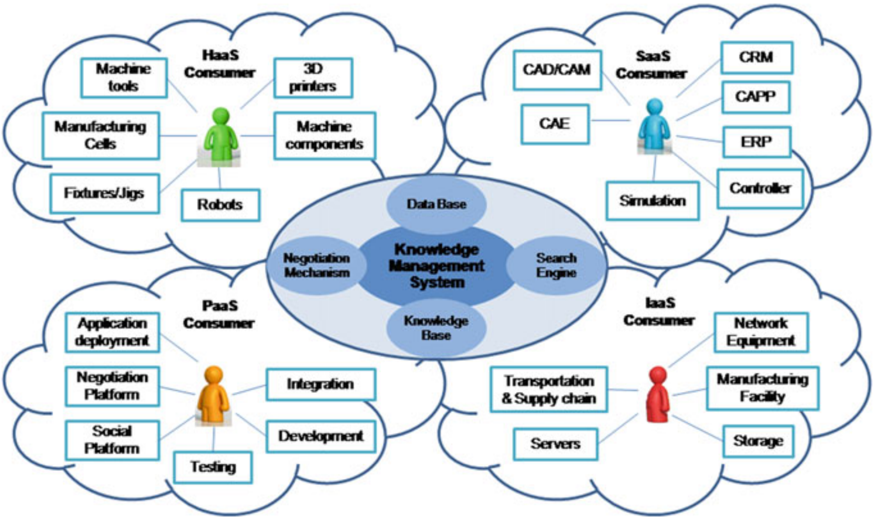


Fig. 4 CBDM example services

Hardware-as-a-Service (HaaS): HaaS delivers hardware sharing services, e.g., machine tools, hard tooling, and manufacturing processes, to cloud consumers through the CBDM system. Cloud consumers are able to rent and release hardware provided by a third party without purchasing them. The Cubify.com 3D online printing service is a good example, which allows cloud consumers to produce parts through any mobile device using their online 3D printing service without purchasing 3D printers. The consumers of HaaS could be either engineers or end users, who may utilize manufacturing hardware.

Software-as-a-Service (SaaS): SaaS delivers software applications, e.g., CAD, CAM, FEA tools, and Enterprise Resource Planning (ERP) software to cloud consumers. Cloud consumers are able to install and run engineering and enterprise software through a thin client interface without purchasing full software licenses. The cloud service offered by Dassault Systems and Autodesk are by far the best known examples among engineering analysis applications, allowing remotely running 3D software and high performance discrete computing environments (Autodesk 2017; Dassault 2017). The consumers of SaaS can be designers, engineers and managers, who need access to software applications.

Platform-as-a-Service (PaaS): PaaS provides an environment and a set of tools (e.g., an interactive virtual social platform, a negotiation platform, and a search engine for design and manufacturing solutions) to consumers and application developers to assist them in integrating and delivering the required functionality. A good example is Fujitsu, providing a high-speed thin client environment, server consolidation, and license consolidation, which dramatically reduces manufacturing costs and development times by leveraging a knowledge base in the cloud (Fujitsu 2017).

Infrastructure-as-a-Service (IaaS): IaaS provides consumers with fundamental computing resources, e.g., high performance servers and storage space. These services are offered on a pay-as-you-go basis, eliminating downtime for IT maintenance as well as reducing costs dramatically. The consumers of IaaS could be engineers and managers, who need access to these computing resources.

5 CBDM: A First Generation Implementation

Generally speaking, the integration of Information Technologies systems (IT) with Operation Technology (OT) systems is crucial for the success of Industry 4.0. This is true from a core technology perspective, and IT/OT integration also happens to be a key challenge for the cybersecurity aspects of Industry 4.0. We will discuss the cybersecurity aspects of IT/OT integration for Industry 4.0 later in this chapter. For now, we will discuss it within the context of core Industry 4.0 technologies and how it applies to our real world experience while implementing our first generation CBDM system.

Figure 5 illustrates the ideas of IT and OT convergence. What does it mean to converge IT with OT? First, let's consider the underlying components. Operation technology refers to the traditional hardware and software systems found within

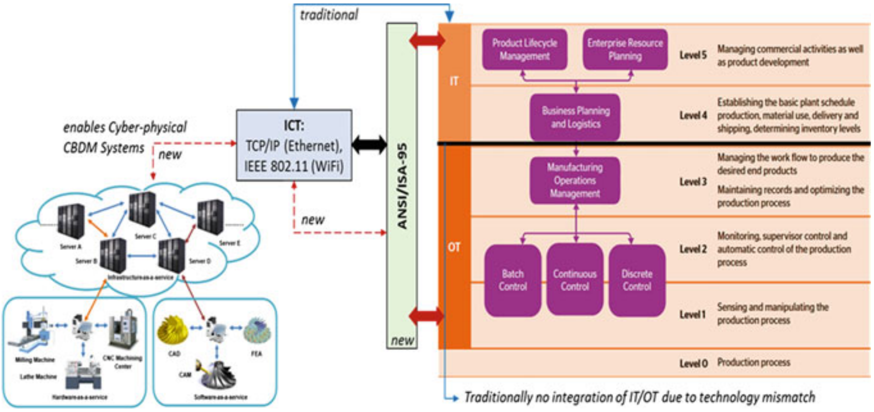

traditional
enables Cyber-physical
CBDM Systems
new
ICT:
TCP/IP (Ethernet),
IEEE 802.11 (WiFi)
new
ANSI/ISA-95
new
Server A
Server B
Server C
Server D
Server E
Infrastructure-as-a-service
Milling Machine
Lathe Machine
CNC Machining Center
Hardware-as-a-service
CAD
FEA
CAM
Software-as-a-service
IT
OT
Product Lifecycle Management
Enterprise Resource Planning
Business Planning and Logistics
Manufacturing Operations Management
Batch Control
Continuous Control
Discrete Control
Level 5
Managing commercial activities as well as product development
Level 4
Establishing the basic plant schedule production, material use, delivery and shipping, determining inventory levels
Level 3
Managing the work flow to produce the desired end products
Maintaining records and optimizing the production process
Level 2
Monitoring, supervisor control and automatic control of the production process
Level 1
Sensing and manipulating the production process
Level 0
Production process
Traditionally no integration of IT/OT due to technology mismatch

Fig. 5 The idea of IT and OT convergence

industrial environments. Some examples include programmable logic controllers (PLC), distributed control systems (DCS), and human-machine interfaces (HMI). These systems are also known as Industrial Control Systems (ICS) because they control the various processes that occur within an industrial environment. Information technology generally refers to the software, servers, personal computers, mobile phones, and such that comprise the business side of an organization. Convergence of IT and OT relates to the interconnection of these systems using modern networking technologies such as Ethernet and IP networking. You see, traditionally, OT systems where 'air gapped' from IT networks. OT systems commonly used proprietary and/or specialized communication protocols and didn't come equipped with networking that was compatible with those of the IT networks. Recently, however, OT systems have rapidly been adopting standards such as WiFi, Ethernet, and IP networking. As such, many enterprises have been connecting OT systems with their IT systems. There are many different schools of thought as to whether this is good or bad. Regardless, having OT systems connected to our IT systems is rapidly becoming the norm and will drive future cyber physical designs for Industry 4.0 stakeholders.

The development of our first generation CBDM prototype was achieved while working on a DARPA research project called Manufacturing Experimentation and Outreach (MENTOR). MENTOR was a sub-project of the DARPA Adaptive Vehicle Make (AVM) program. The overall objectives of these research programs were to aid designers in managing system complexity and in reducing product development time and effort. Our research and development efforts for MENTOR was to develop a prototype infrastructure that served as an enabling platform for the deployment of a variety of programmable manufacturing equipment, such as 3D printers, to over 1000 high schools throughout the country and to orchestrate a series of prize-based challenges to encourage competition and collaboration within high school teams as they design and build cyber-electro-mechanical systems. Figure 5 once again illustrates the basics of our IT/OT integration challenge. The left side of the figure reveals our overall objectives: the need to integrate manufacturing equipment along with software such as CAD programs into an IT architecture. The right side of the figure reveals the functional levels across the IT and OT sides. The figure does not reveal, however, the complexity of the challenge we faced with MENTOR. You see, IT and OT integration within a **single** organization is very challenging. The integration of IT and OT systems across many diverse organizations (i.e., 1000+ high schools) is exponentially challenging due to differing IT and OT governance issues across the independent organizations. As such, we had to develop an systems model and CBDM system that would enable seamless integration of IT and OT systems across organizational boundaries. We solved this issue using a hybrid distributed-centralized system model that formed the basis of our first generation CBDM system. The next few sections describe our model, architecture, and implementation details.

5.1 An Infrastructure for Distributed Collaborative Design and Manufacturing Inspired by the Cloud Computing Paradigm

In general, an infrastructure is a system of assets such as physical components, human resources, operational processes, and organizational structures required to facilitate a particular set of outcomes. For example, a countrys transportation infrastructure facilitates the delivery of raw goods, in which raw goods are used to produce products, in which products are then delivered to consumers. Naively, one might assume that the transportation infrastructure consists simply of a countrys network of roadways. However, the transportation infrastructure is more complex than just the roadway network. Instead, it consists of the roadway network system, the system of organizations producing raw goods, the system of organizations who produce products from the raw goods, the organizations who deliver the products and raw goods, and the consumers of the final product. It is easy to argue that an infrastructure is a complex System of systems. One particular concept common to any infrastructure is that the infrastructures system of assets are employed for the purpose of combining problem holders with problem solvers to produce some set of outcomes that facilitate the solution for the underlying need implied by the necessity of the infrastructure. An infrastructure is a collection (system) of assets that collectively produce a set of desired outcomes, which would not be attainable by any particular asset alone. The value added by the infrastructure is determined by the interconnection of its assets, which is the interconnection between problem holders and problem solvers.

We have developed a distributed infrastructure with centralized interfacing system (DICIS) model for CBDM, which is illustrated in Fig. 6. The components within DICIS include all user interfacing components (i.e. web browsers), communications and security components (the Internet and enterprise firewall systems), human assets (users, producers, consumers, managers, etc.), and the actual Manufacturing process assets. Note that manufacturing process assets (MPA) include software components such as CAD tools and packages as well as physical components such as 3D printers, milling machines, electrical prototyping boards, and robotic equipment. Even though a "pure" cloud computing framework normally only represents software systems, the DICIS model for our CBDM includes both virtual resources (i.e. software, computer hardware, etc.) as well as physical and human resources such as the equipment listed above. In essence, the DICIS model and its implementation as a CBDM system can be viewed as an integrated design and manufacturing infrastructure, which can support industrial applications as well as educational needs such as computer-centric laboratory coursework and research.

The DICIS model categorizes CBDM assets into three primary groups: (1) Human Assets, (2) Communication Assets, and (3) Manufacturing Process Assets. Further, human, communication, and manufacturing process assets are bound to both the centralized interface (CI) and the distributed infrastructure (DI). The distributed infrastructure incorporates the primary physical, virtual, and human resources of the

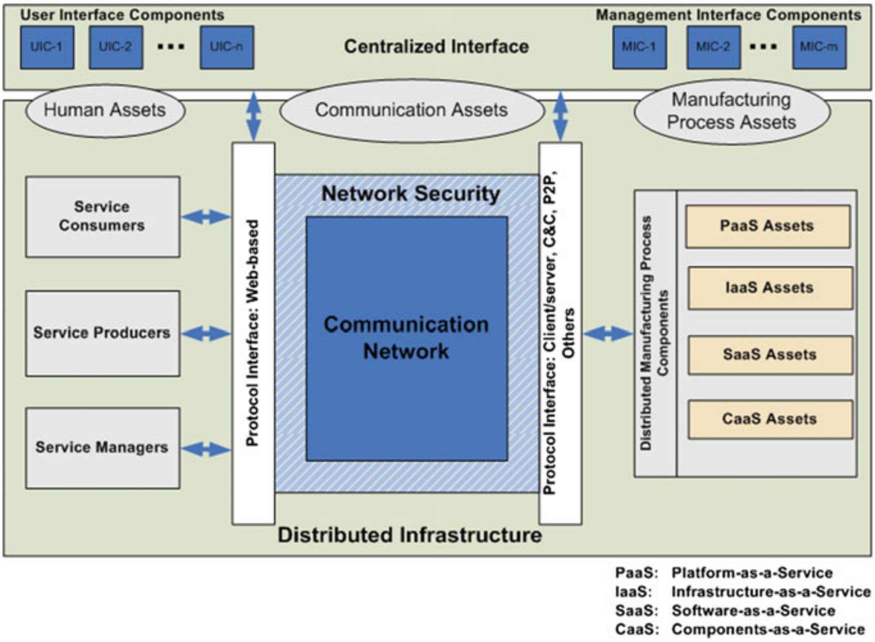

User Interface Components
UIC-1
UIC-2
UIC-n
Centralized Interface
Management Interface Components
MIC-1
MIC-2
MIC-m
Human Assets
Communication Assets
Manufacturing Process Assets
Service Consumers
Service Producers
Service Managers
Protocol Interface: Web-based
Network Security
Communication Network
Protocol Interface: Client/server, C&C, P2P, Others
Distributed Manufacturing Process Components
PaaS Assets
IaaS Assets
SaaS Assets
CaaS Assets
Distributed Infrastructure
PaaS: Platform-as-a-Service
IaaS: Infrastructure-as-a-Service
SaaS: Software-as-a-Service
CaaS: Components-as-a-Service

Fig. 6 The DICIS model for CBDM

CBDM. However, the centralized interface, which includes two primary groups of components referred to as the user interface components (UIC) and management interface components (MIC), provides the resources that glue the system together.

The DICIS model considers three human asset categories: (1) service consumers, (2) service producers, and (3) service managers. Service consumers utilize the services offered by the CBDM. Service consumers include, for example, students participating in distributed design and manufacturing projects, researchers/engineers investigating a new design prototypes, or companies with geographically distributed manufacturing shops that need to manufacture the components of a new product. Service producers provide human resources in term of intellectual capital and labor that result in provisioning of useful services. For example, a laboratory assistant or production manager could be a service producer who installs a new set of devices and equipment into the CBDM and integrates these components to form a new consumer service. An example could be a remote manufacturing site that is installing a new 3D printer and milling machine into the CBDM that should be used by human assets (consumers) of the CBDM. Service managers administer the various resources in the CBDM, depending on the scope of their management roles. Service managers perform operations such as creating new user accounts, assigning user roles, scheduling projects, installing new CBDM resources, and scheduling system maintenance, just to name a few.

In the most general sense, service producers and service managers are problem solvers, whereas service consumers are problem holders. However, service producers and service managers can be problem holders that seek services of other service producers and service managers. Further, a particular user can simultaneously be a service consumer, producer, and/or manager, depending on the users role with respect to the system as a whole. For example, consider the user Alice. Alice can be a student participating in project A, a producer for project B, and a manager of project C.

The communication assets of DICIS are comprised of four primary components: (1) communication network, (2) network security, (3) human asset service communication interface (SCI), and (4) manufacturing process asset service communication interface. We assume that the communication network is based on the Internet Protocol (IP) such that standardized, ubiquitous, Internet-based communications take place. The network security component encapsulates the communication network component, which reflects the idea that securability is needed but also that in modern day enterprise networks, it already exists in several forms, but most notably in the form of firewall systems. In order to capitalize on the ubiquitous web, the human asset SCI uses web based protocols. Using web based protocols such as the HyperText Transport Protocol (HTTP) between human assets and the centralized interface will minimize CBDM deployment costs as it removes the need to develop specialized interface software for system utilization. However, the manufacturing process asset SCI can be more diverse, and different protocols such as client-server, command and control, and peer-to-peer protocols can be used, depending on the particular requirements of a given subset of the CBDM.

The manufacturing process assets of the DICIS model consist of hardware (physical) and software (virtual) design and manufacturing resources. Our current CBDM under investigation, which is an implementation of the DICIS model, consists of a heterogeneous hardware and software environment, and it supports manufacturing and laboratory hardware devices such as milling machines, lathes, laser cutters, 3D printers (3DP), and do-it-yourself (DIY) 3D printers.

For the software systems, our CBDM utilizes various computer-aided manufacturing (CAM) technologies, which are software systems that convert digital models of parts designed by our integrated CAD tools into machine-based fabrication instructions. Moreover, we are developing a range of software applications for design and manufacturing activities, as well as system and resource management. Some of these software applications include the commercial Dassault Systems suite of design and analysis tools such as CATIA and Simulia, which enable high-end CAD and analysis capabilities, as well as collaboration. We are also integrating various additive manufacturing tools into the system, such as tools for locating and utilizing 3D printers within the DICIS network.

5.2 A CBDM Workflow Example

A few basic details of our CBDM architecture are illustrated in Fig. 7. As shown in the figure, the CBDM system consists of a centralized interfacing server (CIS). The current version our CBDM uses a CIS platform that is based on the Sakai learning management system. From Fig. 7, several geographically dispersed users who are collaborating on a design project and are utilizing services of the CBDM such as CAD design tools, 3D printers, and CNC machines. The CIS also provides applications for resource management and scheduling. Once designs are ready for prototyping, STL files generated by the CAD tool are submitted to the CBDM 3D printing service framework. Further, for parts that are to be fabricated in metal, a design file (i.e., STL files) can be sent to a milling machine, which is controlled via software running on a milling machine PC (server), for the actual production of the end product. Note that the user interface is composed of web-browser interfaces into the CAD software as well as the 3D printing and milling machine controller software.

Figures 8 and 9 will be used to further explain the CBDM process. Figure 8 illustrates how our CBDM provides distributed and collaborative design and manufacturing services to three engineers. From Fig. 9, two of the engineers are working locally while the third is located at a distant site. Real-time collaboration is enabled via video telecollaboration services. Further, the three engineers are able to access the CAD design software, but not simultaneously. Instead, CAD control is transferred on-demand to any give designer in the collaborative design session by way of issuing a transfer input control request to the software application. Figure 9 shows how the design file from Fig. 8 is transferred to a remote 3D printer within the CBDM. In essence, once the collaborating engineers from Fig. 8 have completed their design and are ready to develop an AM prototype of the design, other software within the CBDM such as AM-Select is used to transfer design files from the CAD service to the 3D printer service.

6 Software Defined Cloud Manufacturing

Industry 4.0 and smart manufacturing of the future will, indeed, take advantage of numerous Internet-based technologies and associated paradigms. In the previous sections, we have described several key paradigms driven by Industry 4.0, including technologies such as cloud-based design and manufacturing systems that we have personally investigated over the past few years. An underlying objective of our research for the past few years is illustrated by Fig. 10. Particularly, one of our main research objectives, reflected by our research described above as well as what follows in this next few sections, is to enable globally distributed and collaborative cyber-physical product creation using cloud-based design and manufacturing, which in turn establishes an inter-relationship between the industrial Internet of Things

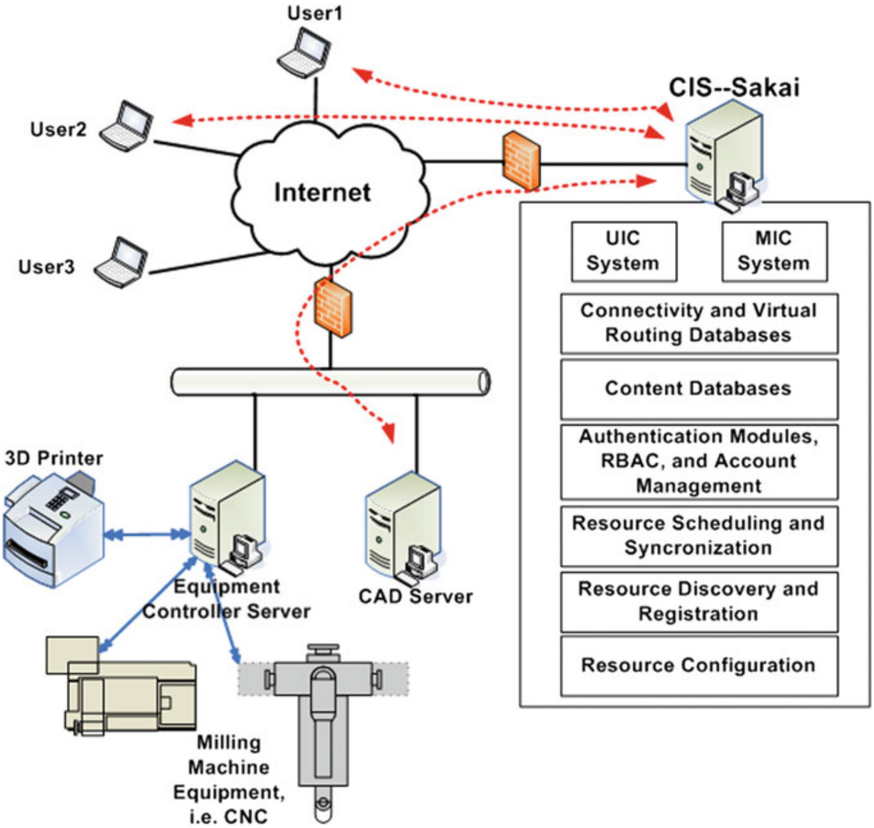
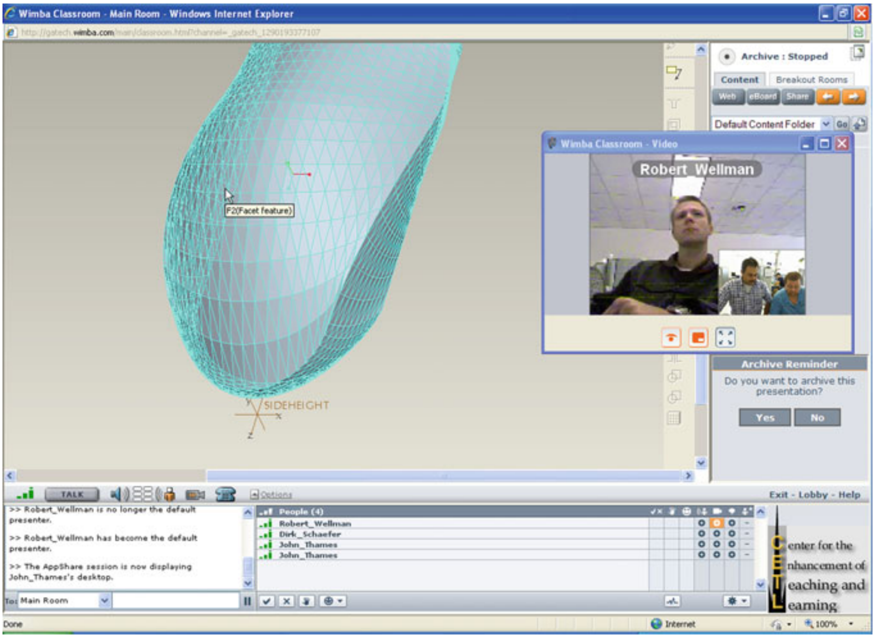

User1
CIS--Sakai
User2
Internet
User3
UIC System
MIC System
Connectivity and Virtual Routing Databases
Content Databases
Authentication Modules, RBAC, and Account Management
Resource Scheduling and Syncronization
Resource Discovery and Registration
Resource Configuration
3D Printer
Equipment Controller Server
CAD Server
Milling Machine Equipment, i.e. CNC

Fig. 7 CBDM workflow example

and the Internet of Services. We have tried to capture the ideas underlying these objectives in Fig. 10. The right hand side illustrates a CBDM system that is enabling cloud-based manufacturing and design services. This are essentially viewed from a consumer perspective as an Internet of Services enabled by an Industrial Internet of Things. As the figure reflects, design services can be globally distributed as well as the manufacturing services. It is the underlying CBDM framework that allows this abstraction. The 'consumer view' is that of using resources provided by an Internet of Services, which is composed of the actual entities (hardware entities, software entities, etc.) within the Industrial Internet of Things.

The objectives are aligned with the overall vision of Industry 4.0. However, the overall implementation is not trivial. Many challenges and open problems remain along the research path we have taken. This book seeks to address a fundamental problem faced by Industry 4.0, which is that of cybersecurity and is addressed by the remaining chapters in this book. However, many other challenges remain. In particular, system complexity and the ability to manage Industry 4.0 system complexity



>> Robert_Wellman is no longer the default presenter.

>> Robert_Wellman has become the default presenter.

>> The AppShare session is now displaying John_Thames's desktop.

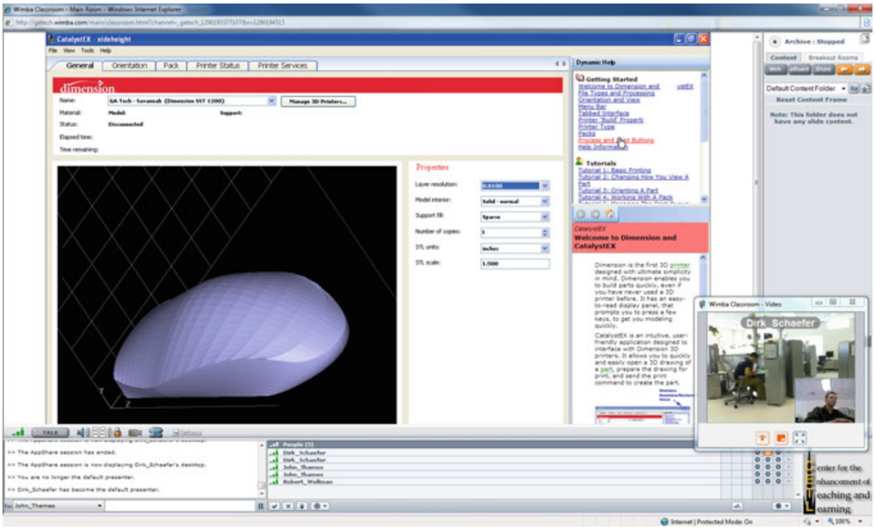
Fig. 8 Collaborative design via CBDM

is very important. In light of this, we have taken our research to a new level seeking to address complexity challenges, while also enabling cybersecurity functionality. Our new direction was guided by our first generation CBDM implementation as described above. Our latest advancements that seek to address these issues is based on an idea we refer to as Software Defined Cloud Manufacturing (SDCM). In the following sections, we will describe the ideas underlying SDCM.

6.1 Software-Defined Systems

Recently, the information technology field has begun to utilize software defined systems. It is a new paradigm of thinking about hardware and software, largely enabled by inexpensive, highly-functional hardware and virtualization technologies. Technologies that have emerged within this domain include software-defined networking, software-defined storage, software-defined computing, software-defined data center, and software-defined radio.

Software-defined networking (SDN) is defined as the physical separation of the network control plane from the forwarding plane where a control plane controls several devices. To understand the ramifications of this design, one must consider the paradigm it is replacing. Particularly, non-SDN networking devices are based on a



Wimba Classroom - Main Room - Windows Internet Explorer

CatalystEX - sideheight

General | Orientation | Pack | Printer Status | Printer Services

dimension

Name: GA Tech - Savannah (Dimension SST 1200)

Material: Model: Support:

Status: Disconnected

Elapsed time:

Time remaining:

Properties

Layer resolution: 0.0100

Model interior: Solid - normal

Support fill: Sparse

Number of copies: 1

STL units: inches

STL scale: 1.000

Dynamic Help

Getting Started

Welcome to Dimension and CatalystEX

File Types and Processing

Orientation and View

Menu Bar

Tabbed Interface

Printer 'Build' Properti

Printer Type

Packs

Process and Print Buttons

Help Information

Tutorials

Tutorial 1: Basic Printing

Tutorial 2: Changing How You View A Part

Tutorial 3: Orienting A Part

Tutorial 4: Working With A Pack

CatalystEX

Welcome to Dimension and CatalystEX

Dimension is the first 3D printer designed with ultimate simplicity in mind. Dimension enables you to build parts quickly, even if you have never used a 3D printer before. It has an easy-to-read display panel, that prompts you to press a few keys, to get you modeling quickly.

CatalystEX is an intuitive, user-friendly application designed to interface with Dimension 3D printers. It allows you to quickly and easily open a 3D drawing of a part, prepare the drawing for print, and send the print command to create the part.

>> The AppShare session has ended.

>> The AppShare session is now displaying Dirk_Schaefer's desktop.

>> You are no longer the default presenter.

>> Dirk_Schaefer has become the default presenter.

To: John_Thames

People (5)

Dirk_Schaefer

Dirk_Schaefer

John_Thames

John_Thames

Robert_Wellman

Wimba Classroom - Video

Dirk Schaefer

Archive : Stopped

Content | Breakout Rooms

Default Content Folder

Reset Content Frame

Note: This folder does not have any slide content.

TALK
Center for the Enhancement of Teaching and Learning
Internet | Protected Mode: On
100%

Fig. 9 Sending a design file to a CBDM 3D printer resource

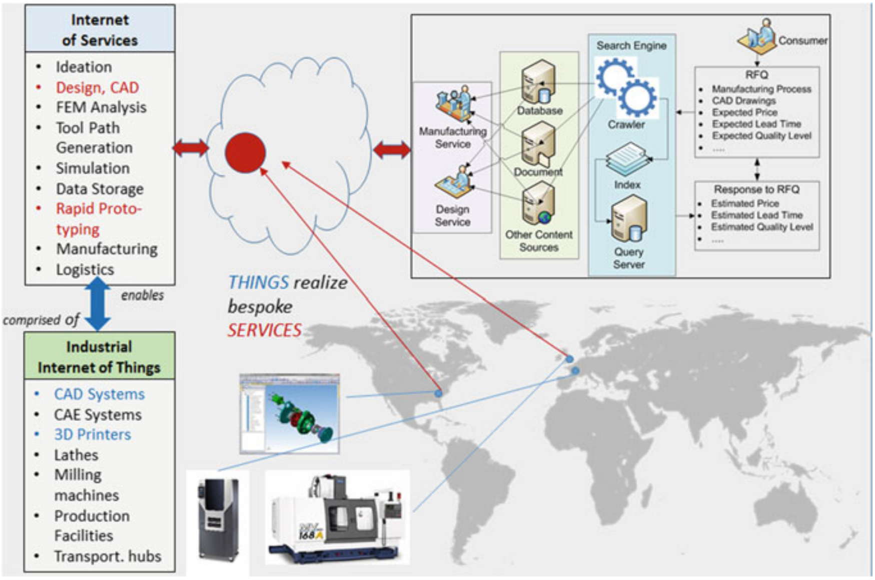


Fig. 10 Relationship between CBDM, the industrial internet of things, and the internet of services

design whereby each network device is totally isolated from the other devices in its network. Although it might coordinate and work with other devices, its so-called control plane is isolated to itself and its control plane functionality cannot be modified (outside of traditional patching, upgrades, etc.). With SDN, the control plane is managed centrally, it is defined by software, and it can apply to multiple devices. The idea is that network devices have generic hardware that does not require vendor-specific software, and the control plane functionality can be molded to fit a given design goal and can apply to multiple devices. SDN is known to be flexible, manageable, adaptive, and very cost-effective. It allows the control plane to be directly programmable instead of fixed software that is only configurable.

The software-defined supply chain is yet another emerging software-defined system recently described by Paul Brody (2013). Brody suggests that product design and manufacturing are changing, and the change is due to emerging, maturing, and converging technologies. Namely, Brody suggests that three particular technologies will reshape manufacturing. These technologies include 3D printing, next generation intelligent assembly robots, and open source hardware. Brody goes on to say that "Success in the future will require developing and adopting a new set of mental models, business processes, and enterprise technologies" (Paul Brody 2013).

6.2 A Software Defined Cloud Manufacturing Architecture

Recall from the previous sections that our first generation CBDM model and architecture was based on a hybrid distributed-centralized system. The architecture was driven by ideas included in the DICIS model. The architecture was composed of highly distributed design and manufacturing components. However, the entire system was 'glued' together using a centralized interfacing server. The reason for such a design was to remove IT/OT integration challenges across disparate organizations with different IT governance policies. To do this, a command and control communication (C2) architecture was developed whereby each entity in the collaboration network, i.e., all of the MENTOR high schools' hardware units such as 3D printers, where interfaced with a lightweight C2 software agent that established a TCP session with the CIS. The CIS was then in charge of interconnecting the various devices, software, and users of the collaboration network, i.e., the CBDM network. Basically, a single CIS server served as the core intelligence of the CBDM network. While this design works well for small networks, it does not scale. Moreover, the centralized nature of this design does not align with our overall vision of enabling CBDM as a fully distributed, global network of cloud-based resources.

Considering these issues, we went back to the drawing board and developed a new architecture that converted the CIS into a fully distributed cloud-based network of intelligent components (which you will see in a few minutes we call SDCM controllers). Our new architecture is modeled by software defined systems. In general, software-defined systems are characterized by properties such as being agile, programmable, manageable, configurable, interoperable, adaptable, and protectable. Indeed, Industry 4.0 technologies and smart manufacturing systems can benefit from these characteristics.

In what follows, we describe our new Software-Defined Cloud Manufacturing (SDCM) architecture to achieve these characteristics for various Industry 4.0 systems

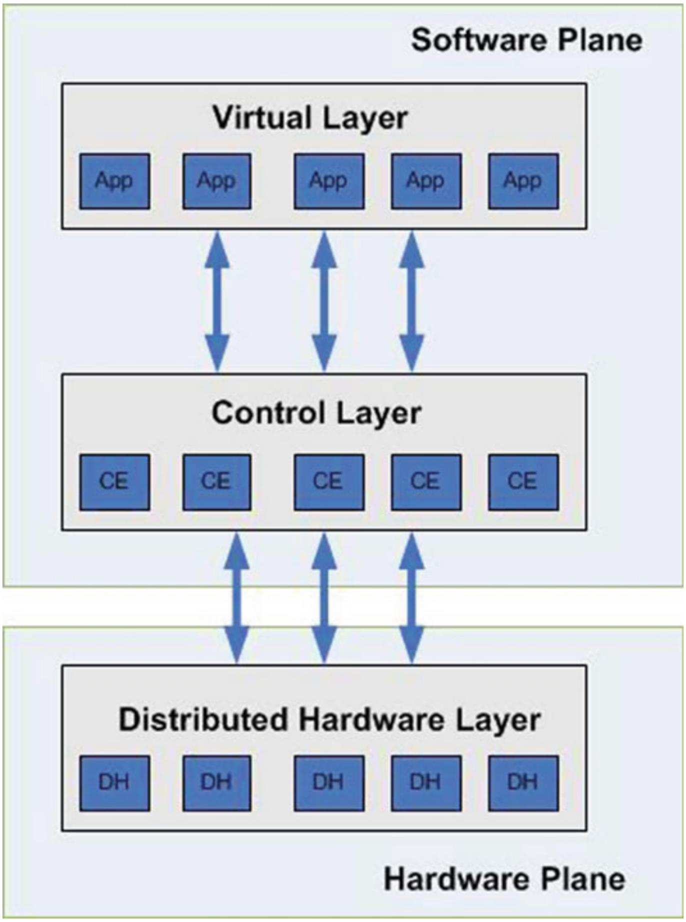


Fig. 11 A simplified software-defined cloud manufacturing architecture

in order to enable cyber physical product creation via a more distributed approach to CBDM. Our simplified SDCM architecture is illustrated in Fig. 11.

In this architecture, we assume a large network of hardware and software elements that have Internet-based communication frameworks, i.e. a TCP/IP stack. The goal is to utilize elements that constitute an Industry 4.0 system such as an IIoT, CBM, or SPD or combination thereof.

An important aspect of the SDCM architecture is separation of concerns (SoC). SoC is a design principle that allows one to break extremely large and complex systems into manageable parts. For example, the world-wide Internet is based on the SoC design principle. Our proposed SDCM architecture is first broken into two planes: the Software Plane and the Hardware Plane. In the architectures current state, we seek to distinguish the hardware elements from software elements. In particular, hardware does the final work whereas software will define how the work is orchestrated through to completion. The hardware plane includes a Distributed Hardware Layer (DHL). The DHL is further comprised of Distributed Hardware (DH) elements. For example, a DH could be a generic 3-D printer built on generic hardware from some particular maker community.

The software plane contains two layers, the virtual and control layers. The control layer is comprised of control elements (CE) and the virtual layer contains final user applications. Information flows are indicated by the arrows. The DHL communicates with the control layer and vice versa using an appropriate communication interface. Likewise, the virtual layer interfaces with the control layer.

Within each layer, multiple elements can be composed to create higher-level elements. As such, we define a software defined cloud manufacturing entity as a three-tuple $M = (V, C, D)$, where M is an SDCM entity, $V = \{a\}$, $C = \{ce\}$, $D = \{dh\}$. We say that V is a set representing an application composition, C is a set representing a control element composition, and D is a set representing a hardware composition. Particularly, our software defined cloud manufacturing model represents per-level element composition services that provide, in general, the capability to produce complex manufacturing services.

6.3 SDCM Domain Specific Configuration Language

Being ‘software defined’ immediately implies that things are defined by software. As such, we have developed a very light weight domain specific language that, at this time, serves more so as a configuration language than a pure programming language. The syntax was inspired by the VHDL hardware description language and the ideas underlying structured query language (SQL). The structure is given as follows:

BEGIN Doman_Specific_Language:
SELECT service **AS** “X”
TYPE: {“key”:“value”}
END
END

The goal of this light weight language was to provide a simple machine readable language that enables an entity within the SDCM network to find some service that is available based on various types of characteristics. This basic language serves well in terms of a prototype implementation. However, during the next phase of our research, we will be incorporating a more established and more mature language. In particular, in our future work we will be adopting the Software Component Ensemble Language (SCEL) (Nicola et al. 2014). Observe that an SDCM composition can be viewed as an ensemble of components. It turns out the SCEL “is a language for programming service computing systems in terms of service components aggregated according to their knowledge and behavioral policies” (Nicola et al. 2014). We believe that SCEL has a perfect mapping to SDCM that will allow us to enhance our overall goals and objectives.

6.4 SDCM Workflow Scenarios

In this section, we will provide a short overview of how the SDCM architecture will work in practice. A key functionality of SDCM is composition. At “runtime” applications, control elements, and distributed hardware elements are dynamically composed, and the composition depends on the overall SDCM service being provided.

Control elements are responsible for composition. Composition is initiated via an applications invocation (residing at the virtual layer). Controller elements are the core masterminds of a given SDCM service and contain the controller logic for composing the elements of the given service.

Composition of hardware elements can be achieved across a vast spectrum of scenarios. Here, we provide an overview of the ideas of this composition process at two opposite ends of the spectrum. On one end of this spectrum, we consider the idea of design and manufacturing hardware that might be found in domains such as open source hardware, DIY hardware, and maker spaces. As Brody ?? suggests, 3D printing, next generation intelligent assembly robots, and open source hardware will have significant impact on future manufacturing processes. Open source hardware (and its associated open source software) will lead to fast and incremental updates to hardware platforms. This could be utilized by various manufacturing entities. One aspect of this scenario is the ability to reconfigure these hardware platforms based on a desired set of functionality; this is where SDCM comes in to the picture. Figure 12 will be used to illustrate the ideas.

From Fig. 12, there is an open source hardware platform (OSHP) that contains 3 high-level components (C1, C2, and C3). This OSHP is considered to be a single hardware element (DHE). It has manufacturing capabilities that can be initiated via the composition of component C1 with component C2 or with component C2 and component C3. In this example, a controller element is in charge of uploading and

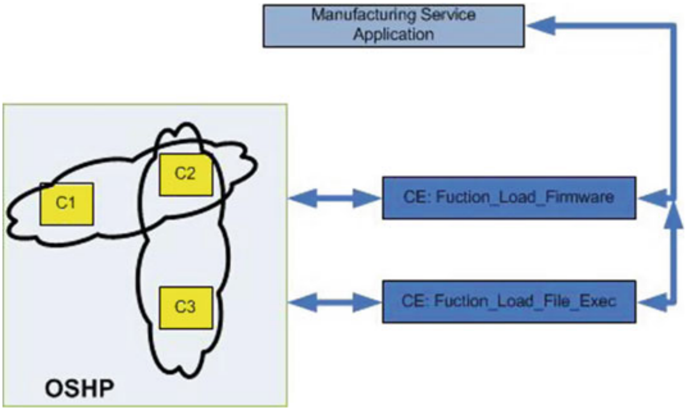

Manufacturing Service Application
C1
C2
C3
OSHP
CE: Fuction_Load_Firmware
CE: Fuction_Load_File_Exec

Fig. 12 An illustrated view of the SDCM workflow

installing firmware that configures the device based on the desired composition. After the firmware has been installed and initialized, a second control element loads a design file into the system and begins its particular manufacturing service.

The previous example exploited the ideas of open source hardware of the near future where resources included within a given hardware platform can be composed to produce a certain type of manufacturing service. Further, it assumes that the platform could be reconfigured for different types of manufacturing services. Obviously, this will depend on the hardware platform and its internal resources. The workflow that is described, however, can be utilized at a different level of abstraction. This workflow provided by SDCM can be applied to multiple, independent hardware platforms. This abstraction is indeed a powerful aspect of SDCM. An equivalent workflow, for example, could be the composition of a manufacturing robot (i.e., C1 is the robot) along with a 3D printer and CNC milling machine (C2 and C3, respectively). An SDCM manufacturing entity could be the composition of the robot and the CNC machine or the robot and the 3D printer. Controller elements and user interfaces (virtual applications) can be developed to implement a manufacturing service that utilizes these compositions to create some artifact. The artifact could in turn be designed by some cloud-based CAD program that is also brought in as a higher-order composition. For example, the CAD program can be yet another component in the total composition.

In the following scenarios, we will connect back to our first generation CBDM prototype in order for the reader to understand the evolution of our work in this area. First, let's review Fig. 13. During our work with MENTOR and our first generation CBDM prototype, we developed C2 communication interfaces that interconnected

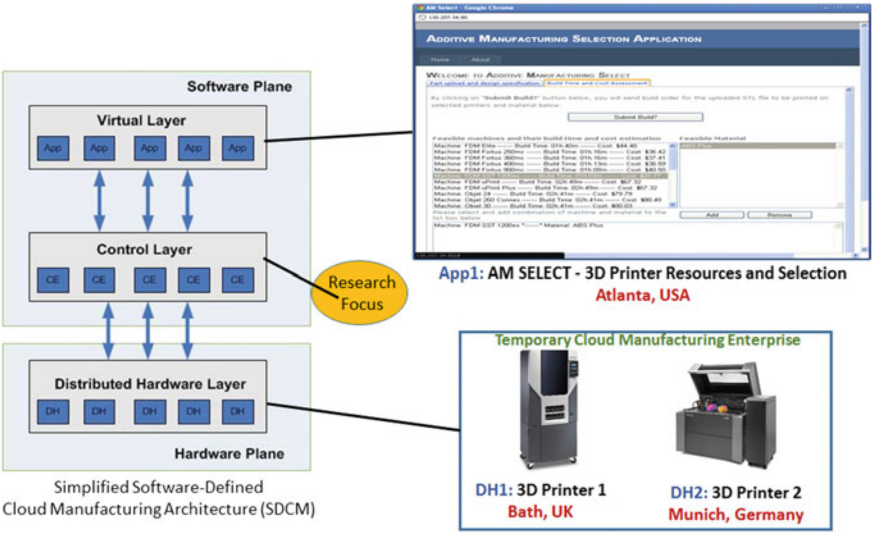
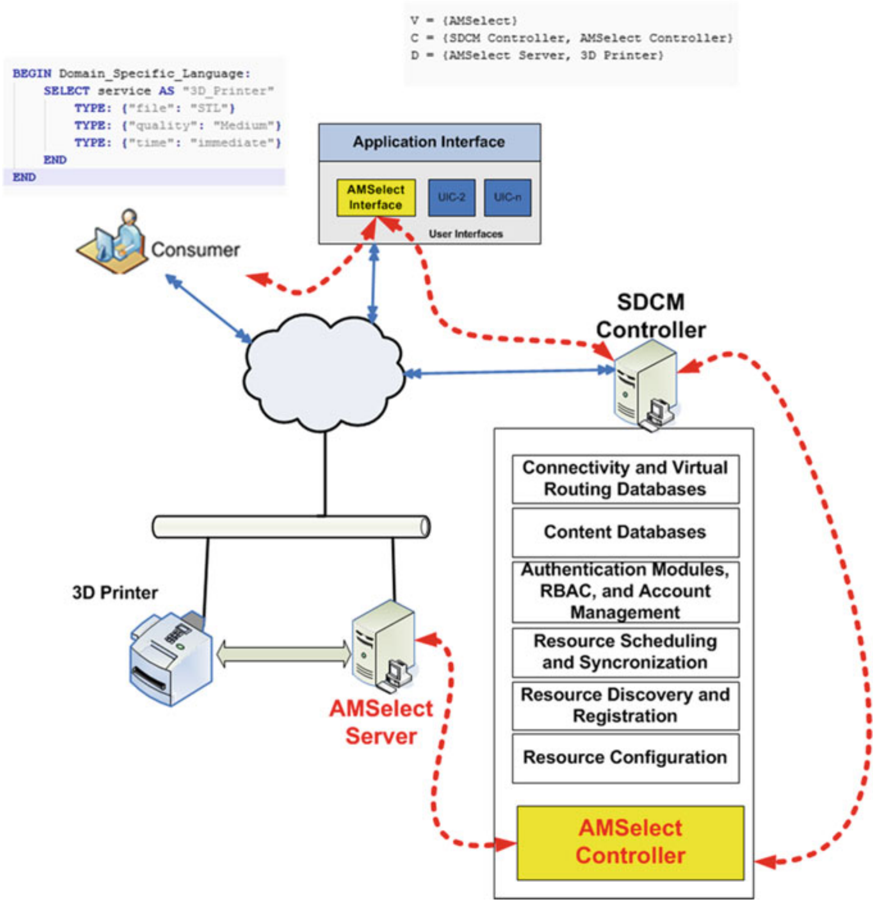

Software Plane
Virtual Layer
App
App
App
App
App
Control Layer
CE
CE
CE
CE
CE
Research Focus
Distributed Hardware Layer
DH
DH
DH
DH
DH
Hardware Plane
Simplified Software-Defined Cloud Manufacturing Architecture (SDCM)
Additive Manufacturing Selection Application
Home
About
Welcome to Additive Manufacturing Select
Submit Build?
Add
Remove
App1: AM SELECT - 3D Printer Resources and Selection
Atlanta, USA
Temporary Cloud Manufacturing Enterprise
DH1: 3D Printer 1
Bath, UK
DH2: 3D Printer 2
Munich, Germany

Fig. 13 SDCM and CBDM—high level

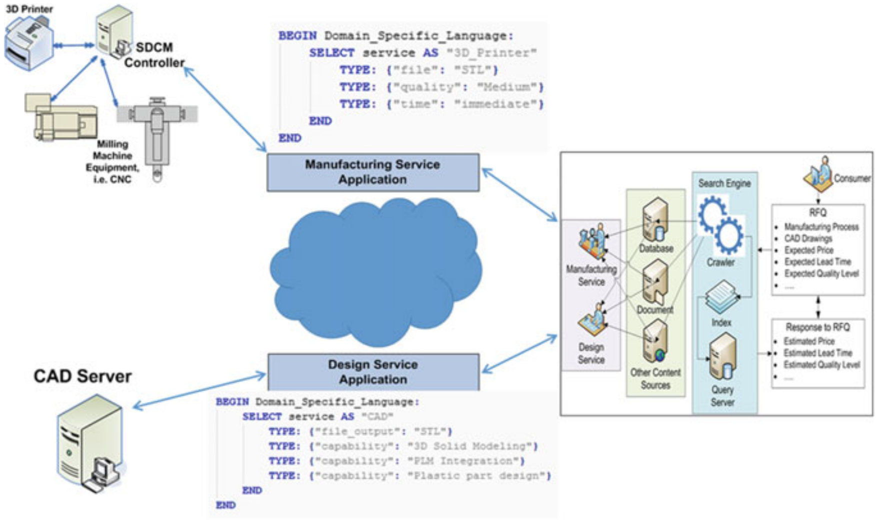
via the CIS all of the hardware and software entities in the network. Once such software application was called ‘AM SELECT’ (Additive Manufacturing Select) and it was used to allow users of the CBMD network to find additive manufacturing devices with the CBDM network. Once selected, based on types such as materials, cost, time to complete the job, etc., the CIS interconnected the user to an available printer. Figure 13 reveals how this is accomplished, at a high level, with our SDCM architecture. It is very similar. The AM SELECT application is located within the virtual layer and the 3D printers are located within the distributed hardware layer. However, the intelligence required to connect the pieces together (as well as all other functionality such as resource discovery, virtual routing, authentication, authorization, access control, etc.) is implemented at the control layer, which is a vast collection of control elements highly distributed throughout a cloud environment.



```
V = {AMSelect}
C = {SDCM Controller, AMSelect Controller}
D = {AMSelect Server, 3D Printer}
```

```
BEGIN Domain_Specific_Language:
    SELECT service AS "3D_Printer"
        TYPE: {"file": "STL"}
        TYPE: {"quality": "Medium"}
        TYPE: {"time": "immediate"}
    END
END
```

Fig. 14 SDCM and CBDM—low level



```
BEGIN Domain_Specific_Language:
    SELECT service AS "3D_Printer"
        TYPE: ("file": "STL")
        TYPE: ("quality": "Medium")
        TYPE: ("time": "immediate")
    END
END
```

```
BEGIN Domain_Specific_Language:
    SELECT service AS "CAD"
        TYPE: ("file_output": "STL")
        TYPE: ("capability": "3D Solid Modeling")
        TYPE: ("capability": "PLM Integration")
        TYPE: ("capability": "Plastic part design")
    END
END
```

Fig. 15 SDCM and CBDM: enabling manufacturing and design services

Let us explain these concept further with Fig. 14. This figure is similar to Fig. 7. The CIS is replaced by a distributed collection of SDCM controllers. These controllers implement functions such as connectivity and virtual routing, content, resource configuration, and such. In Fig. 14 a SDCM consumer interacts with the AM SELECT interface. Upon selection of the appropriate additive manufacturing resource, the interface generates the domain specific language requesting a 3D Printer resource that accepts STL files, produces artifacts with medium quality, and is available immediately. This request gets sent to the controller cloud and gets processed. Once an appropriate 3D printer is located, an SDCM controller interconnects the printer to the AM SELECT interface for the user to submit the STL file.

We provide one last scenario, which is illustrated by Fig. 15. In this figure, we are simply trying to illustrate how we have tied all the pieces together. Our SDCM architecture is the underlying backbone that allows us to implement a fully distributed CBDM network. The CBDM network allows consumers and producers to interact with one another via design and manufacturing services.

7 Closure

In this chapter, we have tried to set the stage for the remainder of this book by introducing key technologies and paradigms that are driven by the overall vision of Industry 4.0. A large portion of the chapter was devoted to discussing Cloud-based Design and Manufacturing (CBMD) because of two reasons. First, the authors have been researching and implementing CBDM technology for over 5 years. Second, we have also studied the cybersecurity aspects of CBDM and felt that our in depth discussion of the topic would serve the reader well in understanding the remaining material in the book. In terms of CBDM, we have presented the big picture of how it has emerged as a new paradigm to support globally distributed design and manufacturing in the broader context of social product development and the so-called new industrial revolution (Anderson 2012). We have explained the underlying technical fundamentals of CBDM, our current extension to CBDM using a software defined cloud manufacturing architecture, and have presented a summary of our various implementations. Once again, the goal was to provide the reader with a broad background of Industry 4.0 technologies and paradigms. Now, however, we must turn our attention to the primary purpose of this book: cybersecurity. The remaining chapters of this book will address many aspects of cybersecurity and its need for advancing Industry 4.0 technologies.

References

Anderson C (2012) Makers: the new industrial revolution. Crown Business

Armbrust M, Fox A, Griffith R, Joseph A, Katz R, Konwinski A (2010) Above the clouds: a view of cloud computing. Commun ACM

Autodesk (2017). www.autodesk.com

Bohm M (2010) Cloud computing and computing evolution. Technical report

Brody P (2013) Get ready for software-defined supply chain. http://www.supplychainquarterly.com/topics/Manufacturing/20140110-get-ready-for-the-software-defined-supply-chain/

Buyya R, Yeo C, Venugopal S (2008) Market-oriented cloud computing: vision, hype, and reality for delivering IT services as computing utilities. CoRR

Chesbrough W (2003) Open innovation: the new imperative for creating and profiting from technology. Harvard Business Press

Dassault (2017). www.3ds.com

De Nicola R, Loreti M, Pugliese R, Tiezzi F (2014) A formal approach to autonomic systems programming: the scel language. ACM Trans Auton Adapt Syst

Foster I, Kesselman C (1999) The grid: blueprint for a new computing infrastructure. Morgan Kaufmann

Foster I, Zhao Y, Raicu I, Lu S (2008) Cloud computing and grid computing 360-degree compared. In: Grid computing environments workshop

Franke N, Von Hippel E, Schreier M (2006) Finding commercially attractive user innovations: a test of lead user theory. J Prod Innov Manage 23(4):301–315

Friedman T (2005) It's a flat world after all. New York Times 3:33–37

Fujitsu (2017). www.fujitsu.com

IBM (2010) Dispelling the vapor around cloud computing. ibm.com

Licklider J (2010) Topics for discussion at the forthcoming meeting, memorandum for: members and affiliates of the intergalactic computer network

NIST (2011) NIST cloud computing reference architecture—special publication 500–292

Pahl G, Beitz W (1988) Engineering design: a systematic approach. Springer

Parkhill (1966) The challenge of the computer utility. Addison-Wesley publication

Suh N (2001) Axiomatic design: advances and applications. Oxford University Press

Tao F, Zhang L, Venkatesh V, Luo Y, Cheng Y (2011) Cloud manufacturing: a computing and service oriented manufacturing model. J Eng Manuf 225(10):1969–1976

Tapscott D, Williams A (2008) Wikinomics: how mass collaboration changes everything. Portfolio trade

Vaquero L, Merino L, Caceres J, Lindner M (2009) A break in the clouds: towards a cloud definition. ACM Comput Commun Rev

Wikipedia (2017). www.wikipedia.org

Wu D, Greer M, Rosen D, Schaefer D (2013) Cloud manufacturing: drivers, current status, and future trends. In: ASME international manufacturing science and engineering conference

Wu D, Schaefer D, Rosen D (2013) Cloud-based design and manufacturing systems: a social network analysis approach. In: International conference on engineering design

Wu D, Thames L, Rosen D, Schaefer D (2012) Towards a cloud-based design and manufacturing paradigm: looking backward, looking forward. In: ASME international design engineering technical conference and computers and information in engineering conference

Xu X (2012) From cloud computing to cloud manufacturing. Robot Comput Integr Manuf 28:75–86

Customized Encryption of CAD Models for Cloud-Enabled Collaborative Product Development

X.T. Cai, S. Wang, X. Lu and W.D. Li

Abstract Collaborative product development via cloud has changed the information distribution, organization and management means of traditional product design. Under this new paradigm, product information needs to be shared flexibly to meet collaborators' requirements. Feature-based Computer Aided Design (CAD) models contain abundant intellectual property information. It is paramount to maintain the security of the sensitive information in CAD models while sharing other information of the models in cloud for effective collaboration. The developed security research works for CAD models are still far away from meeting collaboration requirements. In this chapter, an innovative customized encryption approach to support product development collaboration is presented. The approach is composed of a customized encryption algorithm for feature-based CAD models, a key based authorization algorithm for users to decrypt shared features in the models, and a customized geometric transformation algorithm for effective protection mode-based visualization of the models during collaboration. By using this approach, CAD models can be flexibly encrypted to realize the customized sharing of features used for collaboration and protection of other features of the models according to collaboration requirements. A complex case study has been used to verify and illustrate the effectiveness of the approach to industrial applications.

Keywords Customized encryption · CAD model · Product collaboration

X.T. Cai
School of Computer Science and Technology, Wuhan University, Wuhan, China
e-mail: caixiantao@whu.edu.cn

S. Wang · X. Lu · W.D. Li (✉)
Faculty of Engineering and Computing, Coventry University, Coventry, UK
e-mail: weidong.li@coventry.ac.uk

S. Wang
e-mail: sheng.wang@coventry.ac.uk

X. Lu
e-mail: xin.lu@coventry.ac.uk

L. Thames and D. Schaefer (eds.), *Cybersecurity for Industry 4.0*,
Springer Series in Advanced Manufacturing, DOI 10.1007/978-3-319-50660-9_2

1 Introduction

Collaborative product development via cloud is an inevitable trend in the Industry 4.0 era. To optimize design resources, product development companies have been increasingly designing their products in a cloud-enabled collaborative environment. Design features contained in a Computer Aided Design (CAD) model reflect design goal and functions. It is a challenging issue how to effectively protect the sensitive feature information of a model when the model is shared in cloud (Cai et al. 2012; Li and Mehnen 2013). The related research either cannot protect the sensitive information in the sharing process of CAD models effectively or cannot support the sharing of CAD models in the feature level flexibly.

In this chapter, an innovative approach for customized encryption on feature-based CAD models to support collaboration via cloud is presented. The approach supports a typical collaborative scenario illustrated in Fig. 1. In Fig. 1, there are two types of people, i.e., a model owner and collaborators. The model owner uploads an encrypted CAD model into cloud, and collaborators download and decrypt the model from cloud. To effectively share as well as protecting information, features in a CAD model are classified into the following three categories:

- Protected features (e.g., the blades in Fig. 1): The features contain sensitive and private information of the model. These features are only owned by the model owner and not shared with the collaborators. From the collaborators' perspective, the protected features will be only visualized in transformed (deformed) geometry and critical parameters of the features are hidden;

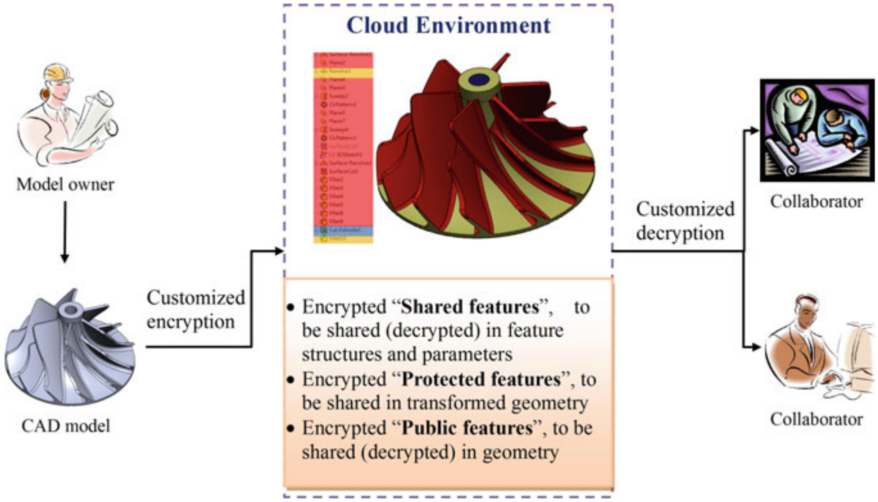

Cloud Environment
Model owner
CAD model
Customized encryption
Customized decryption
Collaborator
Collaborator
• Encrypted "**Shared features**", to be shared (decrypted) in feature structures and parameters
• Encrypted "**Protected features**", to be shared in transformed geometry
• Encrypted "**Public features**", to be shared (decrypted) in geometry

Fig. 1 A typical collaborative scenario for a CAD model

- Shared features (e.g., the central hole in Fig. 1): The shared features are shared to interface with collaborators. The features are encrypted by the model owner, decrypted in the cloud for the collaborators;
- Public features (e.g., the base in Fig. 1): The features do not contain sensitive information. They are shared with collaborators in the form of geometry without deformation.

To process features, this approach is composed by the following algorithms:

- A customized encryption algorithm. In the algorithm, the protected and shared features of a CAD model are encrypted through sketch transformation and random invertible matrices of the features. In addition, the generation of an encryption matrix is controlled in a parametric means to provide flexibility to the model owner to adjust and ensure the security of the model;
- A key based authorization algorithm. When the model owner selects the features to be encrypted, the keys of the shared features are recorded in an authorization file, which is used to decrypt the shared features;
- A customized geometric transformation algorithm. In order to hide the design procedure and feature parameters, the protected features and public features in the CAD model are transformed to a geometric model. The geometric model is combined with the decrypted shared features to collaborators.

The innovations and characteristics of this approach include: (1) Protected, shared and public features can be selected by the model owner flexibly; (2) The CAD model is always manifold and valid in geometry no matter which feature is encrypted or decrypted; (3) The parameters of the model are effectively protected through the encryption and geometric transformation mechanisms; (4) The model owner can authorize any shared feature by issuing the keys of the features to meet the customized requirements of various collaborators; (5) The shared features in the model are still parameterized after decryption to be interoperated by collaborators flexibly; (6) This approach is content-based and customized and applicable to CAD model-based collaboration in cloud.

In the following sections, the previously developed security approaches for CAD models in networked environments are first reviewed. The approach of customized encryption of feature-based CAD models is then detailed. Finally, case studies and validation of the approach are described.

2 Related Research

The Internet provides convenience for information sharing, but simultaneously, brings security risks during sharing. Security risks have been becoming barriers to implement product development collaboration via the Internet. According to the theory of the information security, there are two main requirements to ensure security during information sharing: (1) Information hiding: an unauthorized user

Table 1 Related security research for collaborative product development

	A	B	C	D	Purpose	Problems
Watermark	√			√	Protect the intellectual property by embedding the watermark into CAD models	Design information (design knowledge, parameters) cannot be hidden by watermark in a safe way
Access control		√	√		Control the access of the design data by users' authorization according to a group of access control rules	Unable to support information protection of a CAD model
Multi-resolution approach		√		√	Multi-resolution is to simplify a CAD model during data sharing in a network with limited bandwidth	It can realize the secure sharing of a CAD model to some degrees, but not flexibly
Encryption of CAD models		√		√	Hide the design information by encryption	No research applied to CAD models

Notes: A—Information authentication; B—Information hiding; C—Architecture-level security; D—Data-level security

cannot access the confidential information; (2) Information authentication: information has a verification capacity which can ensure the information has not been changed (Rutledge and Hoffman 1986). Various research works about the secure sharing of CAD models have been developed according to the above two requirements. The developed approaches can be classified in Table 1. More technical details are expanded below.

2.1 Watermark of CAD Models

The watermark concept was first proposed (Tirkel et al. 1993). The digital watermarking technology is used for the intellectual property protection and the integrity authentication of electronic files. The creation information and logo of a creator are embedded in an electronic file. Watermark embedded into a product model cannot be removed during sharing, and the information can be detected by a special software package (Tao et al. 2012). Various watermarking approaches for 2D/3D CAD models were developed for intellectual property protection (Cayre et al. 2003; Chou and Tseng 2006; Wang et al. 2008; Ai et al. 2009; Peng et al. 2011; Lee and Kwon 2012; Su et al. 2013). However, the design information can still be retrieved so that the model is not safe.

2.2 Access Control of CAD Models in a Network Environment

Access control is an important security method for a network environment. Access to special resources is controlled by users' authorization. The related works can be classified in the following categories.

The general access control approaches. The access control appeared in the 1970s. Lampson initiated the concept of access matrix. The access control became an important approach for information protection in networked environments (Lampson 1974). Conway used the concept of secure matrix for access control, and standardized the secure matrix and finally presented the theory of discretionary access control (Conway et al. 1972). Later, more access control approaches were developed. A role based access control approach was developed (Sandhu et al. 1996). Task role-based Access Control was proposed (Oh and Park 2003), and Usage Control called the next generation of access control model was presented (Park and Sandhu 2004).

The access control approaches of files. To support product development collaboration, many special access control approaches were developed. van der Hoeven proposed an access control based CAD architecture (van der Hoeven et al. 1994). However, access control is still file based. Stevens developed an ADOSX system to support product development collaboration between two enterprises, while the system just focuses on the access control of files (Stevens and Wulf 2002). Cera et al. developed a secure access control mechanism for 3D models (Cera et al. 2006). The approach, however, supports the collaborative view of product models not the full-scale collaborative design. Leong et al. devised a security approach for a distributed product data management system. The approach combines the Lampson's access matrix and it is still file based (Leong et al. 2003).

The sharing space based access control approaches. Considering the frequent sharing of design data, sharing space based access control methods were proposed, in which a secure sharing space was designed. A dynamic data sharing and security approach for product development collaboration was developed (Rouibah and Ould-Ali 2007). Chang et al. developed the security system for sharing engineering drawings in the sharing space (Chang et al. 2008).

The multi-method based access control methods. In order to improve the security during product development collaboration, multi-method based access control methods were proposed. Some other security methods are combined with access control to ensure better security. Yao devised a security model of data for collaborative design and management system, which combines multi security methods with access control (Yao et al. 2007). A security system for sharing CAD drawings which used a multi-method approach was developed (Chang et al. 2008). Speiera et al. also used a multi-method approach to mitigate product safety and security risks (Speiera et al. 2011). A network security mechanism for the collaborative combined Virtual Private Network and access control was proposed (Xiang and Li 2012).

The access control method constructs a secure environment based on the architecture level. On the other hand, all the existed general and special access control approaches are file based. They cannot handle the case that a CAD model contains both confidential information and sharing information.

2.3 Multi-level Design Data Sharing Based on the Multi-resolution Models

Multi-resolution modeling can be used for the secure sharing of CAD models. The approaches can be classified further into the following categories.

Multi-resolution mesh model. In the past, a solid model is changed to a mesh model, and then the mesh model is transformed to a multi-resolution mesh model for model simplification (Hoppe 1996). Han proposed a multi-resolution modeling approach of CAD models to support collaborative design (Han et al. 2003), Qiu et al. designed a T-Curve based simplification method for CAD models (Qiu et al. 2004). Li et al. present a 3D simplification algorithm for distributed visualization (Li et al. 2007). All the methods are mesh model based. However, a mesh model lacks design information (history, features, parameters and so on) to support product collaboration effectively.

Multi-resolution B-rep, solid and feature modeling. Belaziz et al. provided an analysis tool of a B-rep model, which can delete some features without any complex Boolean operations (Belaziz et al. 2000). A B-rep based multi-resolution modeling method based on the Wrap-Around was developed (Seo et al. 2005); Wrap-around, smooth-out and thinning were integrated to develop a new B-rep based multi-resolution modeling method (Kim et al. 2005). Lee et al. designed the Progressive Solid Model (PSM) to support the multi-resolution solid model (Lee et al. 2004). A feature based multi-resolution modeling method was developed (Lee 2005), which is based on the calculation of the valid volume.

Combination of the multi-resolution feature model and the access control. Cera et al. combined the multi-resolution modeling and access control to realize the access control of multi-level CAD models (Cera et al. 2006). Chu et al. focused on multi-level data sharing based on multi-LOD (Level of Detail) models (Chu et al. 2009). A matrix-based modularization approach for supporting collaboration in parametric design was developed (Li and Mirhosseini 2012).

Multi-level design data sharing based on the multi-resolution models can realize the customized secure sharing of a CAD model in some degrees. However, this method is not flexibly enough due to the following limitations: (1) The hidden information cannot be selected by the model owner; (2) The approaches cannot support collaboration freely because the sharing model is not complete.

2.4 Encryption of CAD Models

Data encryption is an important approach for information hidden in network. It can ensure that the hidden information cannot be obtained by unauthorized users. In recent years, the encryption methods have been widely used for multi-media data, such as the image encryption. Due to the complexity, there are a few research works about 3D models. Huang et al. proposed a method of encrypting 3D data information with virtual holography (Huang et al. 2009). Esam and Ben proposed secured sharing approaches for 3D mesh model encryption (Esam and Ben 2011). An approach for encryption based multi-level data access control to share the images in a collaborative environment was developed (Naveen and Thomas 2011) On the other hand, until now, there are few research works about the encryption of CAD models.

2.5 Summary of the Related Works

The requirements for customized sharing of CAD models are complex. Based on the above discussions, the existing research for the secure sharing of design data has the following shortages: (1) Lack of flexible and feature based protection mechanism; (2) Lack of different levels of security; (3) Lack of flexible authorization mechanism for accessing CAD models;.

To support complex collaboration requirements, it is imperative to develop a more flexible encryption approach with the following characteristics: (1) The approach needs to support a model owner to flexibly realize customized protection of a CAD model for different users; (2) The approach should provide user friendliness and flexible control to ensure less deformation and geometric validity of CAD model during customized encryption; (3) The approach is feature based.

3 Customized Encryption of Feature-Based CAD Models

Data encryption is an important approach for information protection in a network environment. Effective approaches can prevent the sensitive information to be obtained by unauthorized users. In the early time, any files represented in binary formats are regarded as encrypted. Later, content based encrypted approaches based on the encryption of the basic content elements appeared. Based on that approaches, the encrypted file could be open. However, the content cannot be distinguished correctly by unauthorized users (such as the image encryption). As thus, content-based encryption can be used to protect the information of a CAD model when it is being shared. The approach presented in this chapter is content-based, and a new research work for customized encryption of CAD models.

3.1 Encryption of a CAD Model

A group of design or manufacturing features and their related position constraints are the building blocks of a CAD model. As thus, a CAD model can be defined as the following Representation (1).

$$M = \bigcup_{i=1}^{n} (C_i \otimes f_i) \tag{1}$$

where M denotes a CAD model, and f_i means a feature of M, C_i is a set of containing all the constrains between f_i and its father features, $\otimes$ means a geometric operation on the model applied by the constraints on the features.

A definition of the constraint between two features is given as following.

Definition 1 *$\forall f \in M$ and $\forall f' \in M$, $f \rightarrow f'$ means f has* constraints propagated to *f'.*

Where M is a CAD model, the f and f' are both the features of M.

Definition 2 If $a \propto b$, means the shape of a is decided by b.

According to Definition 2 and Representation (1), Representation (2) is given below, which means the shape of a CAD model is decided by all its features.

$$M \propto \bigcup_{i=1}^{n} f_i \tag{2}$$

According to the constitution of a feature, the features can be classified as two types: Sketch Based Feature (SBF) and Non Sketch Based Feature (NSBF).

Definition 3 Sketch Based Feature (SBF). SBF means the feature's creation is based on its sketch(es), and the primary shape of a SBF is decided by its sketch(es)

Definition 4 Non Sketch Based Feature (NSBF). NSBF means the feature's creation is dependent on its nesting feature(s), and the primary shape of a NSBF is decided by its nesting feature(s)

The above can be represented in Representation (3):

$$\forall f_i \in M, \quad f_i \propto \begin{cases} \bigcup_{j=1}^{p_i} s_j, \ (f_i \, is \, SBF) \\ \bigcup_{j=k_1}^{q_i} f_j, \ (f_i \, is \, NSBF) \end{cases} \tag{3}$$

where $\cup_{j=1}^{m_i} s_j$ is the sketch set of f_i if it is a SBF, p_i means the number of the sketches; and $\cup_{j=k_1}^{m_i} f_j$ is the nesting feature set of f_i if it is a NSBF, q_i means the number of the nesting features and k_1 means the id of the basic feature f_{k_1}. Obviously, the first feature of any CAD model is SBF.

Based on Representation (2) and Representation (3), Theorem 1 is given.

Table 2 Proof of Theorem 1

Step 1: To prove the shape of any feature is finally decided by a group of sketches.

(1) For the features in Level 0

$\because$ *f_0 is the first feature of model M*

$\therefore$ *f_0 is a BSF*

$\therefore$ *According to Representation (3):* $f_0 \propto \bigcup_{j=1}^{p_0} s_j$

(2) For the features in Level 1

Based on the DLG, for any feature on Level 1: $\forall f_{1i}.level = 1$

$\because$ *f_0 is the only feature in Level 0, according to Representation (3):*

$$f_{1i} \propto \begin{cases} \bigcup_{j=1}^{p_{1i}} s_j, (f_{1i} \text{ is } SBF) \\ f_0, (f_{1i} \text{ is } NSBF) \end{cases}$$

$$\because \ f_0 \propto \bigcup_{j=1}^{p_0} s_j$$

$$\therefore \ f_{1i} \propto f_0$$

$$\therefore \ f_{1i} \propto \bigcup_{j=1}^{p_0} s_j$$

$$\therefore \ f_{1i} \propto \begin{cases} \bigcup_{j=1}^{p_{1i}} s_j, (f_{1i} \text{ is } SBF) \\ \bigcup_{j=1}^{p_0} s_j, (f_{1i} \text{ is } NSBF) \end{cases}$$

(3) For the features in Level n

$\therefore$ *The rest may be deduced by analogy*

Based on the DLG, for any feature on Level n: $\forall f_{ni}.level = n$

$$\because \ f_{ni} \propto \begin{cases} \bigcup_{j=1}^{p_{ni}} s_j, (f_{1i} \text{ is } SBF) \\ \bigcup_{j=k_1}^{q_{ni}} f_j, (f_{1i} \text{ is } NSBF) \end{cases}$$

$$\therefore \ if \ f_{ni} \propto \bigcup_{j=k_1}^{q_{ni}} f_j \ ,then \ f_{ni} \propto \bigcup_{j=k_1}^{q_{ni}} (\bigcup_{t-1}^{p_{k_1}} s_t)$$

$$\therefore \ f_{ni} \propto \begin{cases} \bigcup_{j=1}^{p_{ni}} s_j, (f_{1i} \text{ is } SBF) \\ \bigcup_{j=k_1}^{q_{ni}} (\bigcup_{t-1}^{p_{k_1}} s_t), (f_{1i} \text{ is } NSBF) \end{cases}$$

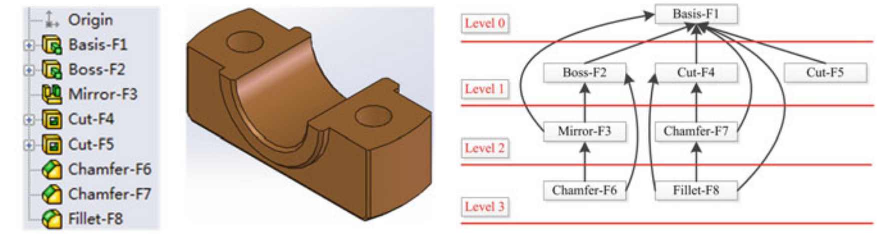
Step 2: To prove the primary shape of any CAD model is finally decided by a group of sketches.

$\because$ *According to Representation (2),* $M \propto \bigcup_{i=1}^{n} f_i$

$$\therefore \ f_i \propto \begin{cases} \bigcup_{j=1}^{p_i} s_j, (f_{1i} \text{ is } SBF) \\ \bigcup_{j=k_1}^{q_i} (\bigcup_{t-1}^{p_{k_1}} s_t), (f_{1i} \text{ is } NSBF) \end{cases}$$

$$\because \begin{cases} \bigcup_{j=1}^{p_i} s_j, (f_{1i} \text{ is } SBF) \\ \bigcup_{j=k_1}^{q_i} (\bigcup_{t-1}^{p_{k_1}} s_t), (f_{1i} \text{ is } NSBF) \end{cases} \quad \text{is a sketch set represented as } S_i$$

$$\therefore \ M \propto \bigcup_{i=1}^{n} S_i$$



(a) the feature tree **(b)** the CAD model **(c)** the DLG

Fig. 2 An example of the DLG

Theorem 1 *The shape of a CAD model is decided by all the sketches included in the CAD model.*

Theorem 1 can be proved as Table 2. In order to prove Theorem 1, a Dependence Level Graph (DLG) is defined first.

Definition 5 DLG: For a CAD model M, f_i is a feature and $f_i \in M$, N_i is a node of a DLG. $N_i = (id, level,$ parent$\{\}, children\{\})$. *id* denotes the id of f_i; *level* denotes the level of f_i in the hierarchical DLG (For instance, if the max level value of f_i's parent features is n, the *level* value of f_i is $n + 1$). *parent{}* is a set of f_i's parent features; *children{}* is a set of f_i's children features.

An example is given in Fig. 2. Figure 2a shows the feature tree of a CAD model, Fig. 2b shows the CAD model, and Fig. 2c shows the DLG of the CAD model.

As proved above, because the primary shape of a CAD model is decided by all the sketches belonging to the CAD model, the sketches of the CAD model are its key elements. The encryption of the sketch set in a CAD model realizes its shape encryption, and the encryption of a sub-set of the sketch set in a CAD model realizes its shape encryption.

3.1.1 Encryption of Sketches

The sketch in a CAD model is a 2D or 3D graph. The coordinate of point i in a sketch can be expressed as $(x_{i1}\ x_{i\ldots}x_{in})$, the sketch can be expressed as Representation (4), n denotes the dimension of the sketch and m denotes the number of points in the sketch.

$$\begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ x_{m1} & x_{m2} & \cdots & x_{mn} \end{pmatrix}, (n=2||n=3) \tag{4}$$

The goal of encrypting sketches is to protect the shape of a CAD model when it is shared and interoperated, so that there are two assumptions for the sketch encryption: (1) The encryption is secure enough; (2) The encrypted CAD model is valid (remains manifold) which can be shared and interoperated.

To meet the requirements, a random invertible matrix based encryption method is developed with the following characteristics. (1) The random invertible matrix transformation can defend almost all the common attacks. Because the encryption method is based on a random invertible matrix, various attack methods for the periodic matrix based transformation of graph are invalid; since the encrypting key is generated temporarily for every feature, the most dangerous "Known Plaintext Attack" (Rajput and Nishchal 2013) and "Chosen Plaintext Attack" (Barrera et al. 2010) for the periodic matrix based transformation of graph are also invalid; and the random invertible matrix is random, so that it is cannot be guessed. (2) The random invertible matrix transformation can change the shape of a feature, but its topology is not changed to guarantee the validity of the encrypted CAD model.

The realization process of the above is as follows. A_{nn} is a random invertible matrix, and S_{mn} is a sketch, the encryption of S_{mn} is as Representation (5):

$$S_{mn} \times A_{nn} = S'_{mn}, A_{nn} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \tag{5}$$

As the random invertible matrix is invertible, the inverse matrix of A_{nn} exists, represented as A_{nn}'. The sketch can be decrypted directly by its inverse matrix, as Representation (6):

$$S_{mn} = S'_{mn} \times A'_{nn} \tag{6}$$

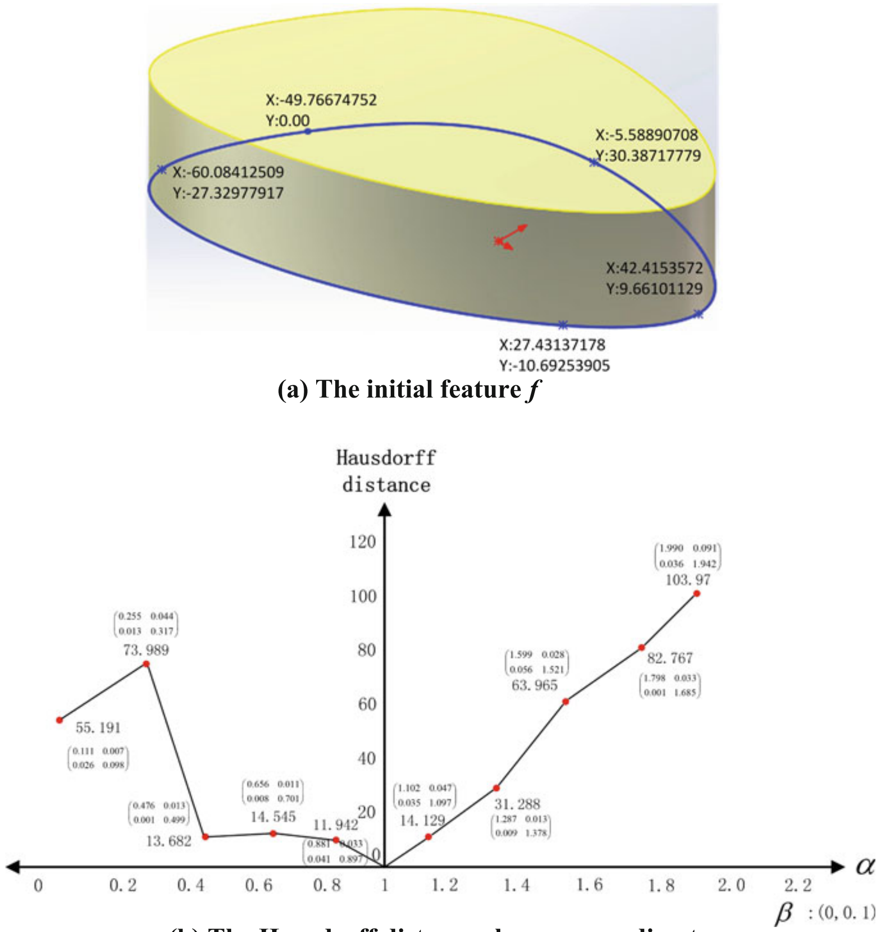
Because the features have a set of constraints, once the shape of a feature is changed, the following features maybe wrong. In order to guarantee the encrypted model is valid, the transformation of the feature should be able to be adjustable to some degrees.

For a point in a sketch, it can be described as $X = (x_1\ x_{2\ldots}x_n)$. According to Representation (4) and Representation (5), the transformation of the X is as Representation (6). Any element in the X' can be expressed as Representation (7):

$$X' = \begin{pmatrix} x_1 & x_2 & \cdots & x_n \end{pmatrix} \times \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} = \begin{pmatrix} x'_1 & x'_1 & \cdots & x'_n \end{pmatrix} \tag{7}$$

$$x'_i = x_i \times a_{ii} + (x_1 \times a_{1i} + x_2 \times a_{2i} + \cdots x_n \times a_{ni}) \tag{8}$$

The polynomial of $(x_1 \times a_{1i} + x_2 \times a_{2i} + \ldots x_n \times a_{ni})$ can be replaced by δ_i, Representation (8) is changed to Representation (9)



(a) The initial feature *f*

(b) The Hausdorff distance change according to α

Fig. 3 The transformation of the feature f

$$x_i^{'} = x_i \times a_{ii} + \delta_i \tag{9}$$

When $\delta_i << x_i \times a_{ii,}$ the transformation of x_i' based on the coefficient a_{ii} is similarly linear. Therefore the random invertible matrix is defined as Representation (10). α, β, Δ_1, Δ_2 are the parameters used to adjust the matrix.

$$A_{nn} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}, \ a_{ij} \begin{cases} i = j, \ a_{ij} \in (\alpha - \Delta_1, \alpha + \Delta_1) \\ i \neq j, \ a_{ij} \in (\beta - \Delta_2, \beta + \Delta_2) \end{cases}, \ |A_{nn}| \neq 0 \tag{10}$$

When $\alpha << \beta$, the transformation of the sketch is controllable. As shown in Fig. 3, the feature f is encrypted by different matrices, Fig. 3b shows the Hausdorff distance between the initial feature and the encrypted feature with different values of α (the Hausdorff distance is used to express the degree of similarity between two models (Tang et al. 2009)). When $\alpha << \beta$ (as the right of the axis), the change of the Hausdorff distance based on the adjustment of α is approximately linear. When the value of α is close to the value of β (as the left of the axis), the change of the Hausdorff distance based on the adjustment of α is uncertain.

Based on the above analysis, the transformation of sketches can be justified by changing the values of α and β to guarantee the validity of the CAD model. According to Representation (10), when $\alpha = 1$ & $\Delta_1 = 0$ and $\beta = 0$ & $\Delta_2 = 0$, the encrypted feature is the same to the initial feature, so the model is valid when the feature is encrypted. When $\beta << \alpha$, according to Representation (10), the effect of δ_i is stable, the transformation degree is mainly affected by the value of α, and the transformation is controllable according to the value change of α; when the β and α are close, according to Representation (6), the effect of δ_i is obvious and the transformation is uncontrollable according to the value change of α.

3.1.2 Encryption Algorithm of CAD Models

In order to support the flexible customized sharing of CAD models, every feature must have its own encryption key. The key generation algorithm based on Representation (10) is shown in Table 3.

Based on Algorithm 1 and Representation (1), the feature encryption algorithm is given in Fig. 4.

Table 3 Key_generation (α, β, Δ1, Δ2, n)

```
//$\alpha$, $\beta$, $\Delta_1$, $\Delta_2$ arethe adjusting parameters of the key and n is the dimension of key
double A[n][n];
do {
for (int i=0; i<n; i++)
for (int j=0; j<n; j++)
    {
if i=j
{ A[i][j]=**Random**($\alpha$,$\Delta_1$); } //means getting a random digit in the($\alpha$-$\Delta_1$, $\alpha$+$\Delta_1$)
else
    { A[i][j]=**Random**($\beta$,$\Delta_2$);}//means getting a random digit in the($\beta$-$\Delta_2$, $\beta$+$\Delta_2$)
    }
}while (|A|=0)
```

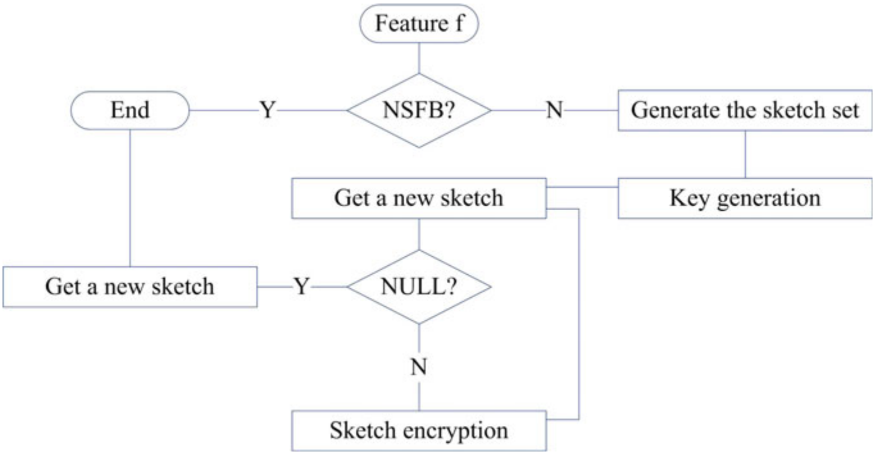


Fig. 4 Feature encryption algorithm

To support the flexible customized sharing of the CAD model, the encrypted model must be valid. According to Representation (1) and Representation (2), the validity of a CAD model in the model encryption is defined as follows.

Definition 6 If the features of the CAD model are created successfully, all the constraints of every feature are valid, so that the CAD model is manifold. As thus, the model is valid.

Based on the Definition 6, three conditions must be satisfied in the encryption process of a CAD model to guarantee the customized encrypted model is valid. The three conditions are as follows.

Condition 1: The CAD model *M*, is encrypted from bottom to top based on its DLG.

Condition 2: For any feature *f* in *M*, after the encryption of *f*, all the constraints of *f* are still valid and the *M* is manifold.

Condition 3: For any feature *f* in *M* and its any child feature *f'*, decrypt the *f'* after the encryption of *f*, all the constraints of *f'* are still valid and *M* is manifold.

A theorem for validity of CAD model is given as Theorem 2.

Theorem 2 *If the above three conditions are satisfied in the encrypting process of a CAD model, no matter which part is encrypted in the model, the encrypted model remains valid.*

The encryption algorithm of CAD models is given in Fig. 5, and Fig. 6 shows the encrypting procedure of a CAD model. When the feature of Cut-F4 is encrypted, Condition 2 is not satisfied, so that the value of α and β are adjusted to satisfy Condition 2. When the feature of Basis-F1 is encrypted, Condition 3 is not satisfied, so that the value of α and β are adjusted to satisfy Condition 3.

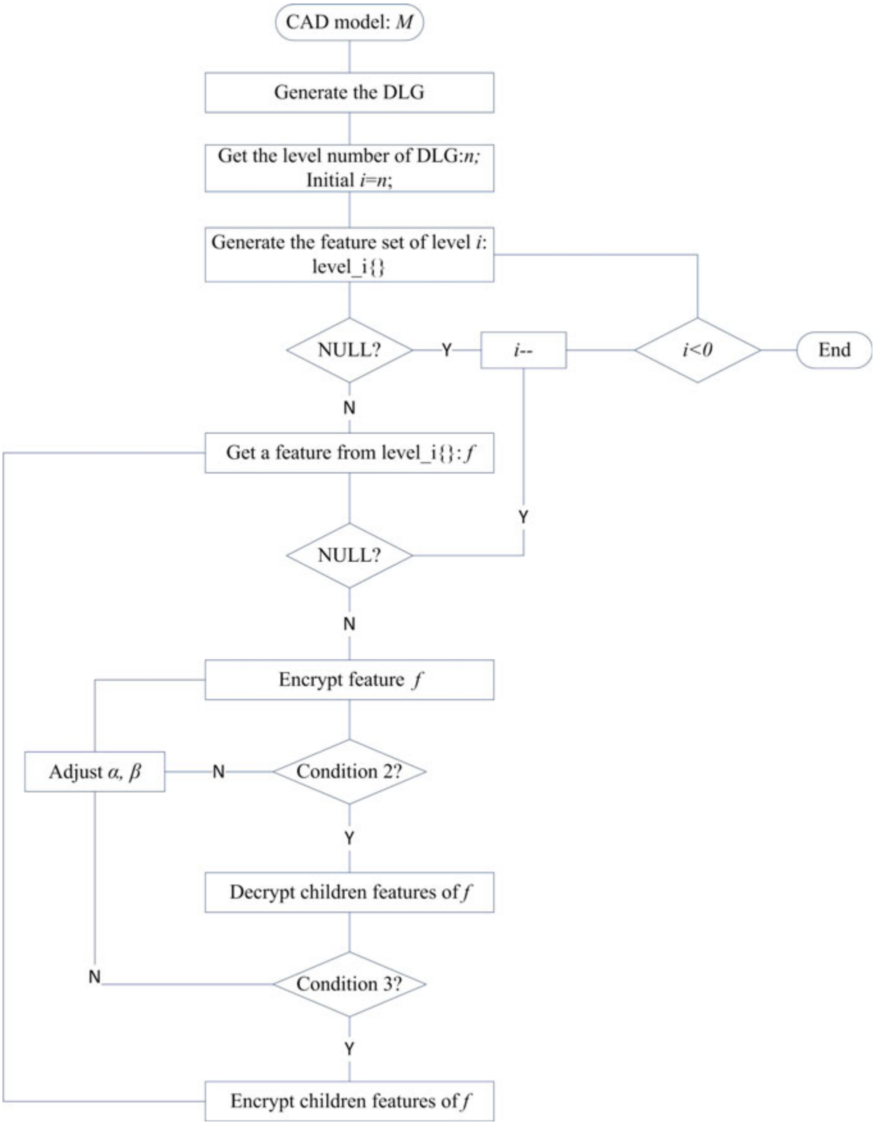

CAD model: M
Generate the DLG
Get the level number of DLG:n;
Initial i=n;
Generate the feature set of level i:
level_i{}
NULL?
Y
i--
i<0
End
N
Get a feature from level_i{}:f
Y
NULL?
N
Encrypt feature f
Adjust α, β
N
Condition 2?
Y
Decrypt children features of f
N
Condition 3?
Y
Encrypt children features of f

Fig. 5 Encryption algorithm of CAD models

3.2 *Encryption Based Secure Sharing of CAD Models*

3.2.1 Key-Based Authorization Algorithm

Before a CAD model is shared, the model owner should authorize the shared features for decryption and assign protected and public features. After the

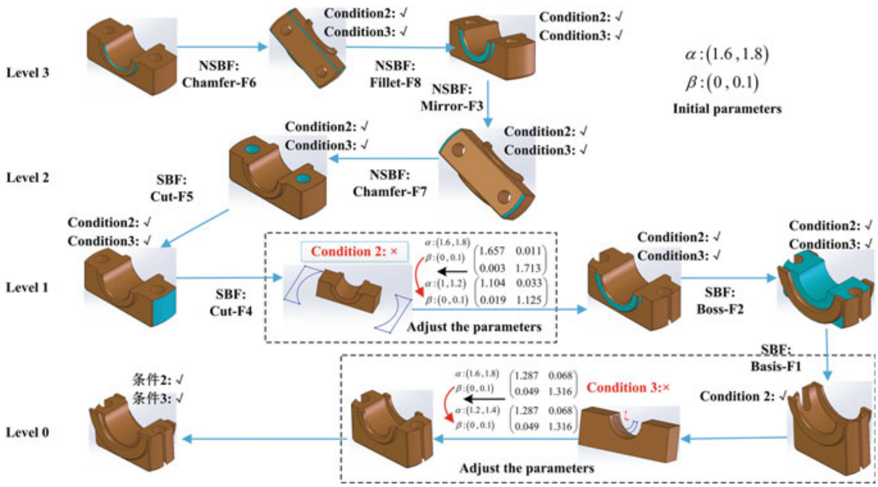


Fig. 6 The encryption procedure of a CAD model

Table 4 Authorization (*M*)

```
get the feature set of M: feature{}
initial key file Key_F.
while(feature{}!=NULL)
{
get $f_i$ from feature{}
if $f_i$ is public part
    {
  Key.id= $f_i$.id;
   Key. matrix=$f_i$.matrix;
  Key. attribution=Public;
    }
else if $f_i$ is sharing part
    {
  Key.id= $f_i$.id;
  Key.matrix=$f_i$.matrix;
  Key. attribution=Sharing;
    }
feature{}= feature{}- $f_i$;
   add key to Key_F
}
```

authorization is given by the model owner, the keys of shared features (the encryption matrices of the features) are retrieved from the Cloud Databases and recorded in an authorization file. The authorizing process is as in the following Table 4.

3.2.2 Customized Geometric Transformation Algorithm

When an authorized collaborator gets the encrypted CAD model and key file, the collaborator would visualize the model and interoperate on the shared features for collaboration. The CAD model owned by the collaborator has two parts: first part is geometric model and the second part is still feature-based on top of the geometric model. The geometric transformation algorithm contains the following three phases:

- **Model decryption**. The DLG of the encrypted CAD model (M_1) is created first, and then the CAD model is decrypted from top to down according to the key file based on the DLG (the decryption process is the inverse process of encryption). After the decryption, a decrypted model is generated: M_2;
- **Shared feature retrieval**. After the geometric transformation, the topology of the CAD model is changed. However, the constraints among features are based on the topological entities. Therefore it should to map the related topological entities into the decrypted model after the geometric transformation. When every shared feature is decrypted, its related information including the geometric representation of constraints and parameters are retrieved and recorded in an XML file;
- **Geometric transformation**. After the retrieval of the shared features, delete all the shared features from M_2, and the rest model is M_3. Then transform M_3 to M_4 which is a geometric format model. Later, retrieve the information of the shared feature from the XML file, and map the topological entities of position constraints based on their geometric representation. Finally, the shared features are recreated in M_4. After that, the final secure shared CAD model is generated: M_5.

4 Case Study for Approach Validation

A real example (provided by the SolidWorks 2012) is given below to verify the approach presented in this chapter. The propeller is one of the key parts in a plane. The design of vane contains rich design knowledge and semantics, so that in a collaborative scenario this feature and parameters should be protected. The following is the process of the applying the approach.

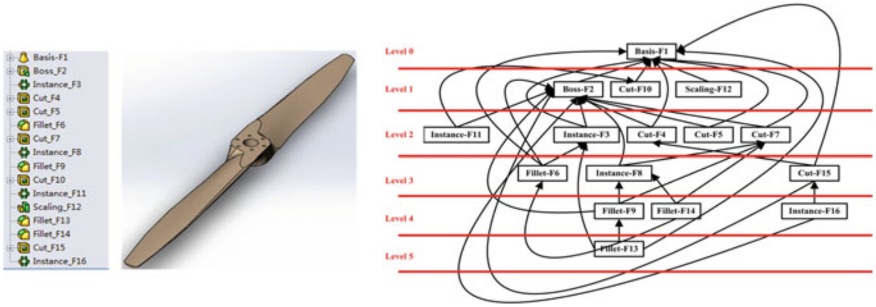
STEP 1: Model encryption

Figure 7a shows the propeller part (M_0) and its feature tree. Based on the feature tree, the DLG is created as Fig. 7b.

According to the encryption algorithm, M_0 is encrypted to M_1. Figure 8b shows the shape comparison between M_0 (in Green) and M_1 (in Red). Table 5 shows the difference of geometry attributions between M_0 and $M_{1.}$

STEP 2: Key-based authorization

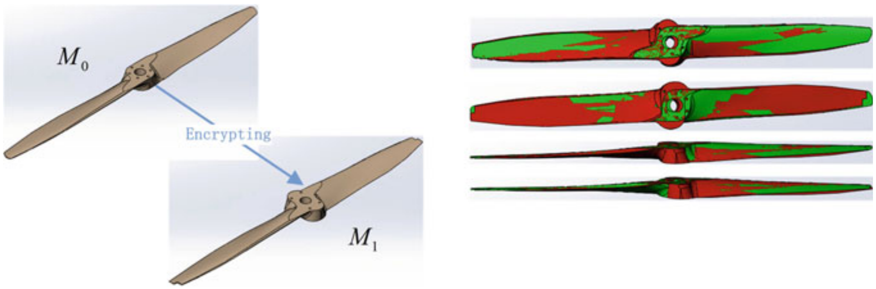
As shown in Fig. 9, when the propeller part needs to be shared, the protected features and shared features should to be assigned. The red part is protected part and it contains four features (Basis-F1, Instance-F3, Cut-F10, and Instance-F11), the



(a) The model M_0 and its feature tree

(b) The DLG of M_0

Fig. 7 The initial model M_0 and its DLG



(a) The M_0 is encrypted to M_1

(b) The shape comparison between M_0 and M_1

Fig. 8 M_0 is encrypted to M_1

blue part is shared part and it contains two features (Cut-F15 and Instance-F16), and the rest green part is public part and it contains all the rest features (Boss-F2, Cut-F4, Cut-F5, Fillet-F6, Cut-F7, Instance-F8, Fillet-F9, Scaling-F12, Fillet-F13 and Fillet-F14). According to the Authorization algorithm, all the keys of the features belonging to the blue part and green part are recorded into a key file. Finally, the key file and M_1 are sent to the authorized collaborator.

STEP 3: Decrypted model generation

Figure 10 shows the process of secure sharing. The details are below:

(1) According to the key file, M_1 is decrypted to M_2 (as in Fig. 10b).
(2) Retrieve the sharing features into an XML file. Figure 11 shows a part of the XML file and the feature information of Cut-F15.
(3) Delete the sharing features from M_2, and get M_3 (as in Fig. 10c).
(4) Transform M_3 to the geometric model, and get the M_4 (as in Fig. 7d)
(5) Recreate the sharing features based on the XML file in M_4, get the final shared model M_5 (as in Fig. 10e).
(6) M_5 is interoperated as Fig. 10f, and the propeller part is shared in a secure means.

Table 5 Comparison between M_0 and M_1

	Original M_0	Encrypted M_0: M_1
Mass (g)	65.67	77.96
Volume (mm^3)	65673.14	77959.78
Surface area (mm^2)	37741.96	40596.08

Center of mass (mm)	X = −6.90 Y = −1.51
	Z = −42.25
		X = −6.72 Y = −1.89
		Z = −37.99

Principal axes of inertia and principal moments of inertia: (g * mm^2)
Taken at the center of mass
	Ix = (0.01, −0.00, 1.00)
	Px = 6700.91
	Iy = (1.00, −0.00, −0.01)
	Py = 578276.11
	Iz = (0.00, 1.00, 0.00)
	Pz = 582857.97
		Ix = (0.01, −0.00, 1.00)
		Px = 11831.11
		Iy = (1.00, −0.00, −0.01)
		Py = 674162.27
		Iz = (0.00, 1.00, 0.00)
		Pz = 683256.19

Moments of inertia: (g * mm^2) Taken at the center of mass and aligned with the output coordinate system	Lxx = 578166.05,
	Lxy = 0.00, Lxz = 7930.56
	Lyx = 0.00
	Lyy = 582857.97,
	Lyz = 0.00
	Lzx = 7930.56, Lzy = 0.00,
	Lzz = 6810.97
		Lxx = 674125.01,
		Lxy = −0.34,
		Lxz = 4967.97
		Lyx = −0.34,
		Lyy = 683256.19,
		Lyz = −4.08
		Lzx = 4967.97,
		Lzy = −4.08,
		Lzz = 11868.38

Moments of inertia: (g * mm^2) Taken at the output coordinate system	Ixx = 695546.85,
	Ixy = 685.25,
	Ixz = 27076.50
	Iyx = 685.25,
	Iyy = 703215.49,
	Iyz = 4195.77
	Izx = 27076.50,
	Izy = 4195.77,
	Izz = 10088.03
		Ixx = 786920.83,
		Ixy = 992.83,
		Ixz = 24880.40
		Iyx = 992.83,
		Iyy = 799296.10,
		Iyz = 5607.88
		Izx = 24880.40,
		Izy = 5607.88,
		Izz = 15672.27

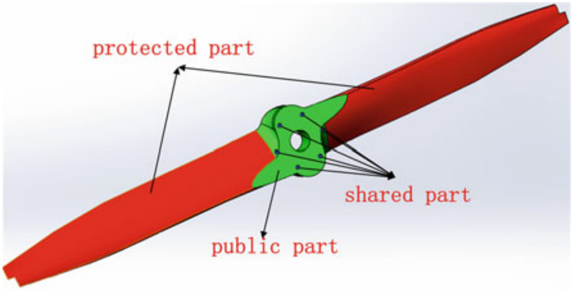


Fig. 9 Key-based authorization of M_1

(7) Figure 10g shows that the propeller part is shared directly without any secure mechanism. Figure 10f shows that the propeller part is shared securely based on the approach presented in this chapter. Figure 10h shows that, in the sharing of the propeller part, the shape of the vanes is protected, the green one is the initial part and the red one is the encrypted one.

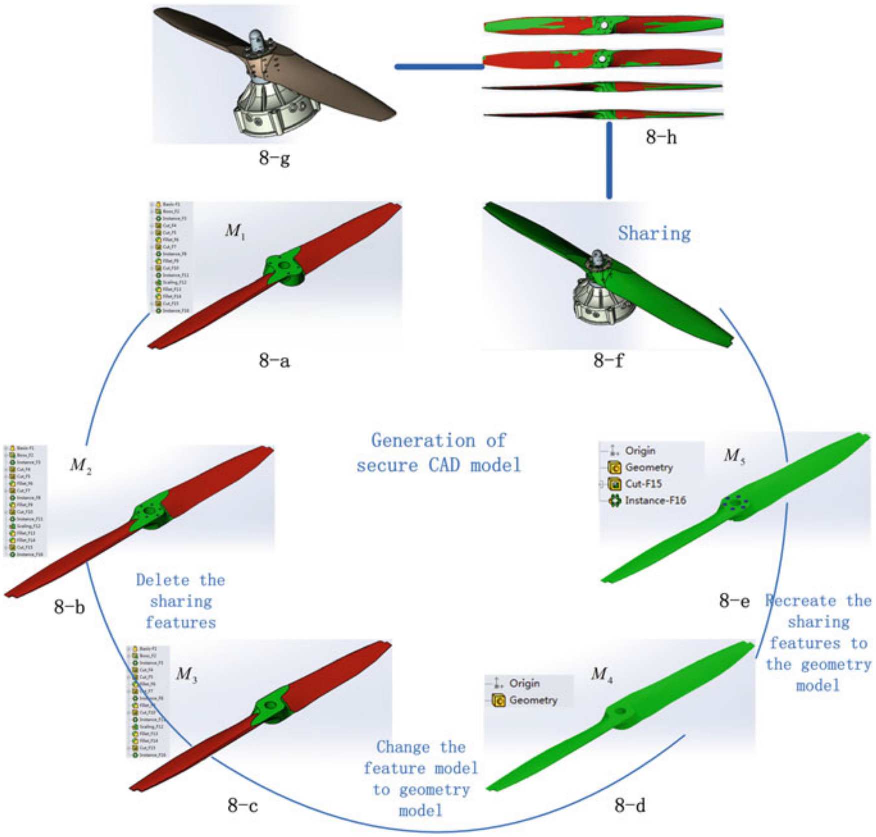
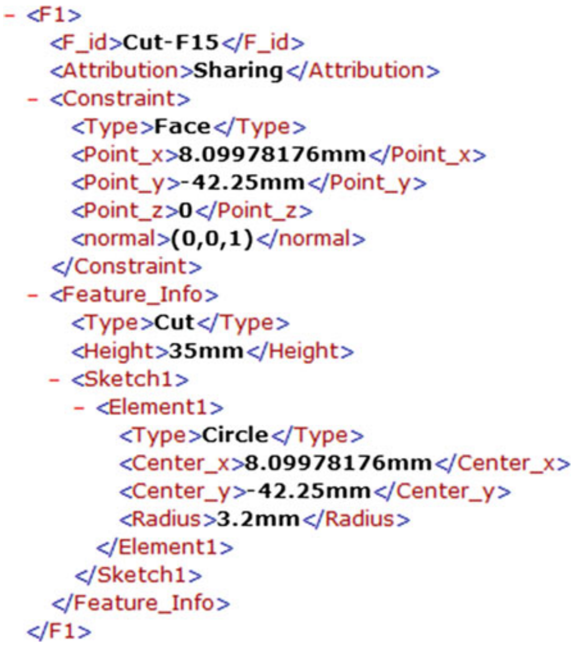


Fig. 10 The secure sharing of the propeller part

5 Conclusion and Future Works

In this chapter, an innovative encryption approach for CAD models in a cloud-enabled collaborative product development is presented.

The unique characteristic of the approach is that protected, shared and public information can be decided by a model owner flexibly. Based on the approach, different features have different keys, supporting the feature-based encryption and decryption of a CAD model under different collaboration scenarios. Besides, the encryption method is robust, so that no matter which feature of the CAD model is encrypted, the CAD model is still valid. Therefore, this approach provides a flexible, customized, and robust collaborative way for CAD model-based cooperation in cloud. A complex case study is used to prove the effectiveness and great potential industrial applicability of the approach.



```
- <F1>
    <F_id>Cut-F15</F_id>
    <Attribution>Sharing</Attribution>
  - <Constraint>
      <Type>Face</Type>
      <Point_x>8.09978176mm</Point_x>
      <Point_y>-42.25mm</Point_y>
      <Point_z>0</Point_z>
      <normal>(0,0,1)</normal>
    </Constraint>
  - <Feature_Info>
      <Type>Cut</Type>
      <Height>35mm</Height>
    - <Sketch1>
      - <Element1>
          <Type>Circle</Type>
          <Center_x>8.09978176mm</Center_x>
          <Center_y>-42.25mm</Center_y>
          <Radius>3.2mm</Radius>
        </Element1>
      </Sketch1>
    </Feature_Info>
  </F1>
```

Fig. 11 Part of the temporary XML file

The further research work is ongoing from two aspects. First, the protected and shared features need to be recognized automatically based on the analysis for the semantics of the CAD model. Second, the approach will be expended to the secure sharing of assembled products.

Acknowledgements This work is supported by the National Science Foundation of China (Grant No. 61303215), EU FP7 Smarter project (FP7-PEOPLE-2013-IAPP-610675) and EU FP7 Cloudflow project (FP7-2013-NMP-ICT-FoF-609100).

References

Ai QS, Liu Q, Zhou ZD et al (2009) A new digital watermarking scheme for 3D triangular mesh models. Signal Process 89:2159–2170

Barrera JF, Vargas C, Tebaldi M et al (2010) Chosen-plaintext attack on a joint transform correlate or encrypting system. Opt Commun 283:3917–3921

Belaziz M, Bouras A, Brun JM (2000) Morphological analysis for product design. Comput Aided Des 32(5–6):377–388

Cai XT, Li XX, He FZ et al (2012) Flexible concurrency control for legacy CAD to construct collaborative CAD environment. J Adv Mech Des Syst Manuf 3(6):324–339

Cayre F, Alface PR, Schmitt F et al (2003) Application of spectral decomposition to compression and watermarking of 3D triangle mesh geometry. Signal Process 18:309–319

Cera CD, Braude I, Kim T et al (2006) Hierarchical role-based viewing for multilevel information security in collaborative CAD. J Comput Inf Sci Eng 1(6):2–10

Chang HB, Kim KK, Kim YD (2008) The development of security system for sharing CAD drawings in u-environment. Comput Inf 5(27):731–741

Chou CM, Tseng DC (2006) A public fragile watermarking scheme for 3D model authentication. Comput Aided Des 38:1154–1165

Chu CH, Wu PH, Hsu YC (2009) Multi-agent collaborative 3D design with geometric model at different levels of detail. Robot Comput Integr Manuf 25:334–347

Conway R, Maxwell W, Morgan H (1972) On the implementation of security measures in information system. Commun ACM 15(4):211–220

Esam E, Ben A (2011) Secret sharing approaches for 3D object encryption. Expert Syst Appl 38:13906–13911

Han JH, Kim T, Cera CD et al (2003) Multi-resolution modeling in collaborative design. In: Proceedings of the eighteenth international symposium on computer and information Sciences, Antalya, Turkey

Hoppe H (1996) Progressive meshes. In: Proceedings of ACM SIGGRAPH

Huang Z, Liu GD, Ren Z et al (2009) A method of 3D data information encryption with virtual holography. In: Proceedings of SPIE-the international society for optical engineering 7125:71250E1–71250E7

Kim S, Lee K, Hong T, et a1 (2005). An integrated approach to realize multi-resolution of B-rep model. In: Proceedings of the 2005 ACM symposium on solid and physical modeling, Cambridge, Massachusetts

Lampson BW (1974) Protection. Oper Syst Rev 8(1):18–24

Lee JY, Lee JH, Kim H et al (2004) A cellular topology-based approach to generating progressive solid models from feature-centric models. Comput Aided Des 36(3):217–229

Lee SH (2005) A CAD-CAE integration approach using feature-based multi-resolution and multi-abstraction modelling techniques. Comput Aided Des 37(9):941–955

Lee SH, Kwon KR (2012) Robust 3D mesh model hashing based on feature object. Digit Signal Proc 22:744–759

Leong KK, Yu KM, Lee WB (2003) A security model for distributed product data management system. Comput Ind 50:179–193

Li S, Mirhosseini M (2012) A matrix-based modularization approach for supporting secure collaboration in parametric design. Comput Ind 63:619–631

Li WD, Cai YL, Lu WF (2007) A 3D simplification algorithm for distributed visualization. Comput Ind 58:211–226

Li WD and Mehnen J (2013) Cloud manufacturing. Springer series in advanced manufacturing, Springer

Naveen KN, Thomas JN (2011) Flexible optical encryption with multiple users and multiple security levels. Opt Commun 284:735–739

Oh S, Park S (2003) Task-role-based access control model. Inf Syst 28(6):533–562

Park J, Sandhu R (2004) The UCONABC usage control model. ACM Trans Inf Syst Secur 7 (1):128–174

Peng F, Lei YZ, Long M et al (2011) A reversible watermarking scheme for two-dimensional CAD engineering graphics based on improved difference expansion. Comput Aided Des 43:1018–1024

Qiu ZM, Wong YS, Fuh JYH et al (2004) Geomelric model simplification for distributed CAD. Comput Aided Des 36(9):809–819

Rajput SK, Nishchal NK (2013) Known-plaintext attack on encryption domain independent optical asymmetric crypto system. Opt Commun 309:231–235

Rouibah K, Ould-Ali S (2007) Dynamic data sharing and security in a collaborative product definition management system. Robot Comput Integr Manuf 23:217–233

Rutledge LS, Hoffman LJ (1986) A survey of issues in computer network security. Comput Secur 4(5):296–308

Sandhu R, Coyne E, Feinstein H (1996) Role-based access control models. IEEE Comput 29 (2):38–47

Seo J, Song Y, Kim S et a1 (2005) Wrap-around operation for multi-resolution of B-Rep model. In: Proceedings of CAD'05

Speiera C, Whippleb JM, Clossc DJ et al (2011) Global supply chain design considerations: mitigating product safety and security risks. J Oper Manag 29:721–736

Stevens G, Wulf V (2002) A new dimension in access control: studying maintenance engineering across organizational boundaries

Su ZY, Li WQ, Kong JS et al (2013) Watermarking 3D CAPD models for topology verification. Comput Aided Des 45:1043–1052

Tang M, Lee M, Kim YJ (2009) Interactive Hausdorff distance computation for general polygonal models. ACM Trans Graph 28(3): Article 74

Tao H, Zain JM, Ahmed MM et al (2012) A wavelet-based particle swarm optimization algorithm for digital image watermarking. Integr Comput Aided Eng 1(19):81–91

Tirkel AZ, Rankin GA, vanSchyndel RM et al (1993) Electronic water mark, Sydeny, Macquarie University

van der Hoeven A, ten Bosch O, van Leuken R et al (1994) A flexible access control mechanism for CAD frameworks. In: Proceedings of the conference on European design automation. Los Alamito

Wang WB, Zheng GQ, Yong JH et al (2008) A numerically stable fragile watermarking scheme for authenticating 3D models. Comput Aided Des 40:634–645

Xiang H, Li M (2012) The research of network security mechanism based collaborative design. Adv Des Technol 421:406–409

Yao KH, Shao J, Sheng GQ et al (2007) Research on a security model of data in computer supported collaborative design integrated with PDM system. In: IITA 2007: workshop on intelligent information technology application

A New Approach to Cyberphysical Security in Industry 4.0

Andre Wegner, James Graham and Eli Ribble

Abstract This chapter presents a new paradigm that limits and protects information flows to internal and subcontracted factory floor devices to complement perimeter security as essential first steps to secure manufacturing as it embraces Industry 4.0.

Keywords Direct-to-Machine Security · PLC (Programmable Logic Controller) · Additive Manufacturing · Operator audit · Design integrity

1 Introduction

Long value chains are among the biggest security concern in manufacturing for Industry 4.0. This is the case for all manufacturing but is especially critical in the military complex. In the USA, regulations trying to manage the situation, such as DFARS 252.204-7012, utilize Information Technology (IT) paradigms that don't reflect Operation Technology's (OT) unique circumstances and focus on perimeter security. Experts in the field privately acknowledge that this kind of solution will fail and compliance requirements will soon reflect this. The absence of a security

A. Wegner (✉)
Core Digital Manufacturing Faculty for Singularity University,
Nasa Research Park, Bldg 20, Moffett Field, CA 94035, USA
e-mail: andre@authentise.com

J. Graham
True Secure SCADA, 10415 W. Hwy. 42, Goshen, KY 40026, USA
e-mail: james.graham@louisville.edu

A. Wegner · E. Ribble
Authentise Inc., 8676 S 1300 E, Sandy, UT 84094, USA
e-mail: eli@authentise.com

J. Graham
Professor Emeritus (Electrical and Computer Engineering) for the University of Louisville,
Louisville, KY 40292, USA

L. Thames and D. Schaefer (eds.), *Cybersecurity for Industry 4.0*,
Springer Series in Advanced Manufacturing, DOI 10.1007/978-3-319-50660-9_3

approach that accepts this challenge while embracing increasing digitization in manufacturing means that confidentiality, integrity, and availability of manufacturing data are at risk.

A solution to this problem should be based on consideration of the special circumstances of OT. Many different types of data are accumulated during the production of a part or product and used to verify quality, predictive maintenance and more (Ballou 1998). However, only a few of them are critical to protecting intellectual property and integrity. It is these that an OT solution should focus on:

- Bill of materials
- Design information
- Control parameters

Due to its digitally integrated nature, Additive Manufacturing (or “3D Printing”) provides a fertile learning ground for this approach. The current 3D printing paradigm requires delivery of the design information and control parameters to an operator, who processes it and sends it to firmware and controller boards that operate the machinery. By contrast, the new approach presented in this chapter is to avoid giving critical data to any person or device other than the lowest level controller on the manufacturing system or systems. It generalizes an experience that is already standard in other digital industries and is becoming so in Additive Manufacturing. The solution embraces the digital manufacturing revolution delivering a connected, data-driven manufacturing process, instead of fighting it.

The next section of this chapter provides some background on computer security and explains how requirements for traditional IT cybersecurity differ from the cybersecurity requirements for Industry 4.0 manufacturing. The following section presents the secure manufacturing information architecture which addresses the security and information management for advanced digital manufacturing. The final section discusses a key component in this architecture, the manufacturing security enforcement device, and then conclusions and directions for future work in this area.

2 Background

Manufacturing cybersecurity had significant gaps even before the emergence of new manufacturing systems driven by increasingly digital devices. They highlight the security tensions as described below.

Cybersecurity and information assurance in IT systems revolve around three traditional central pillars: confidentiality, integrity and availability (CIA) (Bishop 2015). These three foundations are in tension with each other in any real IT system. For example, we can layer protections (physical and electronic) around our data and feel confident that it remains confidential and unchanged, but that is of little use if the data is not available to the person needing that data. On the other hand, making data readily available to legitimate users often means that it is also available to individuals who can glean unauthorized information (thus violating confidentiality) or can maliciously change the data (thus destroying its integrity). The activity of engineering efficient and practical IT cybersecurity systems involves carefully balancing these three objectives to yield useable and reasonably secure results.

The requirements for cyberphysical security of advanced digital manufacturing differ in a number of ways from security of traditional IT systems. IT cybersecurity stresses layered defenses around the central core servers with less attention to peripheral devices (we usually don't care if a remote printer gets hacked). Increasing Internet of Things adoption is putting a strain to that theory (Grau 2015). In digital manufacturing, in particular, we must protect BOTH the central design computer AND the remote manufacturing equipment. Increasing threats (Brocklehurst 2014; Krebs 2012) indicate that industrial control systems are becoming the target for malicious cyber intrusions.

Within this expanded sphere of protection, needed to provide enhanced security for manufacturing and other industrial control applications, the three central CIA objectives are still paramount. Manufacturing data should be confidential in that designs represent expenditures of considerable human and computer time to create, and the creating organizations should reap the full benefit from this effort. Design data must have integrity—it must arrive at the manufacturing equipment exactly in the format and content that it had upon creation. But finally, it must also be available to be produced at any approved equipment anywhere in the world.

The challenge to maintain availability will increase as manufacturing evolves from a centralized system supported by external suppliers to a distributed system in which production occurs closer to the point of use. This is, among others, of critical concern to the defense, aviation and shipping industries, which must ensure that original spare parts reach their intended target in a short timeframe. This "Distributed Manufacturing" paradigm requires extending trust to beyond a small set of contractual suppliers, to a network of thousands of manufacturing sites able to produce the required part at any time. This stretches potential points of failure to thousands of nodes, thus challenging the existing approach of building defenses around a core even further. Instead, Distributed Manufacturing requires extensive monitoring and control-based security to function.

The ecosystem that delivers these monitoring and security features is diverse and varied. At its heart stands the concept of triangulating insight from a myriad of sources, best encapsulated in the nascent Industrial Internet of Things campaign. This brings with it several benefits based on improved collaboration (Harper 2016). Having a variety of devices, including not only the manufacturing device but other internal and external sensors capture and transmit data intensifies the pre-existing cybersecurity threat. This escalates the need for the suggested focus on securing key data points that are part of the manufacturing process.

A further manufacturing-specific security challenge is that of maintaining integrity in a multipolar development environment. The information flow in manufacturing design and production planning is not unidirectional towards the end product but instead incurs many significant iterations between design, material, and production specialists, among others. These specialists may no longer be under the same roof or even in the same country, making it harder to protect them or their interactions. An acknowledgment of this iterative product development cycle and the distributed nature of modern experts highlights the production of the physical artifact as the weak link in a process, not as the irrelevant end of it. This, among other factors, also increases the pressure to connect previously air-gapped manufacturing devices. A lack of data flows both in and out of the machine will stunt the quest for greater efficiency, better products, and higher quality.

The increasing reliance on Computer Aided Manufacturing (CAM) is opening new attack vectors, such as attacks on the initial CAD drawings or its derivatives. Designs can be influenced in a variety of ways (scale, indents/protrusions, vertex movement) which are often subtle and difficult to discover before the part fails (Sturm 2014). This is most dramatically displayed in Additive Manufacturing devices, in which voids can be inserted into the internal geometry of the part to produce geometric failures that are silent, fully enclosed, and yield little discernable change to file size. The attack can be launched on the device firmware itself, similar to Stuxnet, or implanted in any part of the design or production process (in the STL file or the machine code). As most modern Additive Manufacturing devices have USB ports for maintenance, complex attacks may not be necessary. In a lab demonstration of this approach (by Sturm 2014), only one team of five was able to identify the attack by observing the print visually during production. In all others, there was a decrease in part strength of up to 14%. However, as others have demonstrated (Pan et al. 2017), the threat exposed most clearly in Additive Manufacturing stretches across digital manufacturing devices of all shapes and sizes (Fig. 1).

The architecture currently in use in the manufacturing environment does not address existing or emerging challenges. The design is typically entirely separated from the production environment, with manufacturing devices often air-gapped. As a result, there is no control over subcontractors in multi-step manufacturing value chains once data leaves the designer's server. Similarly, operators are also unsupervised once data is received and many issues emerge with data corruption as a result of the multi-tenanted control. The situation prevents bi-directional information flow in multi-polar development processes and is one of the key reasons why manufacturing has been relatively slow to adopt data-driven processes.

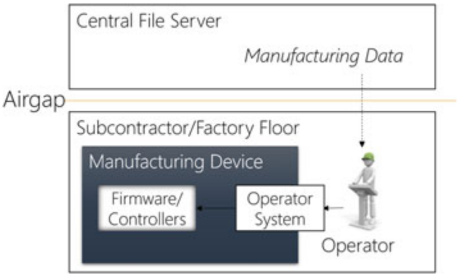


Fig. 1 Current manufacturing data flow

3 Secure Manufacturing Information Architecture

In this myriad of threats, refocusing on what represents critical information in the manufacturing process provides a starting point for better protecting the ecosystem. As discussed above, these include the bill of materials, the design file as well as control parameters. The end use for two of these, the design file and the control parameters, is the manufacturing device. Therefore, a more holistic approach to managing cyberphysical security threats in manufacturing is communicating such data directly with the relevant manufacturing device.

The fundamental problem is one of authentication and authorization: is the request to the manufacturing device authentic and is the actor requesting it authorized? For example, a technician has decided to supply a different material for a part than stated in the bill of materials. Is this request from a good actor? Is the actor authorized to make this request?

In answering these questions, we need to supply a couple of concepts. The first concept is asymmetric encryption keys. These keys come in two parts, a public half and a private half. Generally, the public half is published and used to verify or enforce that some entity possesses the private half. Keys may be held by a person, a machine, piece of software, etc. These keys can be used in encryption. If you have the public half of an entity's key, you can encrypt a message using that public half and send it to the entity. The entity can then decrypt the message with the private half (Fig. 2).

The second concept we need is that of a comptroller. A comptroller's job is to take some input data, provide a key, and store output data. The output data gets added to the end of a virtual document that becomes the record of provenance for a part that is produced. The comptroller is software that runs on a manufacturing network and authorizes each action taken on that network. A Manufacturing Security Enforcement Device (MSED) located close to or on the manufacturing device would cryptographically ensure the integrity of the transmitted data and is described in a separate section.

To illustrate the security architecture, we propose the following example: Let's suppose we want to manufacture a 10 mm cube of plastic. In a normal workflow

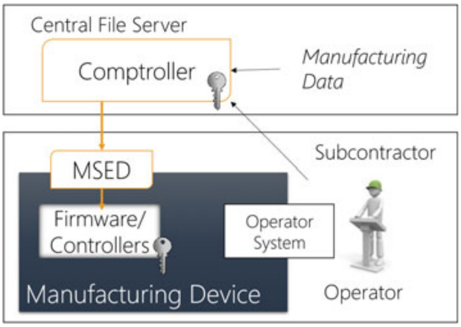


Fig. 2 Manufacturing workflow including a comptroller

today a designer would produce a CAD model of the 10 mm cube and a list of the material (PLA). These files would be provided to a technician who would use toolpath generation software to transform the cube's CAD file into a set of instructions for the printer. These instructions are then fed into the printer along with the PLA to produce the part.

There are many points of attack in this example as we described above: The CAD model could be modified, the technician could use the wrong filament, the machine could have some physical piece of hardware set outside of regular calibration or the toolpath instructions could be modified. Proper cryptographic protections can mitigate all of these attack vectors.

Let's look at this example again with a comptroller in place. At each phase, the comptroller authenticates and authorizes actions that are to be taken. First, our designer uses a CAD program to design the original cube. When the design is complete, the designer and the CAD program both supply their keys to the comptroller along with the original design. The keys confirm that the correct version of software was used and that the designer is allowed to design new models. This starts a new document for the provenance of the part identifying the designer as the root of the part. The designer then adds the bill of materials to the document indicating that this part must be printed using PLA. Later, when the technician generates the toolpath, the software tool he uses also is authenticated with the comptroller. This confirms that the technician is trained and permitted to prepare the file. The provenance document then gets a cryptographic signature with the technician's key and the toolpath generation software key. If the technician attempts any modifications of the original CAD model, the comptroller will refuse the change because the technician is not authorized to change designs, only to prepare toolpaths from the designs.

The toolpath becomes the latest part of the provenance document. The device that will manufacture the final part does not allow unencrypted toolpath bundles—all payloads must be encrypted using the device's public key and a key from the comptroller that the device has been bonded to. This means that the technician must first supply the toolpath he generates to the comptroller and indicate that he wishes to print on device X. The comptroller validates that the technician is authorized to use device X and then uses the public key for device X to produce an encrypted bundle. Device X then decrypts and validates the encrypted bundle. The bundle includes the toolpath, but it also includes the original bill of materials and CAD model since they are all linked by the same provenance document. Device X then validates that the plastic being supplied as part of the build is indeed the PLA required in the bill of materials. If the technician were to mount the wrong material, the build would not proceed. If the technician were to modify the encrypted bundle to sabotage the toolpath, the bundle would no longer cryptographically validate with device X.

During the manufacturing process device X communicates a stream of telemetry data (cryptographically signed) to the comptroller. This telemetry data is attached to the provenance document. QA processes can disqualify the build by analyzing this data and confirming that sensors are within tolerance bands. If our technician kicks

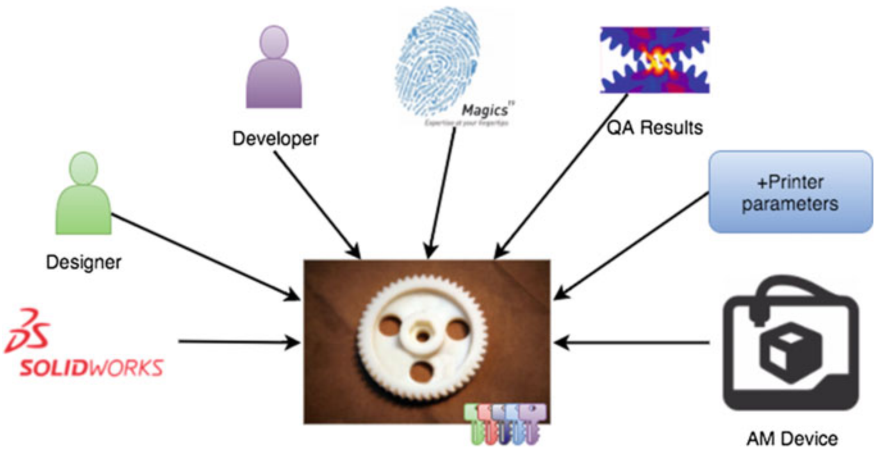


Fig. 3 Data flows managed by the comptroller

device X to sabotage the build, the comptroller can get cryptographically secure data from accelerometers that detect the kick that automatically become part of the history for the individual part (Fig. 3).

This forms the basis for a secure digital manufacturing system: A centralized authentication and authorization entity driven by asymmetric key cryptography and open standards that vendors throughout the ecosystem can implement. This includes CAD software makers, toolpath generators, static analysis, telemetry data gathering, hardware manufacturers, intrusion detection suites, and PLM. Each node in the network need only define what its inputs and outputs are, the permissions required for each action it can take, and a way to supply its key and the key of its user. This ensures a cryptographically secure chain of information about who did what with when using which tool.

Because the system relies on fine-grained, role-based controls, it works both within an organization as well as between organizations. If the comptroller is accessible across the public internet, our example above works the same way even if the original designer and the technician are on separate continents in different organizations under different legal jurisdictions. Data access and modification are based on the availability of authorized keys, not on the presence of legal contracts. Data is encrypted while in transit and only decrypted by the target software and only when it has access to the user's key. Defenses can be further hardened by using key escrow and multi-factor authentication.

From a security standpoint, it is just as important to know the origin of a part as it is to control how a part is produced. It doesn't matter if a bad actor sabotages a fuel injector nozzle as it is being built if they can more easily swap out the fuel injector nozzle for a faulty fake. Accurate part history is then the key to cyber-physical security.

For each part in the system, the comptroller maintains signed data about who took each step and which tool they used. In final part production, the comptroller stores a log of sensor data as the part is being produced. The part can be designed in such a way as to leave voids where uniquely identifying information can be added. This may include manipulations to support structures, changes to infill that respond to X-ray in particular patterns, barely-visible dots on an outer surface, or a serial number etched into the same location (Aliaga and Atallah 2009; Willis and Wilson 2013). These changes can be applied by the manufacturing device itself or as part of the toolpath generation. In either case, they represent a branching of the basic instructions that is unique for each physical part. Different industries will have different requirements and regulations around how this can and should be done, but the ultimate goal is the same: a person can take the part, look up the ID number, and request the full chain of history on the part. This prevents attacks involving supply pollution.

The chain of history can be maintained across organizations. If a prime contractor has several subs, each sub can register an organizational key with the comptroller. Each step they take in fulfilling the contract is then signed by their organization, their users, and their tools. Only data that the organization has been explicitly given access to leaves the comptroller.

In a workflow where different organizations take ownership of the produced artifacts over time, the model still works. This is a critical element as different actors expect to provide a wide range of services (Harper 2016). Each organization has their own comptroller. When an artifact, such as a CAD model, leaves one organization's control and enters another the comptroller negotiates a handle. The original comptroller notes the end of the provenance document as a handoff to a new owner. The receiving comptroller starts a new provenance document signed by the original owner indicating where the artifact came from. Tracking the history of the artifact requires communicating across organizations, but automated systems operating over the public internet makes this easy and automatable. New ledgers built on blockchain technology may be able to enforce these hand-offs should the networks become too large.

The architecture we propose here isn't without its drawbacks. Having a centralized source of authority creates a single point of failure in critical systems and a single primary target of attack for malevolent actors. There are mitigation strategies that we can employ, however.

Uptime is less of an issue than it may seem. It's simple to federate any number of comptrollers and configure them to treat one another's signature as authoritative. A single, federated data store can service the entire cluster of comptrollers if they share encryption keys, or if different clusters of comptrollers can share the underlying data. This makes it possible to take parts of the data store offline while keeping the rest available. In either storage strategy, any single comptroller can validate the provenance chain of other members of its cluster and treat them just as authoritatively, as its own history.

The far thornier issue is how to defend the comptroller as the holder of the keys. If an attacker can exfiltrate encryption keys, they can forge history. The forgery only holds up if the attacker can then surreptitiously insert the forgery into the data store or pose as the comptroller to an external organization. If the attacker can manipulate the comptroller's data store, they could modify data access permissions or sabotage parts in any number of ways. None of this is actually more dangerous than operating without a comptroller at all. Without a comptroller, flat files are open to being manipulated at any point of transit or use, and no one would be the wiser.

Good defense-in-depth for a comptroller involves many layers. First is appropriate physical access controls and network firewalls. A comptroller can be physically secured well beyond what a shop floor would normally require as it is a data service over a LAN. That LAN should include physical intrusion detection mechanisms that can do things like limit IO when threats are encountered. Proper network gateways and firewalls can logically separate the types of data and commands that can flow through the comptroller. Air-gaps may be appropriate for certain use cases. Analysis of system logs can spot errant behavior after-the-fact. Ultimately, the comptroller should be treated with the same IT security policies that organizations employ for their file servers, domain controllers, and other sensitive data services. The added benefit is that once data leaves a file server perimeter, it is forever lost and unprotected. When data leaves the comptroller's security perimeter, it is encrypted and protected reducing the overall attack surface of the organization.

So far we've only discussed documents as single entities: a CAD model, the toolpath instructions for a particular part, the entire history of a part's creation. We can broaden this idea further when we realize that the comptroller idea is designed not to produce artifacts but to control, record, and secure operations. Operations are performed on documents—manipulations to the CAD model, constraints on the toolpath generation process, updating the Bill of Materials—but if we treat the operation as the central focus for a comptroller we open new opportunities for innovation. A CAD program that can communicate with the comptroller can begin to stream operations to the comptroller rather than just check-out and check-in documents. This not only keeps an ongoing history of the different design approaches attempted but allows the comptroller to immediately constrain the operator based on system policies and events. This becomes especially meaningful for technicians operating the manufacturing machinery. With a secure connection to the comptroller and a stream of control signals, the technician can be controlling digital manufacturing equipment in real time under the IP constraints of the design owners.

3.1 Pilot of Direct-to-Machine Security

In a commercial pilot, Authentise provided the service of securing prints to multiple online retailers of printable designs. These include toyfabb.com, cults3d.com, and others. Upon the sale of the design, Authentise's clients transmitted the design and information to Authentise's Comptroller, which then issued a link to the recipient to print. The recipient used the link first to connect their 3D printer to the Authentise

Comptroller and finalize the settings. Using those inputs, the Authentise Comptroller connected to the printer using a secure channel, prepared the machine-readable code, and sent the resulting commands into the printer. Simultaneously the print is monitored and resulting information sent to both the recipient and Authentise's client. This system is in the process of being extended to other g-code reading devices, such as CNC machines.

4 Manufacturing Security Enforcement Device

The MSED plays a key role in maintaining the end-to-end security of the secure manufacturing information architecture and is thus discussed in more detail in this section. This device sits immediately in front of the manufacturing equipment and authenticates the manufacturing instructions which come from the cloud. As the final arbitrator as to whether or not a part gets produced, this device plays a critical role in the overall secure manufacturing information architecture. Together with the other components, it assures that only information sent by an authenticated comptroller will be produced and that the message has not been altered between the cloud and the manufacturing center.

The MSED must perform near real-time decryption of the incoming data stream. As discussed previously, confidentiality of data in traditional manufacturing systems has not been a priority and most manufacturing systems data is not encrypted. The details of the part design are proprietary to the design firm and must be protected until the information is at a trusted manufacturing site. Some latency in the transfer and buffering of the incoming data stream can be supported as a few seconds of delay in the start of the manufacturing activity will not affect overall manufacturing performance.

The essential feature of the MSED is the ability to perform authentication of the design file. Was it produced by the design firm indicated in its pedigree? And was it transmitted through the cloud system without modification? A number of approaches can be used to attempt to provide this needed authentication. The best of these are cryptographically based involving computation of a unique, digital signature of the design file and the creating authority which can be verified by the MSED at the manufacturing site. Public Key Infrastructure (PKI) approaches can be used as well as Hash Method Authentication Codes (HMAC) approaches, with the latter usually requiring less computational power.

Finally, it is desirable that the MSED have a secure operating system base. Many embedded systems use real-time operating systems which are based either on Microsoft WindowsTM or LinuxTM. While these operating systems offer a large base of I/O interface drivers, networking and file systems support, and other useful software, they also contain millions of code and the unwanted byproduct of zero-day (or unknown and thus unanticipated) cyber vulnerabilities. Attacks against these unknown vulnerabilities can be devastatingly effective. Recently, alternate, smaller operating bases, designated as micro-kernels, have become available for embedded systems use. The best of these is seL4 which has been mathematically verified to be secure (Klein et al. 2014).

Several companies currently offer products designated as industrial firewalls that offer some of the needed functionality of the MSED. These products all operate within the process control network to protect field devices such as programmable logic controllers, remote terminal units, and intelligent electronic devices by filtering incoming process network traffic.

5 Pilot of the Manufacturing Security Enforcement Device

True Secure SCADA, LLC, has recently completed a prototype MSED device utilizing the seL4 microkernel. It can be used in general industrial control applications as well as manufacturing applications. The device has been tested successfully in its laboratories for function and compatibility with industrial control devices and protocols and in currently undergoing field tests in several industrial installations. A complete overview of this device is given in (Graham 2016).

6 Conclusion

The outlined direct-to-machine communication approach can overcome the cyberphysical security challenges that arise from modern manufacturing techniques. It does so by streaming critical data directly into machines via a centralized authentication and authorization process. In particular, the solution characteristics include:

1. **Granular Authorization**: Several levels of permission for access, preview, editing, and authorizations to ensure individual users and groups only have necessary access.
2. **Monitored Operator Control**: Operator control is maintained while being monitored and restricted, if applicable.
3. **Device Support**: Due to a thin, operating client, most digital manufacturing devices can be supported, and legacy devices are easy to integrate.
4. **Distributed Responsibility**: Different sectors for manufacturing device, design owner, design transformation, and other factors spread the security risk from a single point of failure.
5. **Location Independent**: The solution can be deployed in central or hosted IT infrastructure.
6. **Data Fragments**: Only the data necessary for execution is transferred, and may be streamed for further protection.

Without such an approach, progress towards a more digitally-enhanced manufacturing environment able to improve productivity and produce higher quality and more relevant products is likely to be slow. Connecting manufacturing devices is a critical part of delivering such improvements, but without addressing legitimate security concerns, they will not progress.

In contrast to existing solutions, the direct-to-machine approach provides security in a number of meaningful ways:

1. **Integrated Security**: Direct-to-Machine Security builds on existing IT security solutions, which can be deployed to enhance the system.
2. **Layered Encryption**: Encryption in transfer with high-grade TLS and multi-layered encryption at rest with 256-bit AES. Encryption keys securely stored in separate locations.
3. **Always Up-to-Date**: Thin clients on devices mean that only central infrastructure needs updating.
4. **Minimum Sharing**: Authorized endpoints only receive minimum data required for execution.
5. **Integrity Protection**: In addition to theft, the delivery of lowest level data protects design integrity. Version, deletion, and expiration controls.
6. **Secondary Defense**: If data does leave the system it is traceable through watermarking and challenging to reverse engineer into a general design file.
7. **System Redundancy**: N + 1 or greater redundancy for all network components and system components.
8. **Threat Protection and Prevention**: Uninterruptible power and backup systems, as well as fire/flood detection and prevention, are used at storage sites.

The solution does not only enhance security and enable innovations to flourish; it creates a more responsive manufacturing environment better suited to the realities of today’s shop floor. In particular, the solution:

1. **Permits Detailed Tracking**: Comptroller creates and tracks complete history of the part.
2. **Encourages Collaboration**: Security and central repository enable different firms and individuals to operate on their strengths: provide a small iteration to the design, run an engineering simulation, or complete material testing.
3. **Enables Distributed Manufacturing**: Trust in the network and ability to capture device feedback in real time allows production of parts closer to the point of use, enabling an entirely new, supply chain system.
4. **Delivers Automation**: Central processing improves automation potential as bottlenecks are identified, solutions can be more easily iterated on and deployed at scale.

Adopting a new security approach won’t be easy. There are natural challenges with the approach, such as the necessity of a single point of failure. Mitigants, examples of which have already been discribed above, will need to be found in cross-industry collaboration. It is likely that these challenges will only be addressed when the will to handle the overwhelming cyberphysical security risk in manufacturing has risen. While we have outlined that handling this problem is as much addressing a risk as it is unlocking an opportunity, the awareness of this among manufacturing executives is still low. Most likely the defense community, whose losses of manufacturing data have a cost that could go well beyond the billions of dollars in book value, will have to make this a compliance issue.

The alternative is that IT departments across the country begin to recognize manufacturing equipment as just another digital asset that needs protecting, and that the direct-to-machine approach is just a natural extension of an approach that they are already using to secure other types of data flows. What has changed is that manufacturing devices are now no longer separate from but part of that data flow. The direct-to-machine manufacturing approach is, for the first time, an approach to acknowledge that and move manufacturing into the digital century.

Acknowledgements This work is partially supported by Benjamin Collar (Siemens), Dr. Jeffrey Hieb (University of Louisville), and William Sobel (System Insights and MT Connect). The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

References

Aliaga D, Atallah M (2009) Genuinity signatures: designing signatures for verifying 3D object genuinity. Comput Graph Forum 28(2):437–446. doi:10.1111/j.1467-8659.2009.01383.x

Ballou D, Wang R, Pazer H, Tayi G (1998) Modeling information manufacturing systems to determine information product quality. Manage Sci 44(4):462–484. doi:10.1287/mnsc.44.4.462

Bishop M (2015) Introduction to computer security. Addison-Wesley, Boston

Brocklehurst K (2014) DHS confirms US public utility's control system was hacked. The State of Security Newsletter. https://www.tripwire.com/state-of-security/incident-detection/dhs-confirms-u-s-public-utilitys-control-system-was-hacked/#. Accessed 12 Dec 2016

Grau A (2015) Can you trust your fridge? IEEE Spectrum 52(3):50–56. doi:10.1109/mspec.2015.7049440

Harper K, Gooijer T, Smiley K (2016) Composable industrial internet applications for tiered architectures. ABB Corporate Research. https://www.researchgate.net/publication/301846825_Composable_Industrial_Internet_Applications_for_Tiered_Architectures. Accessed 3 Dec 2016

Klein G, Andronick J, Elphinstone K, Murray T, Sewell T, Kolanski R et al (2014) Comprehensive formal verification of an OS microkernel. ACM Trans Comput Syst 32(1):1–70. doi:10.1145/2560537

Krebs B (2012) DHS warns of hactivist treat against industrial control systems. Krebs on Security. https://krebsonsecurity.com/2012/10/dhs-warns-of-hacktivist-threat-against-industrial-control-systems/. Accessed 3 Dec 2016

Graham J, Hieb J, Naber J. (2016) Improving cybersecurity for industrial control systems. In: 2016 IEEE 25th international symposium on industrial electronics (ISIE). doi:10.1109/isie.2016.7744960

Pan Y, White J, Schmidt D, Elhabashy A, Sturm L, Camelio J et al (2017) Taxonomies for reasoning about cyber-physical attacks in IoT-based manufacturing systems. Int J Interact Multimedia Artif Intell 4(3):45. doi:10.9781/ijimai.2017.437

Sturm L, Williams C, Camelio J, White J, Parker R (2014) Cyber-physical vulnerabilities in additive manufacturing systems. In: Solid freeform fabrication symposium 2014. http://sffsymposium.engr.utexas.edu/sites/default/files/2014-075-Sturm.pdf. Accessed Aug 2016

Willis K, Wilson A (2013) InfraStructs. ACM Trans Graph 32(4):1. doi:10.1145/2461912.2461936

SCADA System Forensic Analysis Within IIoT

Peter Eden, Andrew Blyth, Kevin Jones, Hugh Soulsby, Pete Burnap, Yulia Cherdantseva and Kristan Stoddart

Abstract A new wave of industrial technology has emerged in the form of Industry 4.0, which has seen a progression from electronic devices and IT (Information Technology) systems that automate production advance to a new revolution of Cyber-Physical Production Systems used for Smart Manufacturing and Smart Factories via IIoT (Industrial Internet of Things). As more and more devices are becoming connected and networked to allow for Smart Manufacturing to take place the number of data sources significantly increases as a result. Real-time Information is then becoming increasingly interlinked across multiple industries for a more efficient productivity process and a reduction in cost. Aside from Smart manufacturing and factories, Industry 4.0 has already seen huge advances in infrastructure management, energy management, transportation and building and home automation. With such industries relying so heavily on real-time data from connected sensors the security of these systems are at risk due to the reliance on low-latency and reliable communication for critical processes. The increase of interconnected networks and devices

P. Eden (✉) · A. Blyth
Information Security Research Group, Faculty of Computing, Engineering and Science,
University of South Wales, Wales, UK
e-mail: peter.eden@southwales.ac.uk

A. Blyth
e-mail: andrew.blyth@southwales.ac.uk

K. Jones · H. Soulsby
Cyber Operations, Airbus Group Innovations, Cyber, UK
e-mail: kevin.jones@airbus.com

H. Soulsby
e-mail: hugh.soulsby@airbus.com

P. Burnap · Y. Cherdantseva
School of Computer Science and Informatics, Cardiff University, Cardiff, UK
e-mail: BurnapP@cardiff.ac.uk

Y. Cherdantseva
e-mail: CherdantsevaYV@cardiff.ac.uk

K. Stoddart
Department of International Politics, Aberystwyth University, Aberystwyth, UK
e-mail: kds@aber.ac.uk

L. Thames and D. Schaefer (eds.), *Cybersecurity for Industry 4.0*,
Springer Series in Advanced Manufacturing, DOI 10.1007/978-3-319-50660-9_4

across the Internet significantly increases the amount of entry points into these systems, increasing their vulnerability and allowing outsiders to take advantage of any weaknesses within them. This has already been highlighted by the events of Stuxnet, Havex, Black Energy and the German Steel Mill that targeted ICS (Industrial Control Systems) and SCADA (Supervisory Control and Data Acquisition) Systems causing catastrophic results. The use of SIEM (Security Information and Event Management) services, IDS (Intrusion Detection Systems), IPS (Intrusion Prevention Systems) and firewalls may be implemented within ICS but only operate on the perimeters of their networks or segmented networks and not at the lower operational level where critical processes rely on speed and availability simply because by doing so could introduce latency between critical processes. When events do occur, regardless of whether an incident is accidental or deliberate, an immediate incident response should take place. This chapter focusses on the forensic challenges and analysis of the physical infrastructure that underpins the systems operating within IIoT. It discusses the development of SCADA system architecture over the past few decades and how it has arrived at IIoT, creating the new generation of SCADA systems. The chapter then discusses the current available tools that exist that can help carry out a forensic investigation of a SCADA system operating within IIoT space before closing with a suggested SCADA Incident Response Model.

1 Introduction

The Industrial Internet of Things can be thought of as the next generation of SCADA systems providing the underlying infrastructure for much of the worlds critical infrastructure, such as nuclear plants, oil refineries, water treatment, manufacturing, energy and transport. These systems build on their existing infrastructure by introducing cloud based technologies into the overall network topology. A SCADA system is a hugely distributed computerised system often spanning huge geographical areas, that gathers and analyses real-time data from field devices to automate, monitor and control physical processes. SCADA systems, essentially, monitor and control a network of Programmable Logical Controllers (PLCs) and Remote Terminal Units (RTUs) that use sensors to measure performance of local operation and provide automation. A SCADA control centre collects data from field devices and allows for human interaction and supervisory control of these devices from a central location. IIoT convergence with SCADA has seen more and more control being placed in the cloud.

Originally, SCADA systems were designed to operate on closed networks, using an "air gap" to physically separate them from local networks and the Internet, and therefore minimising the risk of intrusion from the outside. Their main focus had been on making the data available but not necessarily secure or confidential. Over the years, the developments in technology have resulted in SCADA systems communicating over, TCP/IP (Transmission Control Protocol/Internet Protocol), wireless IP

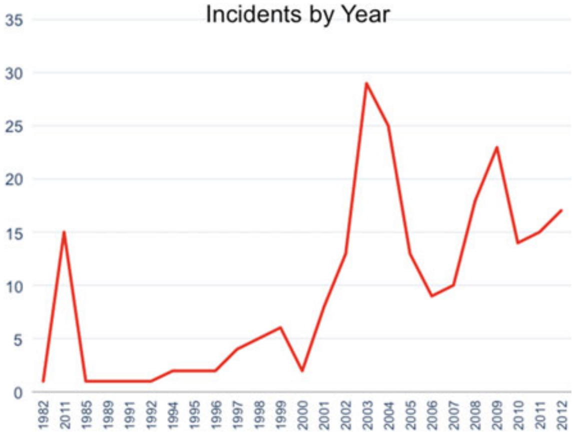


Fig. 1 RISI—no. of ICS incidents per year

and Bluetooth increasing their vulnerability to external attacks. We have seen dedicated attacks on CNI (Critical National Infrastructure) such as Stuxnet, Flame and Duqu.

Figure 1 clearly shows the number of reported incidents steadily rising from 1982 before jumping significantly in the early 2000s. This dramatic change in figures can be attributed to the fact that, around this time, more and more SCADA systems started communicating via TCP/IP and being connected to corporate LAN (Local Area Network). The figures start to decline around the mid 2000s before rising again towards the end of the decade. With IIoT bringing more and more interconnectivity through the cloud and across the internet the number of entry points into a SCADA environment increases, making them more vulnerable and therefore providing more opportunity for attackers to exploit.

When incidents occur it is vital for a forensic investigation to take place to determine the cause and those responsible, but due to the bespoke elements of SCADA systems traditional IT forensic tools and methodologies cannot be applied.

1.1 SCADA Progression and the Development of IIoT

Since the introduction of SCADA into ICS there has been some significant changes and evolutions to the SCADA system architecture that has led to the IIoT revolution.

1.1.1 Monolithic SCADA System

In its infancy SCADA architecture consisted of a centralised standalone mainframe system, with strictly no connectivity to another systems. WANs (Wide Area Networks) allowed for communication between mainframe and various RTUs, using

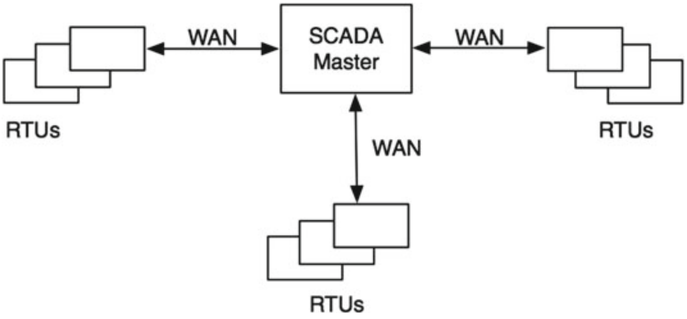


Fig. 2 Monolithic SCADA system

proprietary protocols developed by the RTUs manufacturer and supporting very limited functionality other than carrying out what was required of them. Monolithic systems also made use of a second identical mainframe system that acted as a backup in the event of any redundancy of the master (McClanahan 2003) (Fig. 2).s

1.1.2 Distributed SCADA System

With the introduction to LAN technology, within SCADA, processing could be distributed across many systems allowing for specific station functionality to communicate and share information in real-time with other stations connected to the LAN. This increased the overall processing power of the system. Rather than using mainframes for each station the SCADA architecture now utilised system miniaturisation and now implemented minicomputers at a much lesser cost (Karnouskos and Colombo 2011). Networks were limited to the local environment and the proprietary protocols used were still vendor-specific which limited the networking of different manufacturers devices (McClanahan 2003) (Fig. 3).

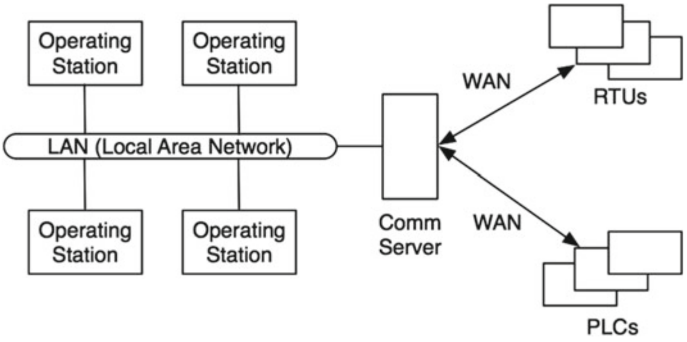


Fig. 3 Distributed SCADA system

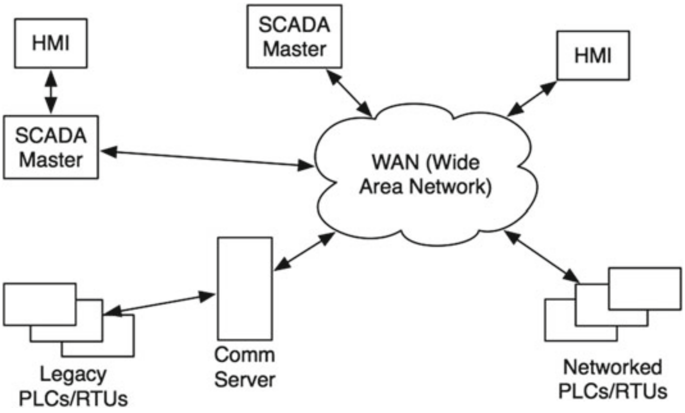


Fig. 4 Networked SCADA system

1.1.3 Networked SCADA System

The emergence of the current networked SCADA system applies the use of open architecture allowing for multi-vendor devices to be networked. It also incorporates open protocols and standards that allows for distributed SCADA functionality across the WAN Rutherford (2012). Significantly, it meant that third party peripheral devices could connect to the network and for communication between master stations ad field devices via IP (McClanahan 2003) (Fig. 4).

ICS and SCADA Information Security Principles are normally in the order of availability, integrity, confidentiality, rather than the traditional IT CIA (Confidentiality Integrity Accessibility) model, as it is deemed more of a priority to have system functionality over confidentiality of information.

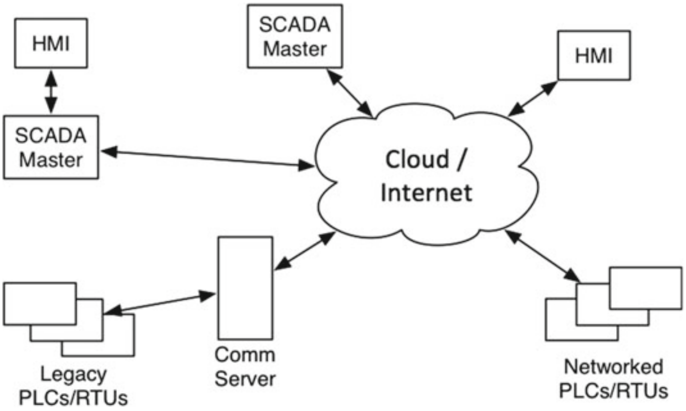


Fig. 5 SCADA system operating over IIoT

1.1.4 Industry 4.0 SCADA System

The latest breakthrough in SCADA system development arrives in the form of the Industrial Internet of Things, which in turn, accounts for a significant part of Industry 4.0. It utilises cloud computing and its commercial availability to improve productivity and reduce infrastructure costs by adopting IoT (Internet of Things) technology (Fig. 5).

2 Conceptual Architecture of a SCADA System

Modern SCADA systems comprise of a series of vital components, both hardware and software, that allow operations to be carried out successfully. These components

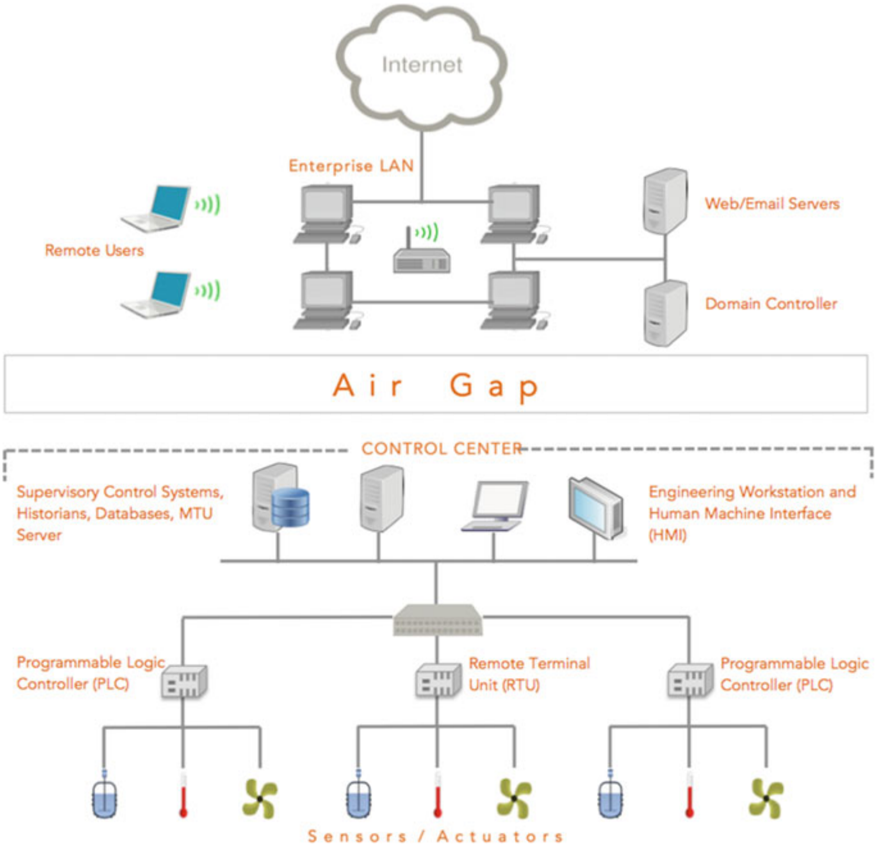

Internet
Enterprise LAN
Remote Users
Web/Email Servers
Domain Controller
Air Gap
CONTROL CENTER
Supervisory Control Systems, Historians, Databases, MTU Server
Engineering Workstation and Human Machine Interface (HMI)
Programmable Logic Controller (PLC)
Remote Terminal Unit (RTU)
Programmable Logic Controller (PLC)
Sensors / Actuators

Fig. 6 Conceptual architecture of a typical SCADA system

can be divided into two main sections within a SCADA system; the control centre; and the field sites. The most common components of the control centre include a Human Machine Interface (HMI), Historian, and Master Terminal Unit (MTU). The field sites will normally of comprise of a series of Programmable Logic Controllers (PLCs) and Remote Terminal Units or Remote Telemetry Units (RTUs) (Fig. 6).

2.1 SCADA Hardware

PLC (Programmable Logic Controller): PLCs are computerised devices connected to sensors and are used to control automated processes. They consist of a CPU (Central Processing Unit), memory, power supply, and an input/output interface. They are programmed using a specific control programming language, the most common of which being ladder logic. During operation a PLC will perform an iterating cycle of operations known as a “Program Scan”. Firstly, input is received via a sequential scan of the PLC’s input interface, which is then stored in memory representing the status of a physical process. This is followed by an execution of the control program that uses the input to decide whether the status needs to change. Finally, the outcome of that decision is stored in an output table and is used to make a change to the operation of the physical process. One complete cycle of the controller is known as a “Scan” and the time for a cycle to complete is known as the “Scan Time”. The Program Scan needs to iterate continuously so that it can react to any change in input. The shorter the scan time the faster it can react to these changes.

RTU (Remote Terminal Unit): An RTU is very similar to a PLC and performs virtually the same function in that it gathers data and transmits it back to the control centre. More recently both RTUs and PLCs have become more and more alike sharing common design features. Prior to this, the major difference between the two had been how they communicate with the control centre as well as their size and capabilities. Generally, RTUs have faster CPUs and a much larger support for communication. They also tend to be a bit more rugged and reliable in tough environments. They boast the ability for quick expansion through modularity and also provide flexibility within CPU and I/O (Input/Output) (Boyer 2004).

IED (Intelligent Electronic Device): IEDs allow for monitoring and control functionality as well as electrical protection and perform upper level communication completely independently without having to rely on any other devices.

Control Centre: A unique part of SCADA functionality is the ability to collect information about the state of its field devices and physical processes. PLCs and RTUs will continually transfer data regarding their status to a central control centre. This control centre can play a very important role in a forensic investigation when piecing together events that may have occurred. Its main components consist of an HMI (Human Machine Interface), Historian, MTU (Master Terminal Unit).

HMI (Human-Machine Interface): In order to interpret and visualise data that is transferred to the control centre SCADA systems use an HMI. The HMI not only provides a way to visually present the data that is processed but also allows for human interaction with the system as a way of controlling its overall state. Depending on what the SCADA system is controlling will ultimately depict the size and design of the HMI interface. This can range from a large-sized, computerised control panels at a nuclear plant to a small computer or even an application on a mobile phone.

Historian: In order to carry out any forensic investigation data needs to be analysed, but first that data needs to be collected and stored ready to be made available to users for analysis and interpretation. The Historian is the Database Management System that stores and archives this data and provides audit logs for all activity across a SCADA network. The functionality of the Historian was originally to provide data trending.

MTU (Master Terminal Unit): The Master Terminal Unit, sometimes referred to as the SCADA server, is responsible for receiving and processing all the data transmitted to the control centre from the field devices as well as providing communicating with those devices. It may pre-process data before sending it to the Historian and also provides a graphical representation of the information stored in it to be transferred ands displayed on the HMI (Stouffer et al. 2008).

2.2 SCADA Software

Software found within a SCADA systems field devices will differ in its objectives depending on the devices it is programmed into but software relating to a SCADA systems HMI or servers will generally provide a level of real-time diagnosis, management control, management information, information relating to specific sensors or systems, logging and reporting (Robles and Choi 2009).

2.3 Networking

SCADA systems communicating throughout the cloud, just like any other network, rely on a network topology across its various layers of communication between its components. Over the years, the originally intended “closed” SCADA control network has not only joined with corporate networks but has also seen a huge integration with the cloud offering a broader level of control and allowing access and monitoring from outside. From a security perspective this severely increases the risk of intrusion and attacks and provides a large level of complexity for a forensic response, as will be discussed. Firstly we will identify the various networking components essential to a SCADA network.

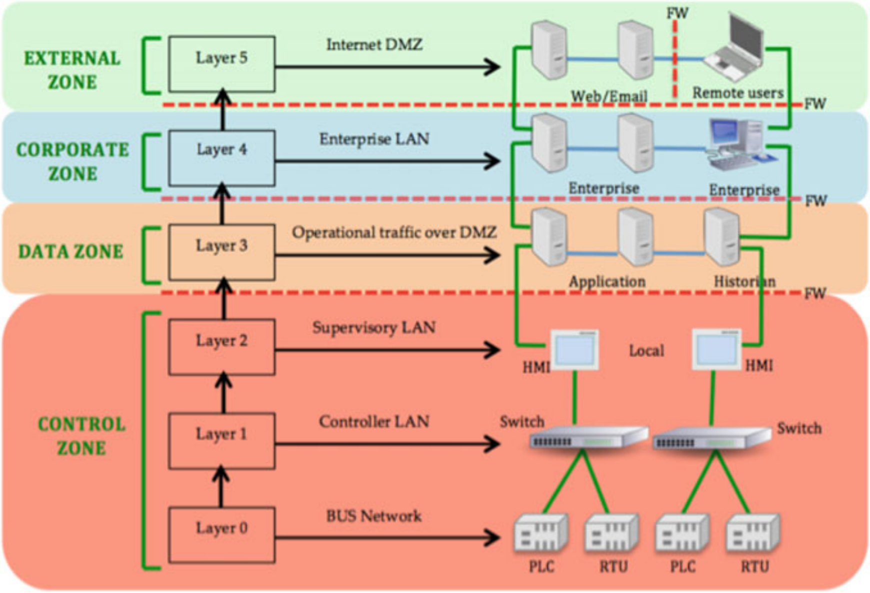


Fig. 7 Communicational zones of a SCADA system

2.3.1 Communication Zones

Modern SCADA systems operating in the IIoT space have evolved considerably since their original flat network architecture and as a result the network structure can be separated into zones. To increase security within the network, SCADA systems perform their most critical communications within the lowest most secure layer (Stouffer et al. 2011). Because connectivity within a SCADA network has multiple layers the forensic acquisition of the necessary data can often be difficult to trace (Wu et al. 2013).

According to Ahmed et al. and further developed by Pedro Taveras there is consistency when describing SCADA system forensic analysis as a 6 layer model. Figure 7 shows that model as well as the zones each layer belongs to.

Control Zone

Layer 0: At layer 0, a bus network connects up the various field device hardware, such as RTUs and PLCs.

Layer 1: Layer 1 contains the controllers that receive signals from the field devices via electrical input. Using standard networking protocols these are then decoded and signals can also be sent as outputs back to these devices as a means of control but also to layer 2 for analysis and further control.

Layer 2: As previously mentioned, layer 2 connects to layer 1 and receives information regarding the lower layers and uses this to present this data to a HMI for interpretation and control.

Data Zone

Layer 3: Layer 3 is made up of historians and application servers as well as domain controllers.

Corporate Zone

Layer 4: Layer 3 consists of all business and enterprise servers for email, DNS (Domain Name System) etc. and business workstations allowing for corporate communication (Stouffer et al. 2011).

External Zone

Layer 5: Layer 5 resides in the external zone of the SCADA network and includes connectivity to remote operations, third party vendors and business partners which ultimately defines IIoT (Knijff 2014).

2.3.2 Communication Protocols

The modern SCADA system is designed to offer real-time updates on the status of its physical processes within its network. These can sometimes cover large geographical areas and contain thousands of sensors and field devices. In order for these updates to occur, and for the successful control of the physical processes, data needs to transmit using secure communication between the field devices and the SCADA host. This is achieved through using a range of specific communication protocols that transport the information from field devices to a central control centre, whether in the cloud or locally (Fig. 6).

Vendors began developing their own communication protocols before standards organisations started developing open standards. Some manufactures even carried on creating proprietary protocols after open standards were made available (Boyer 2004). The convergence with IIoT has seen the number of varying protocols increase, but despite this large number of both proprietary and non-proprietary protocols there are some that are more common than others, such as Modbus, DNP3 (Distributed Network Protocol-3), PROFIBUS (Process Field Bus), WiMax (Worldwide Interoperability for Microwave Access), Wi-Fi, HTTP (Hypertext Transfer Protocol), CoAP (Constrained Application Protocol), AMQP (Advanced Message Queuing Protocol) (Fig. 7).

3 Examples of SCADA System Incidents Prior to IIoT

When security breaches occur within SCADA systems destruction can be life threatening. The following are examples of past system failures within SCADA environments.

3.1 Trans-Siberian Pipeline Explosion

3.2.1 Trans-Siberian Pipeline Explosion The earliest recorded incident involving cyber attacks on a SCADA system was in 1982 on the Trans-Siberian pipeline when a Trojan found its way into its SCADA system software resulting in a 3-kiloton explosion that could be seen from space. The Trojan was responsible for increasing the pressure during a pressure test on the pipeline (Miller and Rowe 2012).

3.2 Maroochy Shire Water System

The SCADA system of the Maroochy Water Sewerage Service consisted of two main computers monitoring 142 sewage pumping stations over 880 kilometres. Each of the stations consisted of SCADA field devices that would raise alarms, process instruction and communicate real-time data describing the pumps status to the control centre. In early 2000 a disgruntled ex-employee named Vitek Boden, who had previously been employed as a site supervisor, hacked into the systems over a period of several months. His actions prevented alarms from being reported to the central control centre as well as stopping communication between the control centre and the certain pumping stations, resulting in a million litres of sewage water flooding into a nearby river. He achieved this by altering the identification numbers of some of the pumping stations so that signals meant for one station would be sent to another. He used wireless equipment to gain access to the SCADA system and redirected insecure radio communications. The problem could have been avoided if the company had placed sufficient access control within its SCADA system especially regarding wireless access restrictions (Abrams and Weiss 2008) (Fig. 8).

3.3 Stuxnet

Still unsure of its architect, by September 2010, the propagation of the Stuxnet worm had infected around 45,000 computers despite appearing to be directed specifically at Iranian Industrial Control Systems running secure facilities a such as nuclear power plants or gas pipelines. By exploiting weaknesses within the Windows Operating System running Siemens Simatic STEP 7 software Stuxnet's aim was to reprogram Programmable Logic Controllers to function outside of their intended boundaries. This resulted in the plants centrifuges, responsible for separating nuclear material, spinning dangerously faster than originally intended causing damage and destruction. Despite being an isolated network the use of a removable storage device such as a USB (Universal Serial Bus) drive allowed the worm to penetrate and spread into the SCADA system of an Iranian Nuclear Power Plant. As soon as it had crossed the "air-gap" it could traverse through the network via LAN and into PLCs where it

Table 1 Stuxnet vulnerability exploits

Vulnerability	Description
MS08-67: RPC (Remote procedure call) vulnerability in server service	Allows for a remote user to gain equal rights to a local user and take control of an affected system remotely
MS10-046: LNK vulnerability in windows shell	An attacker may exploit vulnerabilities in the handling of windows shortcut files (.LNK) to insert malware remotely
MS10-061: Spool server vulnerability in print spooler service	Allows for an attacker to make a specially designed print request resulting in them taking over the server
MS10-073: Win32k.sys vulnerability in windows Kernel-Mode drivers	Allows an attacker to execute kernel privileges
CVE-2010-2772	Vulnerability in Siemens Simatic WinCC and PCS 7 SCADA system allows for attacker to use known default passwords to gain access

would infect WincCC and STEP 7 files. Documented in Critical Infrastructure Protection by NATO (North Atlantic Treaty Organisation) Advanced Research are the 5 vulnerabilities that Stuxnet exploited (Ibrahim and Faisal 2012) (Table 1).

The lack of any integrity check on messages and their sources allowed for Stuxnet to interfere with commands from the process control network without PLCs or any operators knowing.

3.4 Duqu

A year later, after Stuxnet, a new malware was discovered, resembling many of its design and structure features. It was given the name Duqu because the temporary files created by the malware's key logger all began with "DQ.." (Bencsath). Stuxnet had paved the way for targeted attacks on control systems and Duqu was just another example of the threat to CNI. Duqu was more aimed at stealing information using its key logger to obtain keystrokes, files and screen shots, a kind of industrial espionage or cyber-surveillance attack (Bencsáth et al. 2011).

3.5 Flame

Flame, also known as Flamer and sKyWlper, followed in the footsteps of Duqu as an "information stealer" and is an example of a more complex malware aimed at SCADA and industrial control systems. Like Duqu, it could steal screenshots and keystrokes but it also had the ability to activate web cams and microphones. By disguising itself as a proxy for Windows updates it infected over a thousand systems across the Middle East and Iran (Bencsáth et al. 2011).

4 SCADA Forensics Within IIoT

New age SCADA systems that use cloud-based technology for analysis and control through IIoT ultimately rely on their physical components and sensors in the OT (Operational Technology) layer of the infrastructure to operate correctly and safely. During a forensic investigation of such a system it is these lower level devices that will hold key information that is critical to determining the cause of the incident. Having discussed some of the more commonly known, high-impact breaches of SCADA system security it is important to realise that a thorough investigation is mandatory each time an incident occurs, regardless of whether the incident was a result of malicious intent or not. A forensic investigation of a security breach or system failure aims to identify those responsible as well as the cause of the incident. When incidents occur the need for a forensic response is essential for understanding how the events happened and piecing together who was responsible. Identifying the cause of the attack will then provide a basis for patching the system to improve its security and therefore help prevent the same attack happening twice (Wu et al. 2013).

A forensic response to SCADA system failure is essential for several reasons:

- It identifies the root of an incident, and potentially those involved
- It identifies if the system is still at risk and what changes were made to the system
- It identifies the damage caused and the total probable damage
- It highlights weaknesses in SCADA systems that can be improved to reduce the risk of the incident reoccurring (Ahmed et al. 2012).

4.1 Forensic Challenges

In order to understand the key issues regarding digital forensics within SCADA systems operating within IIoT we must first understand that there is a clear distinction between IT systems and SCADA systems. It is the complexity of a SCADA environment that separates it from a traditional IT system and therefore precludes the application of standard forensic methods and tools. Current research shows a consistency in the issues and challenges faced by the forensic investigator when dealing with SCADA systems and these can be broken down into several key areas. Below is a taxonomy of the current forensic challenges existing in ICS and SCADA incident response.

4.1.1 Live Forensics

As SCADA is at the heart of all critical infrastructures it is essential that it operates continuously and is never turned off for any reason. As a result the usual standard forensic techniques, normally applied in IT, cannot be applied for data acquisition in these instances. Instead, the practice of live forensics is required. This allows for the process of data acquisition and analysis to be carried out whilst the SCADA system is running (Ahmed 2012). It is essential that during this process both volatile and non-volatile data be acquired. Non-volatile data may be stored in hard disks attached to various SCADA hardware, such as MTUs and Historians. Volatile data contains vital information describing the current state of running system and is found in the physical memory of SCADA devices. It differs from non-volatile data in that its content is constantly being overwritten and updated with newer information. This creates even further problems during an investigation.

4.1.2 Rapid Response

Data of any evidential value contained within physical memory will be at its peak just after an incident happens. From that moment on, due to the nature of volatile data, the amount of useful information will decrease as older processes and services are overwritten by newer ones (Taveras 2013). For this reason it is vital that a forensic response is carried out as quickly after an incident has occurred as possible before important information is lost. This can create another challenge when a SCADA system is spread over many thousands of square kilometres. Many of the embedded devices found in SCADA systems, such as PLCs, have a relatively small amount of memory and flash storage. As systems continue to run, data is overwritten and therefore the length of data retention is very small (Wu et al. 2013).

4.1.3 Integrity and Validity

A key part to any digital forensic investigation is to be able to obtain evidence in a forensically sound manner in order to prove its integrity and validity in a court of law. Digital evidence is normally verified by matching the hash value (calculated by applying a hashing algorithm to the data) of the original evidence against its acquired copy. This digital “fingerprint” proves that the data under examination and analysis has not been modified in any way, as any modification would cause the hash value to change and therefore not match the original. According to Ahmed the challenge within SCADA systems is that because the system remains live, and data is continuously being updated, the state of the data can change from the start of the copying process to completing a calculated hash, resulting in the hash being unusable.

4.1.4 Incident Specific Information/Logs

As some SCADA systems have avoided being updated over the years, due to the heavy risk of interference it may cause to a live system, older technologies are still present in many environments. This may be in the form of legacy or no longer supported hardware and therefore, as a result, can lead to a distinct lack of detailed logging (Fabro and Cornelius 2008). Effective logging can assist significantly in a forensic investigation and help piece together a timeline of events. According to Fabro et al., it is not uncommon for systems with logging and audit functionality to be deployed with these functions disabled. It is vital that when logging features are absent or insufficient in a system, that network traffic be logged to help understand device communication at the time of an incident.

4.1.5 SCADA Forensic Tools

Research shows a clear absence of data acquisition tools and methodologies designed specifically to incorporate SCADA systems, including their protocols and proprietary log formats (Ahmed et al. 2012). This may be, partly, due to the transparency of the effect such tools can have on live SCADA services as well as many other issues that may have prevented the production of such tools already.

4.1.6 Order of Volatility

For a tool to acquire real-time data from a live system it is inevitable that, during that process, the memory state of that system or device will change. In order to maximise the amount of data of evidential value being extracted during the data acquisition process, the tool would have to follow an order of volatility, beginning with the most volatile (Registers, Cache) and moving towards the least volatile (Archival media) (Fabro and Cornelius 2008). This lightweight approach will minimise the amount of changes memory and reduce the amount of disruption to the network (Wu et al. 2013).

4.1.7 Remote Data Acquisition

Research carried out by EADS (European Aeronautic Defence and Space) (Wu et al. 2013) emphasises the need for such a tool to be able to extract and acquire data remotely from a suspect system to an investigators machine directly via the network. They discuss the current forensic tools able to carry out this method of acquisition such as, ProDiscover and EnCase Enterprise which, when installed on a suspect system, can be used to extract forensic artefacts from an MTU or HMI etc.

4.1.8 Compatibility

In order to operate effectively the tool must be compatible with all SCADA system devices, even with those running their own exclusive operating systems or Linux variants. Many SCADA components run customised kernels in their operating systems in order to improve performance or to provide support for applications. The tool would have to be able to communicate with those operating systems in order to be able to operate successfully and exchange the relevant information (Ahmed et al. 2012).

4.2 Current Data Acquisition Methods for SCADA Systems

Although there are no specifically designed data acquisition forensic tools aimed solely at SCADA systems, there are various tools and methods that are currently being used to extract data from SCADA system components.

5 Forensic Acquisition of SCADA Artefacts

Firstly, a SCADA forensic artefact can be thought of as any data that provides explanation to the current state of a SCADA system, device or media. Data of forensic value within SCADA systems can exist in two separate streams; data that is communicated across a network; and data that is stored in a device (Knijff 2014). The latter can be further categorised as to which zone, within the SCADA architecture, that device exists. This section will aim to highlight the key tools and methods for forensically acquiring data from both the network and from the physical assets.

5.1 Network Data Acquisition

Data passing over a SCADA network can be captured in various ways and using a variety of tools. The following is a list of current tools available to perform network data acquisition within a SCADA environment.

5.1.1 In-Line Network Taps

Sniffing traffic over a network can be achieved through the use of network taps and placing them at keys points within a network, known as ‘choke-points’. Ideally, they would be placed between switches, on ethernet lines or in-between individual assets. A network tap is a device that copies network traffic passing through it to a monitor port (Hjelmvik 2011). Implementing the use of link aggregation taps allow for both downlink and uplink traffic to be captured. Network taps can only be connected onto a SCADA network when it is safe to do so, during downtime of operations or during maintenance periods. This will eliminate any disruption to critical processes. The tap can then be connected to a separate machine dedicated for the collection of that data.

5.1.2 Port Mirroring

When network taps cannot be implemented an alternative can be to use port mirroring or SPAN (Switch Port Analyzer) to obtain SCADA network data from managed switches. By connecting a monitoring system to a managed switch, a copy of the packets sent through that switch, or separate ports on that switch, can be mirrored to a single port. That port can then be used to acquire the data. To acquire the data a monitor session must be started (CA 2015). This includes;

- the session number: to identify the monitoring session
- session source: the desired ports to mirror
- session direction: specifies the direction of the mirrored traffic, i.e. receive (RX) or transmit (TX) or both.

5.1.3 TCPdump

Much like Wireshark, but less labour intensive, TCPdump can be used as both a network monitoring tool as well as a tool to acquire network data from within a SCADA network. Data obtained via TCPdump will include timestamps, network protocol used, source IP and port, and destination IP and port (Green and Vanden-Brink 2012).

5.1.4 Wireshark

Wireshark is an open source protocol analyser and can be used to capture packets being sent across a network. Acquired data will be stored as .pcap files for later analysis or can be monitored live in real-time as data is communicated. Wireshark also supports many ICS and SCADA protocols.

5.1.5 Serial RS232 and RS485 Taps

Many devices found within SCADA networks rely on serial communication and although Wireshark also supports serial communication data there are several other tools that can be used. Much like implementing the ethernet tap an RS232 or RS485 network tap could be introduced to the network during scheduled downtime or maintenance periods to obtain serial communication data.

5.1.6 PortMon

Portmon is a utility found within Windows based systems and allows for monitoring and capturing of serial data. Simply executing the portmon.exe program file will start to capture serial communication data.

5.2 Device Data Acquisition

5.2.1 PLC:

Acquiring data from PLCs is dependent upon certain factors, such as whether the PLC needs to remain active or whether it can be powered down. The first instance poses many problems. If a PLC has to remain live for critical processing any interference to those processes may result in disastrous consequences. When this is the case sometimes the software used to program the PLC can be used to monitor and record certain vital data such as memory variable values as they alter (Wu et al. 2013). Examples of this would include using Siemens STEP7 software to record the data from any Siemens S7 PLCs, or Schneider Electric's SoMachine software to record memory address alterations in their Modicon PLC range.

Over the years there has been a distinct lack of dedicated forensic tools for PLCs and similar embedded devices (Ahmed et al. 2012) but some software tools are starting to emerge to overcome the problem. As well as using the PLCs manufacturing tools to retrieve data there are tools such as PLC Analyzer Pro and PLCLogger that perform similar functionality. PLC Analyzer Pro is a software tool designed for acquisition and analysis of recorded data on Siemens SIMATIC devices.

PLCLogger is an open source software tool and provides similar functionality to PLC Analyzer Pro with the addition of supporting any device using Modbus-TCP or Modbus-UDP.

There has been some research into the development of a solution for the security monitoring of low level SCADA devices which could potentially aid a forensic investigation within a SCADA environment. Cruz et al. (2015) suggests the use of the SSU (Shadow Security Unit) which is placed in parallel to field devices for continuous monitoring of a device. The device can check for abnormal behaviour of a PLC and through physical probing go the I/O modules can provide real-time data acquisition capabilities (Cruz et al. 2015). A similar concept is discussed by Janicke et al., implementing a run-time monitoring framework using an Ardruino Yun device, alongside a field device to ultimately capture snapshots of PLC states, i.e. values for inputs/outputs, counters and timers etc., to aid in the forensic analysis after an incident has occurred (Janicke et al. 2015).

If a PLC can be powered down for forensic analysis or is already powered off as a result of an attack then certain techniques can be used to read data from the on-board memory chips themselves through JTAG (Joint Test Action Group), chip off or ISP (In-System Programming).

JTAGging and In-System Programming are both non-invasive methods for achieving the same results. JTAGging is the process of interacting with the Test Access Points (TAPs) of the microcontroller in such a way to acquire raw data from any connected memory chips.

In-System Programming is a way to acquire data by bypassing the CPU itself and connecting directly to on-board storage chips, such as eMMC or flash storage and then pulling the raw data from them. Hardsploit is a hardware and software device designed with critical electronic and embedded devices in mind. It allows for both ISP and JTAGging to be carried out and a dump of the raw data to be obtained. The raw data can then be interpreted using a hex editor such as WinHex or HxD.

Chip off is regarded as an invasive acquisition procedure as the memory chips are physically desoldered and removed form the PLCs PCB and then read using specific chip readers to acquire the image. Chip off may be the only option if chips are already physically damaged and need to be repaired before imaging. Tools and equipment for this process would include a desoldering station to remove the chip and Hardsploit to acquire the data from it.

Once a raw image has been acquired it can then be interpreted to establish program code and ladder logic such as function.

5.2.2 HMI:

Much like a PLC the HMI typically has a fairly limited amount of on-board storage. However, the data stored on the chips could be crucial in a forensic investigation. The HMI is the interface at which a human interacts with the control devices. Decisions are made based on information passed back from field devices to the HMI. The HMI can store critical information such as event logging, alarm logging, issued commands, diagnostics and reports on the most recent status of particular field devices (Fabro and Cornelius 2008).

Performing data acquisition from HMI devices will mirror very closely the approach used with PLC devices. Vendor-specific software tools used to program the HMIs will often have monitoring and recording features which should be enabled when possible. Physical interrogation of the devices will involve ISP, JTAG and Chip-off to recover an image of the raw data, as explained in Sect. 3.2.1.

5.2.3 Engineering Workstations/General Workstations/Servers:

Workstations and Servers found at the control, data and corporate zones can all be approached in the same manner when it comes to a forensic response. Each system is going to contain different types of forensic artefact depending on the role its plays within the SCADA environment. The underlying fundamental elements are that they will all contain data stored in both memory and on physical storage that may be vital to investigation. Therefore, different tools are generally needed for RAM (Random Access Memory) acquisition and for physical media extraction.

Disk Imaging: There is an array of disk imaging software tools that can be used to extract a forensically sound full image of internal and externally attached disks from a machine. Different tools have varying levels of capabilities and the preferred tool of choice may be dependent upon which operating system is running on the source machine.

AccessData's FTK (Forensic ToolKit) Imager is a common software tool used to create digital images of physical drives as well as the ability to obtain a full memory dump. FTK Imager Lite is a variation of the tool on USB format which eliminates the need to install any software on the source machine.

EnCase Forensic Imager can be used as an alternative to FTK Imager and ultimately performs the same functionality offering similar imaging formats and capabilities. However, a case study carried out by Muir (2015), of a comparison between EnCase version 7.10.00.103 and FTK Imager 3.3.0.5, showed that EnCase created more of a footprint than FTK when being run live on a target machine. This would be a factor to consider when acquiring a memory dump of a system as vital processes may be overwritten.

DD is a Linux command-line tool built in as standard on Linux and Unix systems and one that can also be installed on Windows machines. The dd command can be used to copy entire mounted drives both locally and remotely.

RAM Acquisition: There are also various tools that can be used to acquire memory from a device that is running such as running processes, services, drivers, registry data, network data and event logs. Tools need to be carefully selected when dealing with memory acquisition as the tools being loaded to acquire the memory will also run in memory. This could potentially overwrite vital artefacts. Running command line tools are much more advantageous then GUI tools as they use less memory space.

Dumpit, a tool created by MoonSols for Windows systems, is an open source memory acquisition tool than can be run from a USB.

Memoryze, created by Mandiant, is very similar to dumpit and is run from a USB using the command-line. It is also a free tool and allows a complete memory dump to be passed to an externally connected drive or over a network.

Mandiant Redline is capable of extracting and auditing a full memory image of a workstation in a forensically sound manner. It was designed to detect malicious activity within memory. Its IOC (indicators of Compromise) functionality allows for the identification of malicious files and processes.

LiME can be used to acquire a memory dump from a linux system. Again, this can occur locally buy installing LiME on the host machine or can be acquired over the network via TCP.

Volatility is a cross-platform tool that can also be used to extract digital artefacts from live volatile memory and also provides analysis functionality (Stirland et al. 2014).

5.3 Half-Life of Data Within a SCADA System

When an incident occurs and an investigation is undertaken a forensic investigator needs to know where data is and how long it will last there. Given the complex nature, sheer scale of possible data sources, and various interconnected networks within a typical SCADA system, calculating the half-life of data for an entire system would be impossible as it would change dramatically from one system to another and be dependant on the type of incident that has occurred and the devices running. For example, data would last a lot longer in a historian than it would in an engineers workstation, which in turn would last significantly longer than data stored in a PLC.

This implies that the half-life of data should be identified at a lower level, for each data source but even this would be individual device specific. For example, 2 identical Siemens S7 1212c PLCs that hold 25kb of volatile memory, 1kb of load memory and 2kb of retentive memory will not share the same half-life as, despite the program scan time to scan each of the inputs and outputs will be exactly the same, the list of instructions to execute in the one PLC may be significantly higher than the other meaning that data in memory is written over at a faster rate and therefore resulting in a lot lower half-life.

These characteristics should be carefully considered when prioritising devices during an incident response.

6 SCADA Forensic Process

6.1 Existing Incident Response Models

There are many models for a forensic response to normal IT systems that follow a generic model of identification and preservation, collection, examination, analysis and reporting in a forensically sound manner, but there is very limited documentation regarding ICS/SCADA forensic incident models at the low level. There are various recommended guidelines such as Homeland Security's "Developing an Industrial Control Systems Cybersecurity Incident Response Capability" (Security 2009) (and many similar) which give good guidance on incident planning, prevention and management but lack any detail of how to actually perform forensics on a SCADA system at a low level. There are, however, some effective post-incident SCADA forensic models that have been suggested such as those put forth by Kyle Wilhoit, a threat researcher from Trend Micro, (Wilhoit 2013) and Tina Wu of EADS (Wu et al. 2013) that incorporate the full SCADA System into the forensic investigation. These added elements into the forensic response model are essential for SCADA systems over normal IT systems.

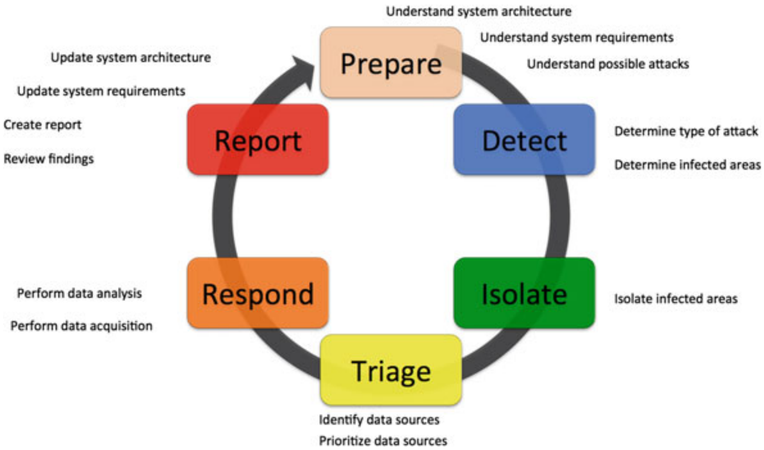


Fig. 8 SCADA forensic incident response model

6.2 *Forensic Methodology for SCADA Within IIoT*

A SCADA forensic response should not just take place after an incident has occurred but also before and during an incident. The more detailed information the investigator has access to regarding a SCADA system under investigation the more it will increase the level of forensic evidence recovered. Below is a proposed Forensic Incident Response Model.

SCADA forensic process models have been suggested in the past, such as that proposed by Wu et al. (2013), which adapts the traditional IT system forensics investigation process and applies it to SCADA systems. However, the incident response model proposed in this paper is an alternative, original model, first submitted to ICS-CSR (Industrial Control System-Cyber Security Research) 2015 (Eden et al. 2015), and now further developed, that treats SCADA forensics as more of an ongoing lifecycle, using the entire process to influence the next event.

Figure 8 shows the SCADA forensic incident response model consisting of six main stages; Prepare; Detect; Isolate; Triage; Respond; and Report. The final stage helps to improve the preparation for the next time an investigation is needed, therefore continuing the cycle.

6.2.1 Stage 1: PREPARE

It is vital that the preparation stage starts before an event takes place. This will involve ensuring all documentation relating to the particular SCADA system is accurate and should comprise of understanding the following areas:

- Understand system architecture: As each SCADA system will be unique in its configuration it is essential that detailed documentation regarding the system's network, hardware and software is collected and recorded. The networking information should involve network configurations, a network map and all entry points into the system. Hardware documentation should include all SCADA components, including manufacturers, makes and models. The software documentation should include all software running on each device across all zones. Accurate geographical documentation regarding locations of field devices and device half-life etc. should also be available.
- Understand System Requirements: Given the classification of certain SCADA devices it is also essential for the forensic investigator to have access to specific system requirements for the SCADA system being investigated. Documented here should be the types of systems and devices that need to remain continually running without fail, those that can be switched to a back-up, and finally those devices that can be powered down.
- Understand Potential Attacks: It is also important to gather threat intelligence and to understand the types of attacks that can occur on the system. It has already been discussed by Zhu et al. (2011) and further acknowledged by Stirland et al. (2014), that the types of possible SCADA related attacks can be divided into 3 sections. These are hardware, software and the communication stack. Detailed information relating to these types of attacks can be found at Zhu et al. (2011).

6.2.2 Stage 2: DETECT

- Determine type of attack: When an event has taken place, or is in the process of taking place, an investigator should try to determine the type of attack based on assessments of real-time data and any unusual behaviour that may have occurred.
- Determine potential infected areas: Attempt to determine potential infected areas based on assessments made from the previous step. This will help in the next stage when identifying possible data sources.

6.2.3 Stage 3: ISOLATE

- Isolate infected areas: After detecting potential infected areas an attempt can be made to isolate those networks and devices, dependant upon their system requirements within the SCADA environment and business operations.

6.2.4 Stage 4: TRIAGE

- Identify data sources: The triage stage should start by identifying possible data sources of interest for interrogation. This will be influenced by the documentation from the planning stage together with the threat intelligence of stage two and within the isolated area. The list should include the device location within the network; device make, model and serial number; and classification status i.e. process critical.

- Prioritise data sources: The next step is to create a prioritisation list of data sources. This needs to be ordered in a way that reflects their value, volatility and accessibility in order to maximise the potential evidence available for recovery (Knijff 2014). The time taken to assemble a priority list could also have an effect on the amount of evidence recovered as certain SCADA systems in critical infrastructure can span huge geographical areas and contain hundreds of data sources.

6.2.5 Stage 5: RESPOND

- Perform data acquisition: With a priority list established the next stage involves forensically acquiring the data from the relevant data sources, which can either come from data stored in components or from data across the network (Knijff 2014).

  Data needs to be admissible in court and therefore, should be acquired using forensically sound methods. The types of data acquired at this stage should include memory dumps, disk imaging and chip imaging from across the system. Traditional IT forensic tools can be used against engineering workstations, servers and historians but for embedded devices such as PLCs and RTUs, flashing software may be required from the manufacturer to extract a raw memory dump using JTAG (Joint Test Action Group) ports and ensuring that no affect is made to the operation of the device if required to remain operational (Stirland et al. 2014). Invasive methods such as chip-off forensics may be used to extract data as a last resort but would be dependant on a component's classification. Clear guidelines would have to be established for each type of asset. The data acquisition stage should also include acquiring network data through retrieving logs data captures.
- Perform data analysis: Data analysis will involve separating the forensic artefacts from other SCADA system data. This may be carried out with the use of traditional forensic analysis tools.

6.2.6 Stage 6: REPORT

- Review findings: Based on the analysis stage relationships can be correlated between the recovered forensic artefacts to ultimately create a timeline of events and to establish the root of an incident.
- Create report: Based on the analysis of recovered artefacts a report should be compiled regarding results and findings. Inferences should be made between relationships of the gathered data, which should also include validation and integrity of data records such as chain of custody reports. It should also include any recommendations towards the development or patching of the SCADA system.

- Update system architecture: The final steps of the reporting stage should be to update the documentation relating to the SCADA system architecture, post incident. This is due to the fact that after an event has taken place the overall configuration of the SCADA environment may have changed and will need to be accurate for the next investigation.
- Update system requirements: Similar to the previous step, in the light of an incident occurring and system configurations changing, SCADA system requirements may also need to be revisited and, therefore, would need to be recorded.

6.3 SCADA Forensic Workstation

To develop and propose a SCADA forensic workstation we first must consider the software and hardware tools needed to perform data acquisition on all types of data sources as well as the analysis of recovered data. Stirland et al. suggest a similar strategy for developing a SCADA forensic toolkit in which I will adapt and add to in order to cater for physical extraction of embedded devices (Stirland et al. 2014).

6.3.1 Hardware

High Spec Machine—To efficiently process large amounts of data. Must include multiple connection ports.

Write-Blocker—To image data sources in a forensically sound manner. Can be used on all SCADA servers, Back-end databases, Engineering workstations, Historians, HMI hosts.

Memroy Imaging Tool—To acquire volatile memory on running data sources. Can be used on all SCADA servers, Back-end databases, Engineering workstations, Historians, HMI hosts that need to remain running.

JTAG Kit (incl. Screwdriver set, Multi-meter, solder iron and solder, Jtagulator, Bus Blaster/Bus pirate—Screwdriver set to disassemble device. Multi-meter to test JTAG ports. Solder and solder iron to connect wires to JTAG ports. Jtagulator to determine JTAG TAPs. Bus Blaster to extract data. Can be used on any SCADA embedded devices i.e. PLCs, RTUs, HMIs.

Storage Drives (HDDs (Hard Disk Drive)/SSDs(Solid State Drive))—To store forensic images of data sources and all acquired SCADA data. Can be used on all captured data.

Camera—To document live data acquisition processes. Can be used on all data sources where live interrogation is performed to capture steps taken by investigator.

6.3.2 Software

FTK Imager—For creating forensically sound images of data on devices. Used for all database servers, HMI hosts, engineering workstations.

AccessData FTK Toolkit/Encase—To process and analyse acquired forensic images. Can be used on all filesystem data from HMI, Engineering workstations, Servers, Historians.

Putty—For use on the forensic workstation to communicate with JTAG devices and PLCs/RTUs.

Vendor-Specific Flasher Software—To be used to acquire raw data during the JTAG process (if available) from PLCs and RTUs.

WinHex—To view acquired raw data dumps from data sources such as PLCs, RTUs, and RAM dumps.

Data Hash Generator—To generate a hash value for captured data to prove integrity. Can be used on all acquired data.

TCPDump—To capture post-incident data remnants of a network. Can be used on all network data.

Wireshark/Network Miner—To filter and acquire SCADA network protocols and traffic. Can be used on all SCADA networks.

Volatility—To perform in-depth analysis of captured live data. Can be used on all database servers, HMIs, Engineering workstations, Historians.

AlienVault ICS SIEM—SIEM and integrated forensics tool that can be used to parse acquired network data allowing the user to define specific rules for monitoring. Can be used on all network data (Stirland et al. (2014)).

7 Conclusion

IIoT provides a fundamental core for industrial control systems, including much of the world's critical national infrastructures, to operate continuously and safely without disruption or interference. As the majority of these systems that were initially SCADA systems designed to operate on closed networks are now operating through the cloud over TCP/IP the risk from outside targeted attack is already evident. Any interference to them could cause huge economical damage and even loss of life. When an incident occurs it is essential that a forensic response is undertaken, following defined procedures and methodologies and with the correct tools. Current research clearly highlights a distinct lack of dedicated SCADA certified forensic tools for incident response and an absence of a forensic triage model for carrying out investigations. As a result suggestions have been discussed to aid the forensic response to SCADA incidents. Ongoing research should be directed at developing such tools, methodologies and models to aid in IIoT forensic investigations post-incident.

8 List of Abbreviations

AMQP—Advanced Message Queuing Protocol
CIA—Confidentiality Integrity Accessibility
CNI—Critical National Infrastructure
CoAP—Constrained Application Protocol
CPU—Central Processing Unit
CRC—Cyclic Redundancy Check
DNP3— Distributed Network Protocol-3
DNS—Domain Name System
EADS—European Aeronautical Defence and Space
HDD—Hard Disk Drive
HMI—Human Machine Interface
HTTP—Hypertext Transfer Protocol
ICS—Industrial Control System
IIoT—Industrial Internet of Things
IOC—Indicator of Compromise
IoT—Internet of Things
IP—Internet Protocol
I/O—Input/Output
IT—Information Technology
JTAG—Joint Test Action Group
LAN—Local Area Network
MTU—Master Terminal Unit
NATO—North Atlantic Treaty Organisation
NIST—National Institute of Science and Technology
PLC—Programmable Logic Controller
PROFIBUS—Process Field Bus
RAM—Random Access Memory
RISI—Repository of Industrial Security Incidents
RPC—Remote Procedure Call
RTOS—Real Time Operating System
RTU—Remote Terminal Unit
SCADA—Supervisory Control and Data Acquisition
SPAN—Switch Port Analyzer
SSD—Solid State Drive
SSU—Shadow Security Unit
TAP—Test Access Point
TCP/IP—Transmission Control Protocol/Internet Protocol
USB—Universal Serial Bus
WAN—Wide Area Network
WiMAX—Worldwide Interoperability for Microwave Access

Acknowledgements This work is funded by the Airbus Group Endeavr Wales scheme under the SCADA Cyber Security Lifecycle (SCADA-CSL) programme with the ultimate goal of improving the forensic handling and incident response process for SCADA systems.

References

Abrams M, Weiss J (2008) Malicious control system cyber security attack case study-maroochy water services. Australia, Technical report, NIST

Ahmed I, Obermeier S, Naedele M (2012) Scada systems: challenges for forensic investigators. Computer 450(12):44–51

Bencsáth B, Pék G, Buttyán L, Félegyházi M (2011) Duqu: a stuxnet-like malware found in the wild. Technical report, laboratory of cryptography and system security (CrySyS)

Boyer S (2004) Scada. ISA-the instrumentation, systems, and automation society, Research triangle park, NC

CA (2015) Data acquisition: best practices guide. Technical report, CA technologies

Cruz T, Barrigas J, Proenca J, Graziano A, Panzieri S, Lev L, Simões P (2015) Improving network security monitoring for industrial control systems. In: 14th IFIP/IEEE international symposium on integrated management (IM 2015)

Eden P, Blyth A, Burnap P, Cherdantseva Y, Jones K, Soulsby H, Stoddart K (2015) A forensic taxonomy of scada systems and approach to incident response. In: 3rd international symposium for ICS and SCADA cyber security research 2015

Fabro M, Cornelius E (2008) Recommended practice: recommended practice: creating cyber forensics plans for control systems. Technical report, department of homeland security

Green T, VandenBrink R (2012) Analyzing network traffic with basic linux tools. Technical report, SANS Institute InfoSec Reading Room

Hjelmvik E (2011) Intercepting network traffic. NETRESEC (Network forensics and network security monitoring). http://www.netresec.com/?page=Blogandmonth=2011-03andpost=Sniffing-Tutorial-part-1---Intercepting-Network-Traffic

Ibrahim M, Faisal M (2012) Stuxnet, duqu and stuxnet, duqu and beyond. Int J Sci Int J Sci Eng Invest 1(2):75–78

Janicke H, Nicholson A, Webber S, Cau A (2015) Runtime-monitoring for industrial control systems. Electronics 40(4):995–1017

Karnouskos S, Colombo AW (2011) Architecting the next generation of service-based scada/dcs system of systems. In: IECON 2011—37th annual conference on ieee industrial electronics society, pp 359–364

McClanahan R (2003) Scada and ip: is network convergence really here? IEEE Industry Appl Mag 90(2):29–36

Miller B, Rowe D (2012) A survey of scada and critical infrastructure incidents. Proceedings of the 1st Annual conference on research in information technology. New York, NY, USA. ACM, pp 51–56

Muir B (2015) Encase imager versus ftk imager. http://bsmuir.kinja.com/encase-imager-vs-ftk-imager-1677906594. Accessed 21st June 2016

Robles R, Choi M (2009) Assessment of the vulnerabilities of scada, control systems and critical infrastructure systems. Int J Grid, Distrib Comput 2

Rutherford D (2012) Make the most of your energy ethernet for scada systems. Technical report, Schneider electric telemetry and remote SCADA solutions

Homeland Security (2009) Recomended practice: developing an industrial control systems cybersecurity incident response capability. Technical report, Homeland security

Stirland J, Jones K, Janicke H, Wu T (2014) Developing cyber forensics for scada industrial control systems. In: Proceedings of the international conference on information security and cyber forensics. SDIWC Digital Library

Stouffer K, Falco J, Kent K (2008) Guide to industrial control systems (ics) security. gaithersburg, md: U.s. department of commerce, national institute of standards and technology. Technical report, NIST (National institute of standards and technology)

Stouffer K, Falco J, Scarfone K (2011) Recommendations of the national institute of standards and technology. NIST

Taveras P (2013) Scada live forensics: real time data acquisition process to detect, prevent or evaluate critical situations. Eur Sci J

van der Knijff RM (2014) Control systems/scada forensics, what's the difference? Digit Invest 110(3):160–174

Wilhoit K (2013) The scada that didn't cry wolf. Technical report, Trend Micro

Wu T, Disso J, Ferdinand P, Jones K, Campos A (2013) Towards a scada forensics architecture. In: Proceedings of the 1st international symposium for ICS and SCADA cyber security research

Zhu B, Joseph A, Sastry S (2011) A taxonomy of cyber attacks on scada systems. In: Proceedings of the 2011 international conference on internet of things and 4th international conference on cyber, physical and social computing, pp 380–388

Big Data Security Intelligence for Healthcare Industry 4.0

Gunasekaran Manogaran, Chandu Thota, Daphne Lopez and Revathi Sundarasekar

Abstract Nowadays, sensors are playing a vital role in almost all applications such as environmental monitoring, transport, smart city applications and healthcare applications and so on. Especially, wearable medical devices with sensors are essential for gathering of rich information indicative of our physical and mental health. These sensors are continuously generating enormous data often called as Big Data. It is difficult to process and analyze the Big Data for finding valuable information. Thus effective and secure architecture is needed for organizations to process the big data in integrated industry 4.0. These sensors are continuously generating enormous data. Hence, it is difficult to process and analyze the valuable information. This chapter proposes a secure Industrial Internet of Things (IoT) architecture to store and process scalable sensor data (big data) for health care applications. Proposed Meta Cloud-Redirection (MC-R) architecture with big data knowledge system is used to collect and store the sensor data (big data) generated from different sensor devices. In the proposed system, sensor medical devices are fixed with the human body to collect clinical measures of the patient. Whenever the respiratory rate, heart rate, blood pressure, body temperature and blood sugar exceed its normal value then the devices send an alert message with clinical value to the doctor using a wireless network. The proposed system uses key management security mechanism to protect big data in industry 4.0.

Keywords Industry 4.0 · Internet of Things (IoT) · Big data · Cloud computing · Security · Healthcare

G. Manogaran (✉) · D. Lopez
School of Information Technology and Engineering, VIT University,
Vellore, Tamil Nadu, India
e-mail: gunavit@gmail.com

C. Thota
Albert Einstein Lab, Infosys Ltd, Hyderabad, India

R. Sundarasekar
Priyadarshini Engineering College, Vellore, Tamil Nadu, India

L. Thames and D. Schaefer (eds.), *Cybersecurity for Industry 4.0*,
Springer Series in Advanced Manufacturing, DOI 10.1007/978-3-319-50660-9_5

1 Introduction

Linking people, things and data provides valuable insights into many environments. Nowadays, many smart environments have provide real time solutions for various applications such as natural resource development, healthcare, education, government and private organizational development, and end user computing. Cost, availability and consumption of resources are considered as main resources to develop an innovative environment for solving many real time issues. Recently, Industry 4.0 has introduced many real time solutions to solve various issues in business and organizations.

1.1 Three Kinds of Integration in Industry 4.0

The Industry 4.0 is developed in fourth industrial revolution. The Industry 4.0 consists of more enhanced technologies and methods to improve the overall quality and productivity of the industry. The integration in Industry 4.0 can be classified into three types as follows:

1.1.1 Horizontal Integration

In general, all the organizations are interested to cooperate with other organizations. Horizontal integration is used to define an efficient eco system that enables to share information, finance, and material among various organizations. This would help to improve and identify a new business model.

1.1.2 Vertical Integration

Every factory consists of numerous physical subsystems such as sensor and actuator, control, invention management, manufacturing, and corporate development and planning. All the organizations are required to have a vertical integration to achieve elastic and reconfigurable manufacturing system. Actuator and sensor signals are most often used in vertical integration. This integration is connected with all the levels of the organization include enterprise resource planning (ERP) level. This integration is used to enable the organization to form a self-organized system and energetically reconfigured to adapt diverse product types. In addition, the huge information is composed and processed to create the visible production process.

1.1.3 End-To-End Engineering Integration

In End-To-End Engineering integration, the following activities is involved such as user prerequisite appearance, manufactured goods design and development, manufacture planning, production engineering, invention, services, preservation, and recover. This integration is used to enable the reusability of continuous and consistent product model. The consequence of manufactured goods design on service and production can be identified by authoritative software tool chain.

1.2 Big Data Use in Healthcare Industry

In recent decades, big data analytics also impact more in healthcare. Nowadays, health care systems are rapidly adopting clinical data, which will rapidly enlarge the size of the health records (Lopez and Sekaran 2016). Concurrently, fast progress and development is achieved in modern healthcare management system (Lopez et al. 2014). A recent study expounds, six use cases of big data to decrease the cost of patients, triage, readmissions, adverse events, and treatment optimization for diseases affecting multiple organ systems (Bates et al. 2014). In yet another study, big data use cases in healthcare have been divided into number of categories such as clinical decision support (with a sub category of clinical information), administration and delivery, consumer behavior, and support services. Jee et al. described that how to reform the healthcare system based on big data analytics to choose appropriate treatment path, improvement of healthcare systems, and so on (Jee and Kim 2013; Lopez and Gunasekaran 2015). The above use cases have utilized the following big data in health care implementation (Lopez and Manogaran 2016). (1) Patient-centered framework produced based on the big data framework to approximate the amount of healthcare (cost), patient impact (outcomes), and dropping re-admission rates (Chawla and Davis 2013). (2) Virtual physiological human analysis combined with big data analytics to create robust and valuable solutions in silico medicine (Viceconti et al. 2015).

1.3 Challenges and Potential Solutions in Healthcare Industry

This section presents the various requirements that need to be fulfilled while developing the healthcare IoT system. Internet of things (IoT) technology is used to connect various devices with the Internet and provides more data interoperability methods for application purpose (Manogaran and Lopez 2016b). Nowadays, IoT system most often used to improve the healthcare. However, developing the IoT healthcare system causes the following challenges (Moosavi et al. 2016).

- In general, IoT system interacts with each other in the network. In order to improve the communication within the network, Service oriented- Architecture (SoA) should be developed efficiently
- Standardization is required to have an efficient and effective IoT syste
- Close the gap between users and service providers
- In order to store huge amount of data, proper data synchronization is needed to integrate Cloud and IoT healthcare system
- Big data analytical framework and algorithms are needed to process the huge amount of data generated by the IoT healthcare system
- In order to minimize the transmission overhead, remove the use of multicast/broadcast flooding as well as the frequency of link scope multicast/broadcast messages
- In order to reduce the fragmentation, latency, transmission overhead of data messages while roaming, the payloads regarding data messages and header information should be optimized carefully
- Modern IoT health system must use the distributed storage to store the patients' medical information rather than conventional centralized data storage to support fault tolerance
- In order to protect and maintain the resources, confidentiality, and integrity of the medical information, the advanced authentication and authorization techniques have to be identified
- The modern IoT system should support and compatible with the current IPv6 protocols such as Mobile InternetProtocol version 6 (MIPv6) and Internet Control Message Protocol version 6 (ICMPv6)
- The healthcare IoT system must support the star and mesh topologies including single and multi-hop routing. This is a major concern in healthcare IoT system
- The presence of the available mobile sensors should be notified by the local gateway in the fog layer. This enables necessary updates about the network and resolves tiny sensors performing heavy tasks
- Healthcare IoT system should support the global addressing in mobility solutions. Medical sensors must be detected and addressable at anytime. This is considered as one of the main challenges in IoT healthcare
- Healthcare IoT system should maintain the robust security solution to protect the patients' medical information. In general, AES algorithm is used in the data link layer to protect the data in IoT system. In addition, IPSec (Internet Protocol Security) in the network layer and DTLS (Datagram Transport Layer Security) in the transport layer also performed security solutions to the IoT system
- Mobility is one of the major concerns in real-time healthcare IoT system to avoid jitter, delays, and interruptions of the data transfer during the data handover process.

1.4 Open Research Issues in Healthcare Industry

The following open research opportunities are available in remote health monitoring system using IoT such as:

- In order to maintain energy efficiency, computational system and power consumption, the heavyweight and high power consumption security schemes are reduced to light weight schemes (Khan et al. 2010)
- The efficient classification of normal and emergency traffic scenarios are needed in healthcare IoT system to avoid any delay (delay may affect the disease diagnosis and taking proper action especially in a real-time health monitoring) (Ullah et al. 2009)
- Reliability and Quality of Service (QoS) are considered as hot issues in Healthcare IoT (Chen et al. 2010)
- It is important to consider the mobility in IoT healthcare system. This helps patients against difficulties and constraint when carried out day-to-day activities (Filipe et al. 2015)
- Data protection and security in healthcare are also considered as open issues in wireless body are networks (Pantelopoulos and Bourbakis 2010)
- Data storage and management are also considered as major issues in IoT healthcare system

2 Overview of the Smarter HealthCare Industry

2.1 Internet of Things and Internet of Everything

In general, Internet connections are always used for laptop, desktop computers and tablets. Nowadays, more number of advanced devices such as heart pressure watches and body temperature belt are also connected to the Internet to transfer the individuals' health information continuously. Not only in healthcare, but also more applications like smart city, smart traffic control and weather monitoring applications. Normally, IoE technologies varies the range from digital sensor devices used for various applications to smarter and numerous interconnected wireless devices, smart industrial applications and various distributed hardware technologies that have just become more automated and smarter (Manogaran and Lopez 2016c). In general, features of IoE have classified into two types namely input and output. Input function is used to allow the external data into a device while output function is used to transfer the device data into Internet (Manogaran et al. 2017).

Recently, The IoE term is plays a vital role in Information Technology fields. For example, Cisco is one of the leading institute has focused more in IoE based technologies. Internet of Everything is enhanced from the previous versions of Internet based technologies such as Internet of Things, Internet of Humans,

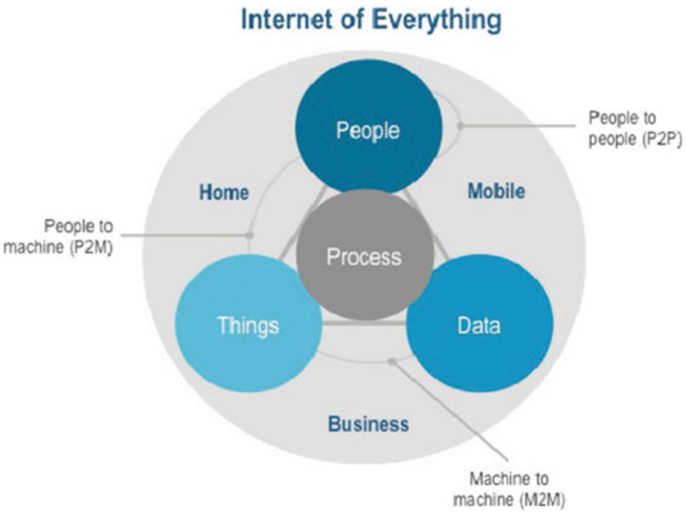


Fig. 1 People, things, data and process of IoE

Industrial Internet of Things and Internet of Digital. In other words, IoE is a System with end to end connectivity among processes, technologies and concepts engaged across all connectivity use cases (Fig. 1). IoE is basically consists of four connections parts such as People, Things, Data and Process.

People. Destination or target nodes are interconnected with the internet to distribute activities and data. In IoE enables people to connect to the Internet in incalculable ways. Nowadays, many people connect to the Internet using their own smart devices such as PCs, TVs, tablets, and smart phones. In addition, they also use social networks such as Twitter, Facebook, LinkedIn, and Pinterest. As the Internet grows toward IoE, we will be connected in more related and helpful ways.

Things. Things are the most important components in the IoE system. Things used to observe the more relevant data from the physical devices. Collected data from IoE devices are used to take valuable decisions in near future and emergency situations. For example, the medical smart devices in IoE healthcare application are used to observe the individuals information that efficiently monitor the patient health in emergency situations. This collected information is transferred into the data store to analyze further appropriate and valuable decisions.

Data. IoT devices normally collect data and stream it over the Internet to the sensor server, where it is processed and analyzed. Due to the capabilities of things connected to the Internet persist to advance; they will become additional intellectual by combining data into more valuable information. Unprocessed data after generated from devices will be process and analyze into valuable statistics to provide control mechanisms and intelligent decisions. For example, high and low heart rate measurements are used to find the average heart rate of patient in healthcare industry.

Processes. Process plays a significant role in measuring how entities like data, people, and things are works with others to bring value in the connected world of IoE. With the accurate process, connections turn into applicable and add value because the exact information is transferred to the specific destination or device in the proper way. In addition, the strong connectivity between the smart devices, data, and individuals are used to gain the high value insights from the IoE system. For example, use of social networks and smart fitness devices to promote pertinent healthcare offerings to prospective customers.

The tools and technologies for developing and deploying the powerful IoT applications are depicted in the Table 1. It includes communications standard, encoding scheme, electronic product code, type of sensor, RFID type and other network details.

Table 1 Tools and Technologies for IoT

Technologies	Standards
Communication	IEEE 802.15.4(ZigBee) IEEE 802.11 (WLAN) IEEE 802.15.1(Bhietooth, Low energy- Bluetooth) IEEE 802.15.6 (Wireless Body Area Networks) IEEE 1888 IPv6 3G/4G UWB
Data content and encoding	EPC Global Electronic Product Code, or EPCTM, EPC Global Physical Mark Up Language, EPC Global Object Naming Sen-ice (ONS)
Electronic product code	Auto-ID Global Trade Identification Number (GTIN), Serial Shipping Container Code (SSCC), and the Global Location Number (GLN)
Sensor	ISO/IEC JTC1 SC31 and ISO/IEC JTC1 WG7, Sensor Interfaces: IEEE 1451.x, IEC SC 17B, EPC global, ISO TC 211, ISO TC J05
Network management	ZigBee Alliance, IETF SNMP WG, ITU-T SG 2, ITU-T SG 16. IEEE 1588
Middle	ISO TC 205, ITU-T SG 16
RFID	RFID air interface Protocol ISO 11785 RFID payment system and contactless smart card: ISO 14443/15693 Mobile RFID:, ISO/IEC 18092 ISO/IEC 29143 ISO 18000-2—for frequencies below 135 kHz ISO 18000-3—for 13.56 MHz ISO 18000-4—for 2.45 GHz ISO 18000-6—for 860 to 960 MHz ISO 18000-7—for 433 MHz

In order to achieve an efficient communication between the devices in the internet, layered architecture (Fig. 2) is identified with different layers as Application, Communication, Security, Embedded, Hardware, Integration and DB Layer (Table 2).

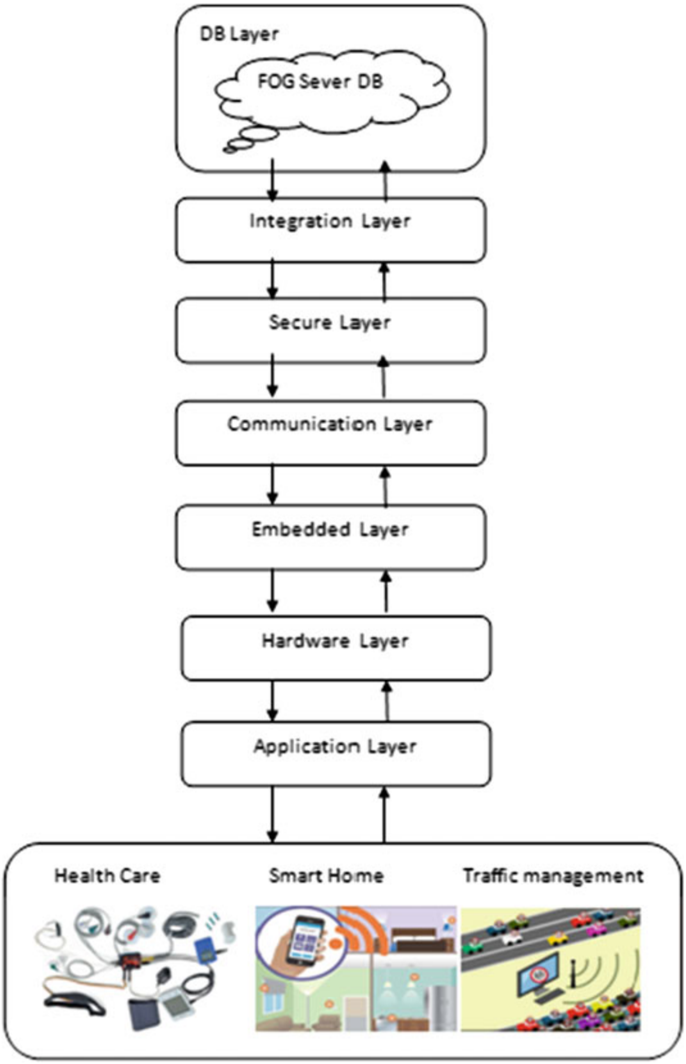


Fig. 2 Layered architecture

Table 2 Layers and their Tasks

IoT layers	IoT components	Tasks	Used technologies
Application layer	Applications	Provide security against read/view health information	Smart home technology, robotics, Cloud computing, fog computing
Hardware layer	Device discovery, access control, data management	Enables communication between applications and things	CoAP, MQTT, REST, OMA Lightweight, OMA DM, EPC, ONS
Embedded layer/sensing layer	Physical objects	Collect, monitor, identify, and provide data about disabled users in their environments	RFID, sensors, actuators
Communication layer/network layer	Communication technologies	Wireless WAN: Transmit information over Internet from devices or gateway	Wireless WAN: 2G, 3G, Long Term Evaluation (LTE), Long Term Evaluation- Advanced (LTE-A), 4G, 5G, Satellite networks, etc.
		Wireless PAN/LAN: Enables devices to share or exchange information	Wireless PAN/LAN: RFID, Bluetooth, Wi-Fi, Li-Fi, ZigBee, 6LoWPAN
Secure layer	Embedded security, application security	Securing the things which are connected by internet, Applications deployed in IoT	PKI Certificate, Encryption and Decryption technologies, Cryptography tools
Integration layer	Hardware layer to fog to cloud integration, devices to fog server integration	Integration means communication from health devices to fog server and fog to cloud remote servers	Java Web services, AWS,
DB layer	Database technologies	Connecting the applications to Data base in the cloud and fog	Oracle Cloud, Microsoft Azure, AWS EBS, AWS EMR,

2.2 Recent Work in Smart Healthcare Industry

Nowadays, wireless mobile sensor network is used in continues monitoring of healthcare applications, where patients are monitored with the help of sensor devices. In recent years, more number of researchers are trying to use Wireless Mobile Sensor network to provide continuous patient monitoring, in-ambulatory, in-hospital, in-clinic, and open environment monitoring (e.g., athlete health monitoring). This section describes the research work related to the healthcare systems using medical sensor networks and sensor devices. Harvard Sensor Network Lab recently developed the CodeBlue project, which aims to monitor the patients (Lorincz et al. 2004; Malan et al. 2004). In this project, several medical sensors (e.g., EKG, pulse oximeter, EMG, and SpO2 sensor board onto the Mica2 motes) are fixed on the patient's body to sense the health conditions. In addition, these medical sensors continuously sense the patient body data and transmit to the end-user devices (laptops, PDAs, and personal computers) using wireless technologies for further data analysis. This data are generally used to find useful patterns to protect the patients from emergency situations. The main function of CodeBlue is very simple, a medical professional or doctor issues a query for patient healthcare data using their personal digital assistant (PDA), which works based on the publish and subscribe architecture. Finally, the collected data from the medical sensors are publishing to a specific channel and end-user need to subscribe the channel by using their laptop and PDA (Kumar and Lee 2011). Wood et al. (2006) from University of Virginia have developed the heterogeneous network architecture named Alarm-Net (Wood et al. 2006). The goal of this project is to monitor the patient health in the home and assisted-living environment. Similarly, Ng et al. (2004) have developed the Ubiquitous monitoring environment for wearable and implantable sensors (UbiMon) (Ng et al. 2004). This project is a type of Body Sensor Network (BSN) architecture composed of implantable and wearable sensors using the wireless ad hoc network. The main goal of this project is to provide continuous monitoring of patient's health status and also predict the emergency conditions.

In addition to the IoT in healthcare, more research and development is going in the field of IoT. For example, Batalla et al. (2016) have developed the hierarchical network infrastructure for connecting IoT objects and services in simple and flexible way (Mongay Batalla et al. 2016). Mavromoustakis et al. (2016) have discussed various technologies and methods in the fast-evolving field of IoT with 5G mobile network. In addition, Hadjioannou et al. (2016) have discussed various security and privacy issues related to IoT systems. Batalla et al. (2016) have proposed a framework to monitor the number of users in IoT environment.

2.3 Security and Privacy Requirements in Smart HealthCare Industry

Components of IoT are classified into various group's namely physical objects, communication technologies and applications (AL-mawee 2012). Table 3 depicts the various components of IoT and its Vulnerabilities, Types of Threats and Attacks, and available Security Requirements and Solutions to overcome the issues.

Table 3 Various security requirements and solutions in components of IoT

Components in the IoT	Vulnerabilities	Types of threats and attacks	Available security requirements and solutions
Physical objects in IoT	• Physical layer devices have limited Communication, calculation and storage resources • Physical objects are distributed in various regions. Hence, unauthorized user can accesses the devices and performs damages and illegal actions such as reprogram the device, extract security keys and information.	• DoS/DDoS attacks • Physical attacks • Integrating WSNs • Integrating RFID • Unauthorized access control and data access	• Encryption/Cryptographic techniques • Continuously evaluates the suspicious nodes' behaviour can reduce the influence of malicious user access • Authentication • Authorization • Access control • Identification
Communication technologies in IoT	• IoT is a dynamic network infrastructure • Power issues • Network issues • Selection of security technique and its challenges	• Wireless WAN communications • Wireless LAN/PAN communications • Secure IoT communication protocols in constrained resources environment • Secure transmitted data	• Communication security: Security algorithm and protocols used to provide smoothness transitions connections among different edge networks • Encryption/decryption is used to provide confidentiality service • Strong authentication also used to provide security solutions • Backup solution is used when network fails • IoT communication protocols enhancement also increase the security • Authorized access and Availability
Applications of IoT	• Data coverage • Cloud computing • Security issues in web application • Secure communication	• DoS • XSS attack • CSRF attack • SQL Injection • Data protection • Data access • PHRs Attacks • Malicious user attacks • Sharing data in different environments • Real-time information processing • Sharing the same sensed data by several applications	• Data separation is used between information content and information source • Encryption/decryption mechanisms • Secure data access • Confidentiality of data • Secure sensitive data • Backup plan • Proposing traditional distributed database technology • Scheduling techniques • Assuring identification • Assuring authentication • Firewall and antivirus • Intrusion detection • Enhanced communication protocols security

3 Industry 4.0 for Smart HealthCare Monitoring System

Nowadays, various organizations are uses Industry 4.0 to achieve great efficiency in production and development. In this chapter the proposed framework for healthcare is developed based on the Internet of Things. In recent years, IoT is used in many healthcare services such as continues monitoring of patient health, automation in clinical test for patient and provide high value insights in healthcare. Especially, continuous monitoring of healthcare system produces huge amount of data that could not processed by traditional data processing tools and techniques. In order to overcome this issue various big data based scalable algorithms and tools are developed to process and analyze such huge data. It is important to provide security in the big data. Though, various solutions are already available in data security. This chapter provides security framework for Meta Cloud (MC) architecture. The Meta Cloud architecture is used to process and store various applications deployed in the cloud. This architecture is efficiently forward the data to the specific cloud service based on Grouping and Choosing (GC) architecture.

The proposed big data intelligence architecture is shown in Fig. 4 used to interact with all data centers deployed in the cloud environment. This interaction is used to build high value business insights and improve the overall effectiveness. The primary function of the proposed big data intelligence system is mentioned below:

- The proposed intelligent system is used to collect various data generated from various cloud data centers
- The proposed intelligent system processes the captured data from IoT and IoE systems and applications
- The proposed intelligent system used to provide the optimal solutions with different alternatives to the end-users
- The proposed intelligent system used to provide intelligence/Knowledge to the stakeholders (Doctors, Scientists, web of things, etc.)

In this chapter IaaS is used to store the big data collected based on the Industry 4.0. The IoT technology is used to collect the data and it stored into the IaaS.

3.1 Meta Cloud-Redirection (MC-R) Architecture

Meta Cloud Data Storage architecture is proposed in this chapter to protect and process the big data in cloud computing (Fig. 3). Different cloud data storage providers such as Amazon and Google Cloud are used to store the user data. Data generated from Meta cloud are classified into three levels such as sensitive, critical and normal. Each categorized data are stored in different data center based on the level of privacy. Proposed Meta Cloud Data Storage architecture uses an interface to redirect the user request to the appropriate datacenter in cloud. AWS Cloud Trail

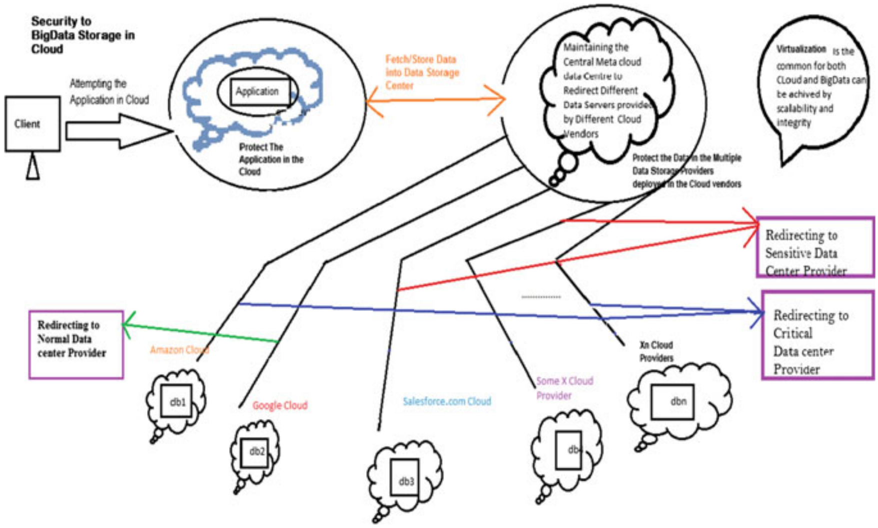


Fig. 3 Meta cloud data storage architecture to secure big data in cloud

is used in this proposed framework to process the log files. AWS Key Management Service (KMS) is integrated with AWS CloudTrail that transfers log files to an Amazon S3 bucket. CloudTrail can easily integrate with any application using proper API. AWS CloudTrail is capable of maintaining the time of the API call, IP address of the API caller, the request and response parameters the AWS service.

In this proposed framework datacenters are distributed into a sequence of n parts, where each part can be denoted by part i (i ¬ (1, n)), and stored at m different storage providers, where each provider is identified as provider j (j¬ (1, m)). In general, (parts of the datacenter) n is always far greater than (number of provide) m, these m storage providers belong to different organizations, such as Amazon, Google and Salesforce. When big data is stored in the datacenter it forms a unique storage path given as: Mapping Storage_Path = {Data((P1(M1, M2 … Mr))(P2 (M1, M2 … Ms)) … (Pn(M1, M2 … Mt))}; where, P denotes the storage provider and M denotes the physical storage media. Big data are always enormous and impossible to encrypt them as a whole, so proposed framework encrypt the storage path of the big data, and get a cryptographic value which can be called cryptographic virtual mapping of big data. So instead of protecting the big data itself, the proposed framework protects mapping of the various data elements to each provider using Meta Cloud Data Storage interface.

The proposed framework will distribute all data parts in different storage service providers, and each provider holds some of the data parts (Manogaran et al. 2016). In order to provide high availability and robustness, the proposed framework will store multiple copies of same data on different cloud storage providers. Though, big data is split and stored in different data center, the administrator of the entire system maintains the storage index information for each data parts. When there is a problem in some data parts on the cloud storage, propose framework can find another copy of the data parts using their storage index information. Figure 3 shows how the end user will access the applications and how the data is stored into the distributed cloud. The proposed security algorithm protects the unauthorized user trying to access the application which is deployed in cloud. Threat_updated data store is used to store the entry related to malicious attempt, whereas Meta Data Storage Cloud table stores information related to the data storage entry of different vendors. Critical, Sensitive and non-sensitive data are stored in other tables.

3.1.1 Data Collection Phase

In general, data collection is the process of measuring and gathering the useful information on targeted variables in an established manner. In our proposed architecture, this phase collects data from different applications of organizations. Here, the customers or end users are trying to access the applications for their business requirements. When a customer logged into the datacenter to access the data, system is automatically generates the user login information, transactional information, personnel information, and financial information etc. The data may be generated from customers, external systems, different datacenters, and digital electronic machines which are directly or indirectly connected to the proposed architecture.

3.1.2 Data Transfer Phase

After successfully identified the authorized user data can securely transfer to different data storage centers provided by different cloud data service providers. Meta Cloud Data Storage architecture is used to transfer the data from applications to cloud data centers and cloud data centers to applications.

3.1.3 Data Processing Phase

After collecting data from the data collection phase, it needs to be processed. In this processing phase, authentication and authorization will be performed to identify the authorized user. Authentication is used to know exactly who is accessing their information or site. Here, Authorization is used to determine if the client has permission to use a resource or access an application deployed in cloud. Once the authentication and authorization process is done, then the proposed architecture protects the sensitive logged in credentials. PKI Certification methodology is used in this proposed architecture to secure the user credentials. In addition, this data protection phase also checks the following conditions such as (a) Logged in user is trusted one or not? (b) User credentials are appropriate or random values? (c) Browser details (d) geo-location of the logged in user (e) IP and MAC address of the logged in user's machine.

Log File Processing

The information captured by log files is used to maintain the history of the applications in different concerns. Logging is a computational activity in which a program records all the activity in a simple text file in a custom format. This text file is generally stored with .log extension. Many log/data analysis programs are available on the internet to analyze the log data. In the proposed methodology our main task is maintain, process and find out the actual results of the applications from customer's perspective.

An audit log is a document that records an event in an information (IT) technology system. AWS Cloud Trail is used in this proposed framework to process the log files. AWS Key Management Service (KMS) is integrated with AWS CloudTrail that delivers log files to an Amazon S3 bucket. Amazon S3 Bucket logging records all the activities and requests made on S3 Bucket. This log records consists of activities and requests details. This includes the date and time the request was made, the type of the request, and the resource request details. CloudTrail integrates with any software application using proper API. AWS CloudTrail is capable of maintaining the time of the API call, IP address of the API caller, the request and response parameters the AWS service.

MapReduce Algorithm for Log Processing in Distributed Cloud Data Centers

Map Reduce is a programming model or framework that process tasks in parallel across a huge size of systems. It contains two functions such as Map and Reduce. Map function splits the huge size of input data into <key, value> pairs. Intermediate <key, value> pairs will be created bases on aggregating several input key value pairs from the Map phase. Finally, Reduce function takes the intermediate key value pairs and produces the output <key, value> pairs that can be easily understood by the end user. In this proposed architecture, Map Reduce framework is used to find the number of users who were logged into the cloud data center. Proposed Map Reduce pseudo code can efficiently process the huge size of log file. The log file contains information regarding users who were logged in with date and the log in time duration. As shown in the Fig. 4, the first process is map phase in which each date that represents the key is assigned a value of one initially. While reduce phase, the key values are summed up to find out the number of users logged in. For example, three users were logged in 01-02-2016, whereas two users were logged in 02-02-2016.

Mapper Function

```
public void Map(LongWritable key, Text value, OutputCollector output, Reporter reporter)
for each key ϵ value do
Emit(term key; count 1)
```

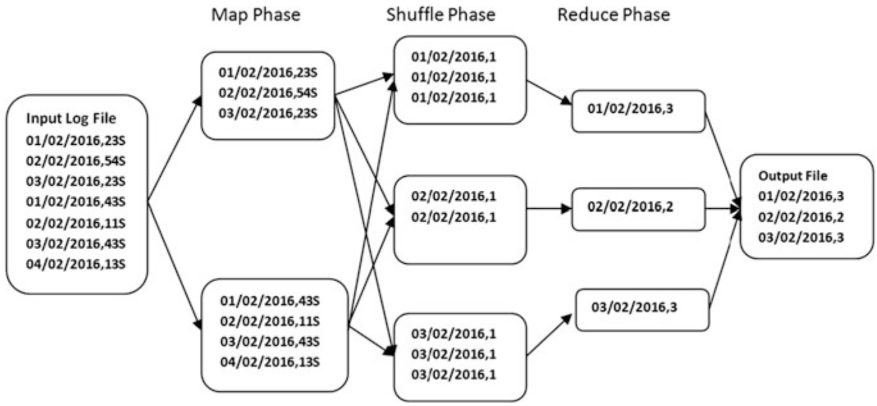


Fig. 4 MapReduce framework for processing log files

Reducer Function

```
public void reduce(Text key, Iterator values, OutputCollector output, Reporter reporter)
sum←0
for each v ϵ value do
sum←sum + v
Emit(key, sum)
```

3.1.4 Categorization of the Data

Critical Data

Critical data are defined as “the data that is critical to success” in a specific business area (line of business, shared service, or group function), or “the data required to get the job done”. The data is critical in one business area may not be critical in another.

Sensitive Data

Sensitive data encompasses a wide range of information that include political opinion, religious or other similar beliefs, memberships, physical or mental health details and personal life or criminal or civil offences. Sensitive data include information that also related to consumer, client, employee, patient or student; and it can be identifying information as well: your contact information, identification cards and numbers, birth date, and parents’ names.

Normal Data

Normal data is a wide range of public data such as reports and news from company or organization. This data will not be protected from any one and always available to everyone.

3.1.5 Big Data Storage Phase

Once the data is transferred from applications to cloud data centers it needs to be store efficiently. Nowadays, a number of data provisions has increased, such as high throughput instruments, telescopes, sensor networks and streaming machines and these environments produce huge amount of data. Hadoop Distributed File System (HDFS) is used in this phase to store such huge amount of data. This phase also categorize the data into different level and store them into different data centers.

3.1.6 Security Phase

In order to provide security in the Meta Cloud Data Storage architecture the following algorithm is used.

/*Process the Audit Log File to check the logged in user’s details like his/her/AI Machine track status, last Logged in time etc.*/

```
Select customerid, password, last_loggedin_time, current status, geolocation, browser type, ipconfig, sysdate from updated_audit_log;
//If any malicious user tried to login application
{
Insert into Threat_updated values (customerid, password, geolocation, browsertype, geolocation, sysdate);
return -1;
}
else {
List l = Select DataStorageproviderName, DataScope from MetaDataStorageCloud where Customer_loggedin_ApplicationId =?;
If (l.DataStorageproviderName ==’’amzoncloud” &&l.datascope ==”critical”)
{
Goto → Amazon Cloud Data Storage
Select * from AmazonCloudDataStorage where Customer_loggedin_ApplicationId =?;
}
elseif(l.DataStorageproviderName ==”googlecloud” &&l.datascope ==”sensitive”)
{
Goto → google Cloud Data Storage
Select * from GoogleCloudDataStorage where Customer_loggedin_ApplicationId =?;
}
elseif (l.DataStorageproviderName ==”xcloud”&&l.datascope ==”normal”)
{
Goto → x cloud data storage;
Select * from XcloudCloudDataStorage where Customer_loggedin_ApplicationId =?;
}
}
}//end else
```

3.2 Big Data Knowledge System for Industry 4.0 Systems

The Characteristics of the Data in Big Data Intelligence System (Fig. 5) following considered:

3.2.1 Data Volumes

The traditional data processing tools and technologies is not applicable to process the huge data generated from various heterogamous sources. The proposed big data based knowledge system is capable of processing and storing large amount of health data generated from various IoT devices. Distributed storage system is used in our proposed framework to achieve scalability and elasticity.

3.2.2 Data Integrity and Security

As proposed framework concentrates on healthcare, there is a need to provide security in the system. Healthcare records consist of patients’ personal information such as name, address and disease details. In order to protect the personal details, the proposed system uses the authorization and authentication process (Fig. 6).

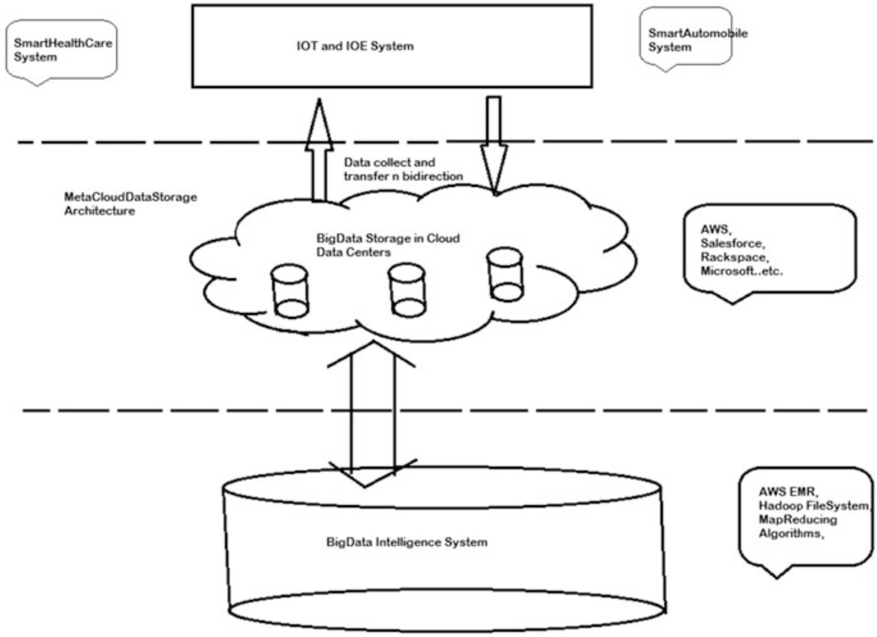

SmartHealthCare System
IOT and IOE System
SmartAutomobile System
Data collect and transfer n bidirection
MetaCloudDataStorage Architecture
BigData Storage in Cloud Data Centers
AWS, Salesforce, Rackspace, Microsoft..etc.
BigData Intelligence System
AWS EMR, Hadoop FileSystem, MapReducing Algorithms,

Fig. 5 Proposing Big data knowledge system for industry 4.0 systems

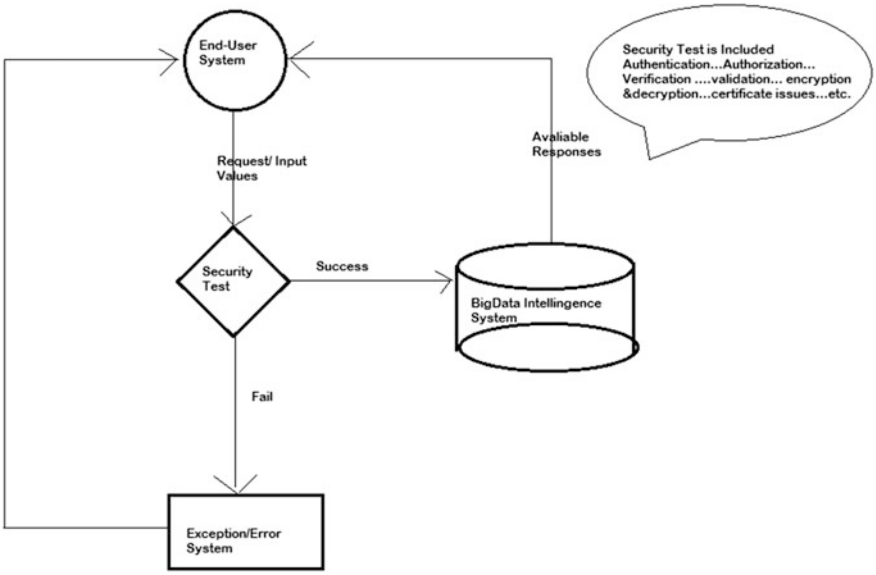

End-User System
Security Test is Included Authentication...Authorization... Verification ....validation... encryption &decryption...certificate issues...etc.
Avaliable Responses
Request/ Input Values
Security Test
Success
BigData Intellingence System
Fail
Exception/Error System

Fig. 6 Flow diagram for proposed system

4 Discussions

4.1 Security Issues in Various Cloud Deployment Models of Meta Cloud Data Storage Architecture

Integration of Big Data with various cloud deployment models (private, public or hybrid) significantly impact cost, technical demands and other factors. Technologies like the Internet of Things assure a tsunami of new data for researchers, businesses and governments to process. While Big Data is not dependent on the cloud, cloud assists Big Data analytics and storage, enabling scalable, on-demand processing at a sensible price. Data security is a major challenge to the CSPs and developers.

Data security is more essential when using cloud computing at all levels: SaaS, PaaS and IaaS. The major aspects of data security are mentioned below:

- Security in Data Transfer
- Security in Data Storage
- Data lineage

4.1.1 Security in Data Transfer

In regards to the security in data transfer, the major risk is not using a vetted encryption techniques and algorithm. While this is understandable to information security professionals, it is not general for others to realize this constraint when using a public cloud in spite of IaaS, PaaS and SaaS. In general, simply encrypting data and using the non secured protocol can enable confidentiality but not ensure the data integrity.

4.1.2 Security in Data Storage

Encryption to protect data storage seem understandable, the actuality is not that easy. If we use a public IaaS cloud service or private cloud service for AWS S3, encryption for data storage is feasible and strongly recommended. Nevertheless, encrypting the data in storage that a PaaS and SaaS cloud based application is using (Google Apps, Salesforce.com) as a balancing control is not all the time feasible. Data in storage used by an application is usually not encrypted since encryption would prevent searching or indexing of that data.

4.1.3 Data Lineage

Once the data is transmitted to the cloud by organization, it may be encrypted or not. It is helpful and might be mandatory (for compliance or audit reasons) to identify accurately where and when the data was particularly placed within the cloud. The path of the data represents mapping application data flows or data path visualization is known as data lineage, is significant for an auditor's declaration. Though, enabling data lineage to organization or auditors is taking more time, still the location is entirely under an organization control.

4.2 Merge Industry 4.0 with Other Healthcare Applications

The various application of IoT in healthcare is depicted in Fig. 7. Wearable sensors and it functionalities is depicted in Table 4.

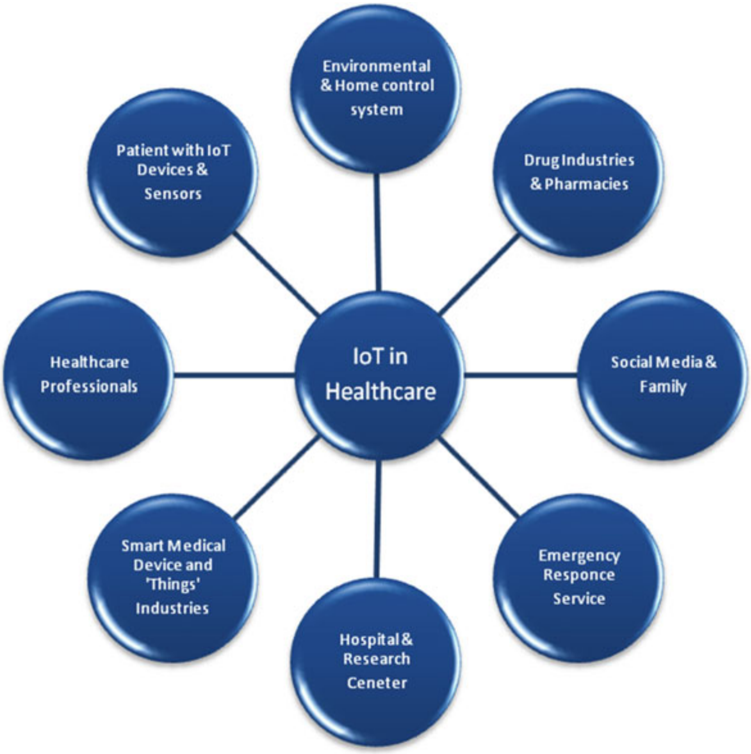

Environmental & Home control system
Patient with IoT Devices & Sensors
Drug Industries & Pharmacies
Healthcare Professionals
IoT in Healthcare
Social Media & Family
Smart Medical Device and 'Things' Industries
Emergency Responce Service
Hospital & Research Ceneter

Fig. 7 IoT applications in healthcare

Table 4 Commonly used wearable sensors in human body

S. no	Name of the sensor	Sensor use	Sensor measurement type	Sensor placement
1	Accelerometer	Measuring the human energy expenditure	Continuous	Wearable
2	Carbon dioxide sensor	Measuring the carbon dioxide level from mixed gas	Discrete	Wearable
3	ECG/EEG/EMG sensor	Measuring the electrocardiograph signal	Continuous	Wearable
4	Gyroscope	Measuring the angular velocity with respect to the body axis	Continuous	Wearable
5	Humidity sensor	Measuring the sweating rate	Discrete	Wearable
6	Blood oxygen saturation sensor	Measuring the percentage of oxygen saturation in blood	Discrete	Wearable
7	Pressure sensor	Measuring the pressure changes of the underside of foot	Continuous	Wearable/surrounding
8	Respiration sensor	Measuring the rate of breathing	Continuous	Wearable
9	Temperature sensor	Measuring the rate of body temperature	Discrete	Wearable
10	Visual sensor	Capturing the motion, length, location, and area	Continuous/Discrete	Wearable/surrounding
11	Blood pressure sensor	Measuring the systolic and diastolic pressure	Continuous	Wearable
12	Heart rate sensor	Measuring the heart rate	Continuous	Wearable
13	Blood sugar sensor	Sensors record glucose levels continuously around the clock	Continuous	Wearable

5 Conclusion

Secure Industrial Internet of Things (IoT) architecture is proposed in this chapter to store and process scalable sensor data (big data) for health care applications. Proposed Meta Cloud-Redirection (MC-R) architecture with big data knowledge system is used to collect and store the sensor data (big data) generated from different sensor devices. The proposed system uses key management security mechanism to protect big data in industry 4.0. In proposed system, sensor medical devices are fixed with the human body to collect clinical measures of the patient. Whenever the respiratory rate, heart rate, blood pressure, body temperature and blood sugar exceed its normal value then the devices send an alert message with clinical value to the doctor using wireless network.

References

AL-mawee W (2012) Privacy and security issues in IoT healthcare applications for the disabled users a survey. Western Michigan University, Master's Theses

Batalla JM, Mavromoustakis CX, Mastorakis G, Sienkiewicz K (2016) On the track of 5G radio access network for IoT wireless spectrum sharing in device positioning applications. In: Internet of Things (IoT) in 5G mobile technologies. Springer International Publishing, pp 25–35

Bates D, Saria S, Ohno-Machado L, Shah A et al (2014) Big Data in health care: using analytics to identify and manage high-risk and high-cost patients. Health Aff 33(7):1123–1131. doi:10.1377/hlthaff.2014.0041

Chawla N, Davis D (2013) Bringing big data to personalized healthcare: a patient-centered framework. J Gen Intern Med 28(S3):660–665. doi:10.1007/s11606-013-2455-8

Chen M, Gonzalez S, Vasilakos A, Cao H et al (2010) Body area networks: a survey. Mobile Netw Appl 16(2):171–193. doi:10.1007/s11036-010-0260-8

Filipe L, Fdez-Riverola F, Costa N, Pereira A (2015) Wireless body area networks for healthcare applications: protocol stack review. Int J Distrib Sensor Netw:20151–20223. doi:10.1155/2015/213705

Hadjioannou V, Mavromoustakis CX, Mastorakis G, Batalla JM, Kopanakis I, Perakakis E, Panagiotakis S (2016) Security in smart grids and smart spaces for smooth IoT deployment in 5G. In Internet of Things (IoT) in 5G mobile technologies. Springer International Publishing, pp 371–397

Jee K, Kim G (2013) Potentiality of big data in the medical sector: focus on how to reshape the healthcare system. Healthc Inform Res 19(2):79. doi:10.4258/hir.2013.19.2.79

Khan J, Yuce M, Bulger G, Harding B (2010) Wireless body area network (WBAN) design techniques and performance evaluation. J Med Syst 36(3):1441–1457. doi:10.1007/s10916-010-9605-x

Kumar P, Lee H (2011) Security issues in healthcare applications using wireless medical sensor networks: a survey. Sensors 12(12):55–91. doi:10.3390/s120100055

Lopez D, Gunasekaran M (2015) Assessment of vaccination strategies using fuzzy multicriteria decision making. In: Proceedings of the fifth international conference on fuzzy and neuro computing (FANCCO-2015). Springer International, pp 195–208

Lopez D, Manogaran G (2016) Big data architecture for climate change and disease dynamics. In: Tomar GS et al (eds) The human element of big data: issues, analytics, and performance. CRC Press, Florida, United States

Lopez D, Sekaran G (2016) Climate change and disease dynamics—a big data perspective. Int J Infect Dis: 4523–4524. doi:10.1016/j.ijid.2016.02.084

Lopez D, Gunasekaran M, Murugan BS, Kaur H, Abbas KM (2014) Spatial Big Data analytics of influenza epidemic in Vellore, India. In: 2014 IEEE international conference on big data. IEEE, pp 19–24

Lorincz K, Malan D, Fulford-Jones T, Nawoj A et al (2004) Sensor networks for emergency response: challenges and opportunities. IEEE Pervasive Comput 3(4):16–23. doi:10.1109/mprv.2004.18

Malan D, Fulford-Jones T, Welsh M, Moulton S (2004) Codeblue: an ad hoc sensor network infrastructure for emergency medical care. In: International workshop on wearable and implantable body sensor networks, vol 5

Manogaran G, Lopez D (2016a) Health data analytics using scalable logistic regression with stochastic gradient descent. Int J Adv Intell Paradigms 9(1):1–18

Manogaran G, Lopez D (2016b) Disease surveillance system for big climate data processing and dengue transmission. Int J Ambient Comput Intell 8(1):1–27

Manogaran G, Lopez D (2016c) A survey of big data architectures and machine learning algorithms in healthcare. Int J Biomed Eng Technol 23(4):1–27

Manogaran G, Thota C, Kumar M (2016) MetaCloudDataStorage architecture for big data security in cloud computing. Procedia Comput Sci:87128–87133. doi:10.1016/j.procs.2016.05.138

Manogaran G, Thota C, Lopez D, Vijayakumar V, Abbas KM, Sundarsekar R (2017) Big data knowledge system in healthcare. In: Bhatt C, Dey N, Ashour A (eds) Internet of things and big data technologies in next generation healthcare. Studies in big data series, Springer International Publishing, pp 1–25

Mavromoustakis CX, Mastorakis G, Batalla J M (eds) (2016) Internet of Things (IoT) in 5G mobile technologies, vol 8. Springer

Mongay Batalla J, Gajewski M, Latoszek W, Krawiec P et al (2016) ID-based service-oriented communications for unified access to IoT. Comput Electr Eng: 5298–5113. doi:10.1016/j.compeleceng.2016.02.020

Moosavi S, Gia T, Nigussie E, Rahmani A et al (2016) End-to-end security scheme for mobility enabled healthcare Internet of Things. Fut Gen Comput Syst:64108–64124. doi:10.1016/j.future.2016.02.020

Ng JW, Lo BP, Wells O, Sloman M, Peters N, Darzi A, Toumazou C, Yang GZ (2004) Ubiquitous monitoring environment for wearable and implantable sensors (UbiMon). In: International conference on ubiquitous computing (Ubicomp)

Pantelopoulos A, Bourbakis N (2010) A survey on wearable sensor-based systems for health monitoring and prognosis. IEEE Trans Syst Man Cybern Part C (Appl Rev) 40(1):1–12. doi:10.1109/tsmcc.2009.2032660

Wood A, Virone G, Doan T, Cao Q, Selavo L, Wu Y, Fang Z, He S, Lin J, Stankovic, J (2006) ALARM-NET: Wireless sensor networks for assisted-living and residential monitoring. University of Virginia Computer Science Department Technical Report

Ullah S, Khan P, Ullah N, Saleem S et al (2009) A review of wireless body area networks for medical applications. IJCNS 02(08):797–803. doi:10.4236/ijcns.2009.28093

Viceconti M, Hunter P, Hose R (2015) Big data, big knowledge: big data for personalized healthcare. IEEE J Biomed Health Inform 19(4):1209–1215. doi:10.1109/jbhi.2015.2406883

Decentralized Cyber-Physical Systems: A Paradigm for Cloud-Based Smart Factory of Industry 4.0

Zhinan Zhang, Xiang Li, Xin Wang and Hui Cheng

Abstract The trend of future manufacturing requires manufacturers to sustainable optimize the utilization of resources (e.g. people, equipment, material, methods, and environment) to lean produce high quality product, and quickly adapts to changes of market demands and supply chain partners. German's Industry 4.0 has attracted extensive attention in the world in recent years, which is believed to be a new paradigm to meet the ever changing requirements of future manufacturing. Industry 4.0 focuses on building cyber-physical systems (CPS) based product creation eco-system with highly flexible and reasonable cost with just-in-time reactivity. However, on the way to build such an eco-system is still need effort to investigate technological foundations of CPS and deeply cognitive understanding of key concepts with considering the context of implementation of industry 4.0 landscape. In the context, this chapter introduces the conceptual model and operation mechanism of decentralized cyber-physical systems (CPS), which enables manufacturers to utilize a cloud-based agent approach to create an intelligent collaborative environment for product creation. A brief introduction to the connotation of industry 4.0 and smart factory of industry 4.0 from the perspective of China's industry and academic is given. The concept of decentralized cyber-physical systems agents is proposed and discussed, with the focus on conceptual model, operation mechanism

Z. Zhang (✉)
School of Mechanical Engineering,
Shanghai Jiao Tong University, Shanghai 200240, China
e-mail: zhinanz@sjtu.edu.cn

X. Li
Beijing Sysware Technology Co., Ltd., Beijing 100192, China
e-mail: lix@sysware.com.cn

X. Wang
Department of Industrial and Manufacturing Systems Engineering,
The University of Hong Kong, Hong Kong, China
e-mail: wangxinmandy@gmail.com

H. Cheng
Shanghai Spaceflight Manufacture (Group) Co., Ltd., Shanghai 200245, China
e-mail: cheng_and_hui@163.com

L. Thames and D. Schaefer (eds.), *Cybersecurity for Industry 4.0*,
Springer Series in Advanced Manufacturing, DOI 10.1007/978-3-319-50660-9_6

and key technologies. After that, a cloud-based smart manufacturing paradigm is presented. The architecture and business process model of such a paradigm is developed. Finally, a case study of how a manufacturing enterprise uses the proposed paradigm to implement the smart factory of industry 4.0 in China. This study benefits both academic researchers and industrial engineers and decision makers with the proposed paradigm as well as case study.

Keywords Cyber-physical system • Industry 4.0 • Smart factory • Cloud-based manufacturing • Lean product creation

1 Introduction

Industry plays an important role in the social development. Recently, Germany introduced an idea of Industry 4.0 and it has drawn wide attention. Industry 4.0 aims at improving the levels of intelligence of manufacturing industry. Since customers are more and more demanding, it will be hard for a company to survive in the competitive market if it fails to catch up with the trend. Given the life cycles of products are becoming shorter and customized goods are more personalized, companies are required to adjust their production chain on a timely basis so that it's possible to upgrade their products and optimize their productivity to cater to the needs. At the same time, the cost should be confined within a reasonable range, including the research cost, development cost, labor cost, maintenance cost, etc. To meet the requirements of Industry 4.0, smart factories need to be built, which are highly adaptable and able to utilize resources efficiently. These factories are expected to digitalize and intellectualize the main activities during production, including supply, manufacturing and sales. In this way, companies are allowed to adjust these sectors of the whole supply chain along with the market demand. However, the implementation of such factories demands solid technical foundation. One of the vital supporting technologies is the Cyber-Physical System (CPS). CPS is defined as complex systems which can integrate cyber and physical world (Baheti and Gill 2011). It makes a comprehensive use of so-called 3C (i.e. computing, communication and control) technologies, through which it is able to percept the status of physical systems in real time and control the system dynamically. In this manner, CPS makes the systems more reliable, flexible, integrated and efficient, which are vital characteristics of smart factories. Therefore, it can be forecasted that CPS should have an extremely widespread application prospect.

Since CPS is of great significance as stated above, it has caught attention of government, industries and scholars in some major countries. The American government listed CPS as one of the most important research projects when they released American Competitiveness Initiative in 2006. After that, they even rank CPS as the top one in eight key information technologies in 2007. They pointed out CPS would change the method how we interact with the physical system. Germany is the first country to put forward the term of Industry 4.0. German government invested a capital of €200 million to promote the intelligent level of manufacturing industry. Analogously, they also put a high premium on the implementation of CPS, as this technology occupies a foundation position to actualize Industry 4.0. Meanwhile, China also attached great importance to transition to an industrial power. In May 2015, the State Department of China issued Made in China 2025 plan that explicitly identify 9 missions and 8 strategic supports. The government pinpointed that only deep amalgamation of informatization and industrialization could well lead the development of manufacturing industry. Moreover, CPS is a momentous thrust for the realization of informatization, since CPS is able to interconvert physical quantity, analog quantity and digital quantity.

In addition to the attention coming from government circles, CPS has also received additional consideration of enterprises. In Germany, the Leipzig factory of BMW achieved the automation rate of 95% in its vehicle body shop. To cope with the challenges brought by electric vehicles, BMW also introduced CPS and kept improving it to facilitate a predictable computation and communication. It founded a consortium for recommendations to implement Ethernet for their automotive applications (Lukasiewycz et al. 2012). Siemens also has a famous factory named Amberg factory, in which the physical and the virtual one are operating synchronously. About 300 million components produced there all have their own identity card to record their information, including the corresponding production line, the materials used, the appropriate screws, etc. Workers are able to supervise the operation conditions of physical factory that are presented by the virtual one, and further control the physical one by CPS accordingly.

Many scholars also began to touch on this topic. However, most of them only had an idea about the potential significance of smart manufacturing, but did not put forward a practical and general approach to apply CPS to build a smart manufacturing system. The problems such as Information Island have not caught up enough attention as well. Some of them might give some trial method to implement CPS to practice, but they usually paid attention to only some techniques, and failed to analyze this trend from the angle of business, such as the new business model. For instance, Davis, et al. talked about the huge impact of global market on the manufacturing industry (Davis et al. 2012). The importance of innovation and customer demand is also stressed. What's more, they also proposed a platform called SM to realize the virtual smart manufacturing. However, they have not inquired into the method to connect the physical factory with the cloud in practice. Neither have they analyzed the significance of the cloud to integrate the whole company or integrate the company with other external parties. Thomas et al. only gave a definition of smart process manufacturing briefly touched its driving force for the development of chemical industry in the 21st century (Edgar and Davis 2008). Nevertheless, they have not explored a practical way to realize this framework and pointed out the key technologies needed. Xu discussed the essential features of cloud computing and cloud manufacturing in his paper (Xu 2012). In addition, he also took notice of the important role of the cloud service for the customers to participate all stages of a product life cycle. However, he mainly focuses on the interaction between the company and the customer via the cloud, yet he ignores the internal operation within the factory. Thus, the approach to achieve internal integration and to improve the overall production performance has not been suggested. Zhekun et al. highlighted the role of RFID in the internet manufacturing field and reviewed the development of RFID technology (Zhekun et al. 2004). An application example is also given to better indicate the importance of RFID. However, it merely focused on this technology, but did not explore the adoption of other technologies in smart manufacturing system. Lucke et al. mainly presented a manufacturing environment that is sensitive to the context (Lucke et al. 2008a). The application of state-of-the-art computing technologies was also highlighted, but they did not touch the procedures to apply those technologies into practice. In addition, they merely concentrated on the operation mode within a factory, instead of talking about the operation of the whole enterprise, not to mention the connection across different companies. Ghonaim et al. primarily proposed a model for building a smart automated manufacturing system (Ghonaim et al. 2011), which is flexible, totally visible and intelligent. They focused mainly on the material/information flow along the supply chain by taking advantage of RFID. Whereas, they did not penetrate into the new generation of operation method within the manufacturing factory and the application of other technologies. Yang and Zhou came up with a CPS virtualization approach and even verified it by applying it to a real-world control system (Zhang et al. 2013). It is proved that their approach to apply CPS is able to well realize the synchronization between the cyber and physical components and capture those dynamic behaviors in the system. They only tried QEMU and Matlab/Simulink to apply CPS into practice, so their approach might be that general. What's more, since they mainly focused on the operation method of the smart factory with the help of CPS, they didn't pay much attention to describing this trend from the perspective of economics. The new business model and the following effect have not been discussed. Sridhar et al. highlighted an important potential risk that is cyber-attack (Sridhar et al. 2012). The possible attack vectors, the risk evaluation method, the current research efforts to enhance security and the challenges that companies have to face are all introduced. On the other hand, other aspects were not covered in this paper. Similarly, Lee et al. also paid attention to one aspect (Lee et al. 2015), i.e. the five-level architecture of CPS to realize the self-configuration of devices, but other issues were not talked about. Munir et al. studied on the potential challenges when dealing with the human-in-the-loop control in CPS (Munir et al. 2013). Nevertheless, the interconnection between the physical factory and the cloud was not discussed.

Since CPS was just raised clearly several years ago, the related models and methods are still not mature, although extensive attention has been paid to this topic. It's admitted many existing academic writings or enterprises are committed to connecting the physical world and virtual one. However, it can be seen that most of them are still studying on the method based on the basis of traditional manufacturing industry. Sequential engineering was always preferred, which was influenced by Theory of the Division of Labor by Adam Smith. Every department only focused on their own tasks and available information. They carried out their jobs after their upper link fulfilled their tasks and passed them on. Every department has few ideas about the operation of other sections and no global view over the whole process. Thus, there is a lack of information sharing and every section stands as an Information Island. Hence, this paper focuses on the approach to implementing CPS while mitigating the problem of Information Island.

In the face of this situation, this chapter was bent to the decentralized cyber-physical systems, which enables manufacturing companies to make use of a cloud-based agent approach to create an intelligent collaborative context for production. Section 1 presents the background of this study. Section 2 discusses the idea of Industry 4.0 and smart factories. Section 3 proposes the concept of decentralized CPS agents and discuss it from the perspective of conceptual model, operation mechanism and key technologies. After that, Sect. 4 presents a paradigm for cloud-based smart manufacturing, to better illustrate the concepts. An application case in China is introduced to show how a manufacturing company adopted the proposed the paradigm to build a smart factory of Industry 4.0 in Sect. 5. Conclusion is summarized in Sect. 6.

2 Smart Factory of Industry 4.0

This section extends the terms of Industry 4.0 and smart factories by articulating Structure Behavior Function (SBF) Models to give insight into their stable components, changes over time and their effects on its environment (Song 2009). The background to introduce these notions will also be covered. Especially, the conditions in China will be discussed in more detail to stand as examples.

2.1 Industry 4.0

2.1.1 Background of Industry 4.0

Industry 4.0 is a concept that was put forward to adapt to external conditions and internal needs. The external conditions can be analyzed using PEST Analysis, from political, economic, social and technological perspectives. The internal aspects could include two aspects, which are income and expenditure (Fig. 1).

The political background mainly consists of law of environmental protection, labor law, government policies, and industry regulations. First, politics is usually exerting great influence on corporate supervision, production and many other related operation behaviors. Especially, the political institutions, systems, policies, laws and regulations always have profound effect on the long-term investment plans. Recently, international community has paid strong attention to the environment protection and reached many conventions, such as Montreal Protocol on Substances. That Deplete the Ozone Layer and United Nations Framework Convention on Climate Change. At home, the Environmental Protection Law of the

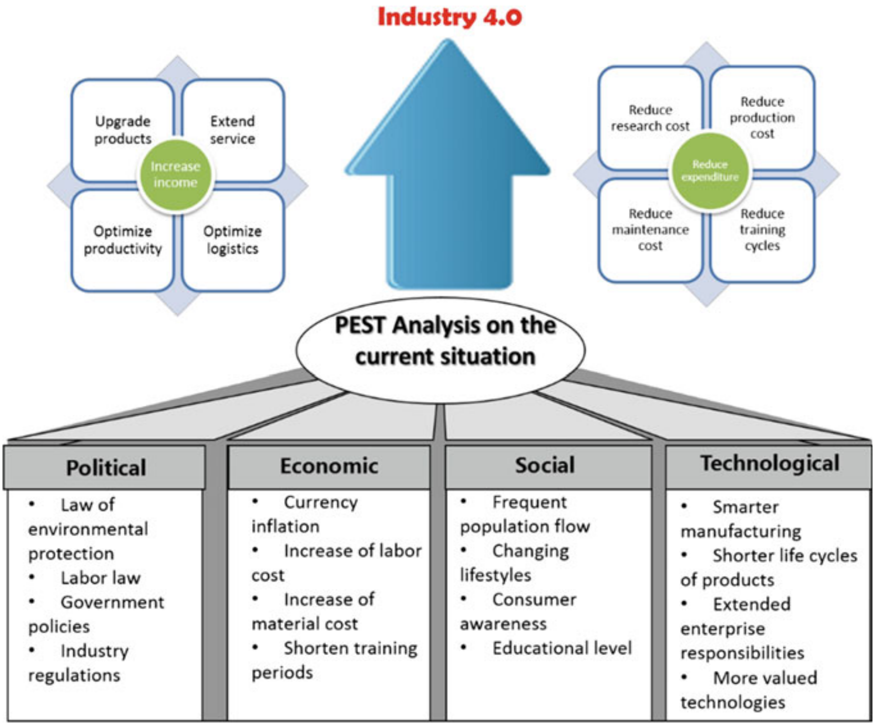


Fig. 1 External and internal needs for Industry 4.0

People's Republic of China was launched in 2015. Hence, the development of some manufacturing companies with high energy consumption and heavy pollution is limited. The labor law is also increasingly improved so that the rights and interests are better protected. In contrast, the operation costs of companies are further lifted. A total of 19 regions in China adjusted the minimum wages in 2014 and the average increase rate was 14.1% (Xinhuanet 2016). In 2015, 6 provincial level administrative regions including Peking and Hunan announced to increase their standards of lowest wages. The legal minimum pay is ¥2190 in Shanghai and the annual increase rate is 13% on average in the past 6 years. In addition, the maximum working hour is also constrained legally. For example, the daily working time is limited in 8 h, generally speaking. It can be easily seen those laws raised the production cost and also has some effect on the productivity. The increase in basic salary and the provision on staff welfare system both improved the labor cost of companies. Then the yield will also be lower if the working hour is 8 h compared to longer time. However, the land rent, the depreciation cost of devices or other fixed costs will not change along with number of products. As the consequence, the average cost per unit will certainly become higher. Hence, the companies have to seek new methods to cut down the redundant workers of low skills and prolong the efficient operation time of the factories. Furthermore, the government is also advocating developing manufacturing industry of new patterns. In 2014, the Prime Minister of China, Li Keqiang signed and issued The Action Outline of Sino German cooperation with the Prime Minister of Germany. This outline emphasized the value of Industry 4.0 to economic development of both countries. It also stated both governments would provide policy support to equitable and mutually beneficial communication and cooperation between the enterprises of two countries. Last but not least, the industry regulations are more and more strict. For instance, it's now required all products be subject to strict quality checks. Customization is also much more prevalent and popular. All of those policies or regulations impel companies continuously to cast about for better operation mode targeting more satisfactory performance.

Economic factors also play a very important role when deciding the development tactics of companies. First, currency inflation forces the purchasing power to go down and the market to depress. As a result, the throughput will be negatively impacted. Then, the labor cost has also been increased these years. Companies are required to provide more welfare benefits to its employees, which incurs higher labor cost, including wages, social insurance expenses, employee education funds, labor protection cost, employee housing cost and other labor cost. Thus, the cost of production is forced to increase so that companies will prefer to put machines into services to substitute for some employees. In addition to labor cost, there is also an increase in material cost, since the prices of many raw materials are rising. Furthermore, it's desired that the training periods should be shortened so that the employees are able to give a help in production quickly. However, it's hard for workers to grasp the operation methods and essentials in a short time. In contrast, it's possible for devices to be put into work at once as long as the programs are set up. It goes without saying that machines can be re-configured quickly to accommodate different production modes. Considering these reasons, companies are inclined to improve the degree of automation so as to save costs and improve the production efficiency.

The social cultures usually exert different influence on enterprises. The social-cultural elements could include social morality, cultural morality, cultural tradition, the trend of population change, education level, social values, the structure of society, etc. Here 4 points will be talked about, which are population liquidity, changing lifestyles, educational level as well as consumer awareness. China is now in a period of rapid social development and frequent population floating. One common example is the daily flow such as the movement of commuters in metropolis. For another instance, irregular population flow is also much more frequent than before in pace with the increase of economic income and leisure time. More people are going to travel for shopping, entertainment, commerce or vocation. Both the distance and the frequency are increasing by leaps and bounds. The population flow will make a difference on the social stratification. It somehow decides the population size, the possessions of wealth and the taste within each consumer classes. Since the population flow is now frequent, those characteristics of social stratum are changing frequently. Thus, it's hard for manufacturing companies to survive to produce exactly the same products from start to finish. They have to be flexible and adaptable to adjust their product mix to cater the fast-changing customer taste. They also need to keep reviewing the size of their target market, the purchasing power and the price-sensitivity of new customers. In addition to population flow, the changing lifestyles and consumer awareness play a vital role in consumer behavior. The changing lifestyle mainly refers to new social trend and fashion. People now are usually exposed to an open, free and pluralistic society so that they are becoming more demanding. Besides fulfilling their physical needs, they have a stronger demand for aesthetic, social intercourse, acquisition of knowledge, etc. This is a major challenge that companies have to face as well. The consumer awareness will also have some influence on the company mission and strategies. Nowadays, customers prefer to stand on the leading edge of trends and keep trying new generations of products. The life cycles of products are becoming shorter and shorter, especially some electronic products and luxury goods. The prices of those items will fall down dramatically as soon as they are out of date. Moreover, customized products are more welcome rather than identical line products. In face of these requirements of customers, companies are not allowed to rest on their laurels and are forced to press ahead with major changes. Last but not least, people are better educated nowadays, no matter the customers or the employees. Customers with higher educational attainment will be more demanding as discussed above. As for employees who receive better education, they demand higher wages and more challenging work. Thus, in order to ensure the maximal usage of education human resource, manufacturing companies cannot win the competition by relying on cheap labor of large scale as before. They have to utilize some machines to replace workers of low skills and recruit or cultivate more top-level talents.

The last external reasons to talk about are technological factors. Technologies are the driving force of enterprise development. Firstly, smart manufacturing is strongly backed by the government, which can be seen from the Conventions or presentation of the leaders. Secondly, as the technology advances at a breathless pace, many products are driven out of existence at a fast speed. The intense market competition causes product development to diversification, small batch, and short life cycle trend. Thirdly, with the social development, people have higher expectations and stricter demands on enterprises. Companies are supposed to show solicitude for environment protection or sustainable development and shoulder the responsibilities to the society. In view of all of these, companies have to upgrade their systems so as to strengthen their positions. Then a large number of valued technologies emerge at the historic moment. These technologies make it possible for companies to effectively grasp ideas about their clients, such as acquiring and analyzing the market data by taking advantage of automatic data bases. Technologies also enable factories to build a more adaptive and efficient production system with more intelligent machines comes into service. On the other hand, companies which are out of touch with reality and have blind confidence might be washed out by the market.

The reform is also needed from within. One is to broaden sources of income; the other is to reduce expenditure. In order to increase the income, companies are supposed to devote their energies to bring products in front of more people while keeping regular customers. Four practical ways are suggested here. The first is to upgrade the products continuously to meet customer demand. The second is to extern service ranges. In addition to perfecting quality of service in purchase process, sellers ought to render pre-sale and after-sale service as well, such as strict management, complete quality management, offering comprehensive instructions and guarantee of repair. The third advice is to make great efforts to optimize the productivity. Given the same cost in time and money, the net profit is likely to be higher with higher yields. The last suggestion here is to optimize the logistics. It's important to note that a need for revers logistics is generated since companies now usually recall new forms of reusable packaging, recycle household electric appliances, questionable vehicles or mild powder, etc. Reverse logistics is a very challenging job.

Similarly, four ways are listed to reduce the expenditure of companies. The first is to reduce research cost. This requires that companies have a deep understanding towards the market needs, define clear product orientations, reasonably coordinate the available resources and establish knowledge experience bases. The second is to cut some production cost. To achieve this target, companies are suggested to optimize the production process and reduce the loss in production. Furthermore, production cost could be saved by adopting new technologies or energy-saving facilities. The third cost to be saved can be the maintenance cost. In the past, workers keep machines running well by enhancing routine checking and maintenance. Assuming the facilities are able to realize self-adjustment or self-configuration and even to predict their own status, the maintenance could be easy and cost-saving. The last one is to shorten training cycles. One solution is to build a sound cloud to store all the materials needed, including the training courses, model libraries, operation guidelines, etc. In this manner, new hire are able to update their knowledge by making use of this cloud. All of the four items mentioned above demand a more advanced and better collaborative system.

Taking into account all the analysis above, it can be known that there is an urgent need for industry reform. On the basis, the study on Industry 4.0 rises in response to the proper time and conditions.

2.1.2 Introduction of Industry 4.0

This subsection serves as a simple introduction to Industry 4.0. The connotation of Industry 4.0 is to set up a new production mode, which is highly flexible and digitized. Instead of just providing products to customers in a one-time sale like before, new generations of manufactures will also continuously render services to their clients. Industry 4.0 is regarded as the fourth industrial revolution which is primarily led by smart manufacturing. It is aimed at making the most of Cyber-Physical System (CPS) to transform manufacturing industry to a more intelligent mode, while CPS is a multidimensional complex system which integrate

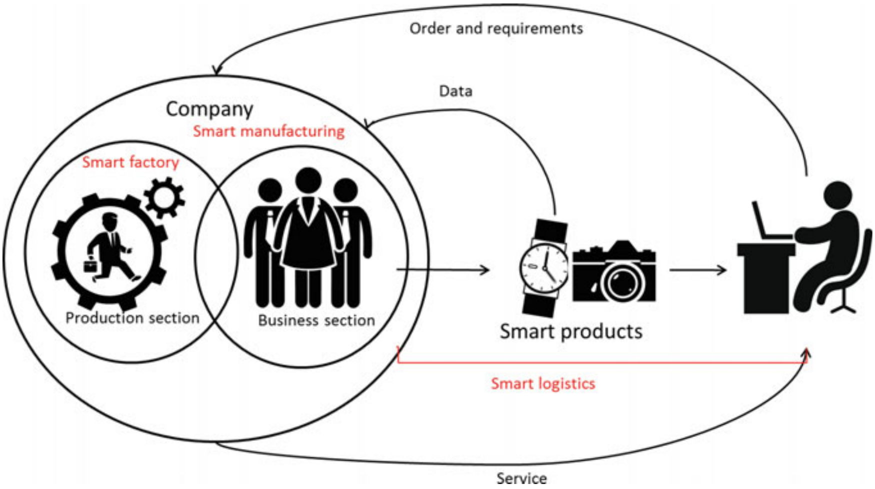


Fig. 2 Concept model of Industry 4.0

computing, networking and physical environments. Figure 2 shows the concept of Industry 4.0.

Industry 4.0 has three major themes, which are smart factory, smart production and smart logistics. The theme of smart factory mainly study intelligent production system and process. The realization of the design of networked distributed production system is also within the scope of this topic. The focus of smart manufacturing is the activities of the whole manufacturing enterprise. It covers the management on production across different departments, man-machine interaction and the application of 3D technologies in the production process. Smart logistics refers to integrate logistics resources via internet, internet of things and logistics network so that available resources are made full use of. The clients are allowed to have quick access to the services they want with the support of smart logistics.

The management on the whole enterprise belongs to the scope of smart manufacturing. The whole enterprise mainly consists of two sections, of which one is production sectors and the other is business segment. In the present companies, production sectors manage themselves with the help of Manufacturing Execution System (MES) and business segments manage themselves using Enterprise Resource Planning (ERP). MES assists the production sector to manage their manufacturing data, planning, scheduling, inventory, quality, Kanban project, data analysis integration, etc. Contrastively, ERP covers supply chain management, sales and marketing, customer service, accounting, human resource, business information system, finance and investment management and so on. At present, many large enterprises are harnessing MES and ERP. As the consequence, collaboration has been well redeemed within departments. However, the two sectors are not communicating well. For example, when there is something wrong in the production process, such as the breakdown of devices or low-quality raw materials, MES will adjust the production plan according to the facts of the situation in the plant. However, the ERP is not able to receive the messages in real time, as a result of which, it will execute orders following the original plans. If this persists, serious deviation between the business sections and production sections will occur. This problem will be settled in Industry 4.0. The whole enterprise shares a cloud which stores all the information all qualified employees have access to it. A cyber system corresponds to the physical world so that employees are able to learn about the actual conditions presented by the cyber company and even control the actual activities by changing the parameters of cyber system. Furthermore, there are no obstacles of the communication between machines and people. Then, the information sharing and collaboration are realized through the whole company.

The management on the production section is so-called smart factory. As soon as receiving the orders from the business sector, the factories will start production. Smart materials and devices are adopted here. Work in Process (WIP) go through highly automated production lines to become end products. Workers observe the operation of the physical factory by checking the status of corresponding cyber system, since models of all the devices, WIP, materials are built and the cyber system can exactly simulate the operation of the actual system. Some critical technologies are needed, including simulation, cloud computing, big data, virtualization security, RFID and so on. Because this chapter mainly focuses on the application of CPS in smart factories, this topic will be discussed specifically later in Sect. 2.2.

Smart logistics refer to the flow of information and materials between suppliers and companies and between companies and clients. The latter is our focal point here. When a customer places an order to the company, the demand will be recorded and stored in the cloud of the company. Both the business sector and production sector will be informed of the related information. The business sector will handle the relative financial affairs and the factory will produce the products for the customers. All the information of the ordered product will be stored in a tag on the product and RFID is used to read it. The customer needs, the production status, the present location and the maintenance needs are all included in the information to be stored. With the help of smart logistics, the smart products will reach the customers within a short time window and will exactly conform to the personal requirements of them.

What's more, even after the products have been owned by customers, the sensors within products will continuously act as information collectors to collect the information of products and customers, if is allowed by the customer. The information will be uploaded back to the cloud of the companies so that they have access to the status of sold products or customers and they will render services when appropriate. For example, when the sensor detected something abnormal or failure with the products, the responsible employees will immediately get all relevant circumstances and send engineers to solve the problem. For another example, a company that produces smart watches will monitor the health conditions of users in real time. The health parameters will be collected by the smart watches and uploaded to the clouds. When there is health disorder of the users, the company will become aware of it even before the users themselves. Then the company will dispatch experts or help inform the doctors to diagnose the users. Thus, in the era of times, manufacturers will transform to the combination of products and service providers.

2.2 *Smart Factory of Industry 4.0*

The smart factory is a factory that intelligently helps people and facilities to carry out the tasks. Such factory is able to take context information into account, such as the status of an object (Lucke et al. 2008b). Before penetrating into smart factories of Industry 4.0, the common form and drawbacks of the present manufacturing factories will be given.

2.2.1 Present Manufacturing Industry

In present manufacturing industries, serious engineer is usually employed. The entire R&D, manufacturing and marketing process is subdivided into many steps. Every department is only in charge of a small part independently. After a department finishes its task, it will hand over to the next department. To illustrate better, Fig. 3 is shown below.

The whole process is as shown in the illustration, from the time when customers place an order until the time when customers receive the product. A customer first places an order with the company and the business department will receive the request for products. Then they are responsible to entry all the detailed information about the order, including checking credit, typing requirements on the product, checking the stock, preparing an invoice, etc. In line with these details, a production plan will be made by business department and sent out to production department and procurement department. Procurement department answers for purchasing all the raw materials needed and give support to subsequent production step. The production department will also receive the production plan and asks each unit of it to prepare for the production. Workers who are in charge of preparing raw materials will receive them from the procurement department as well as make sure the quantity and quality of the materials reach the specifications. Workers who are controlling the machines will check the status of equipment and maintain or adjust them if needed. New technologies will be introduced also if the current technologies cannot satisfy the production requirement or market demand. After everything is ready, production is started formally. Materials, facilities and technologies which are prepared early are magnitude guarantees for producing the products of high quality in a reasonable time window. To further ensure the quality is up to standard, the quality management department will assign supervisors to monitor the production process. When the end product is finished, the logistics department will take over the duties. Its people will retrieve the product first and then pack it for

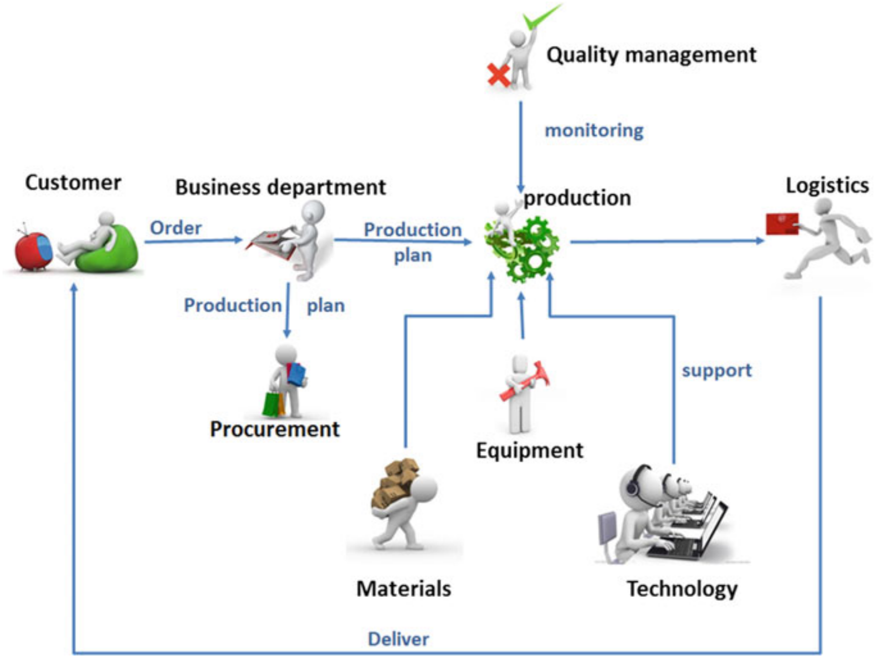


Fig. 3 Current operation modes of manufacturing companies

shipment. They will decide the delivery schedule, select appropriate transportation mode and route, and prepare the shipping document. After a certain period of time, the client will receive the products.

It can be seen the whole process is completed step by step. Various departments presides over diverse jobs and the sequence of accomplishment is unidirectional. Both the information and materials are flowing in one direction. All information resources are broken up into pieces. Every department gets one piece and stands isolated from each other. Hence, the most fateful problem is Information Island, as shown in Fig. 4 Since the whole process is an open loop, the phenomena of information asymmetry and information fragmentation occur within the factory. Downstream sectors get instructions from the upstream departments and they won't communicate any longer. One department has no access to the alterations made by another department, but the change will have an influence on all departments in fact. For example, some machines are out of order in production department so that the workers have no alternative but to take the second best devices to complete the job. As the result, the processing time will be longer and more materials will be consumed. However, only the production department knows the rope, but the business department and logistics department have no idea about it. Thus, the business department will complete the financial reports according to the original plan, in which many datas will deviate from the actual ones. Similarly, the logistics department will make the delivery schedule and contact the customers as planned,

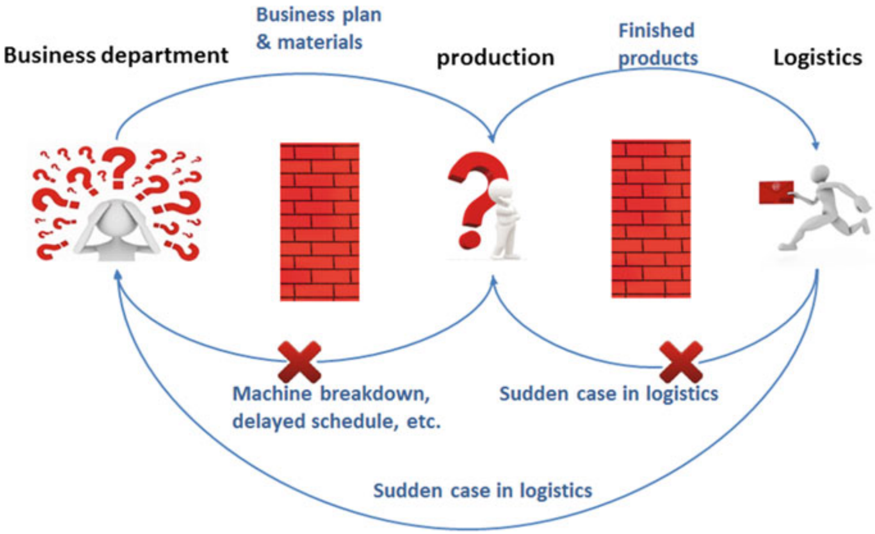


Fig. 4 The problem of Information Island

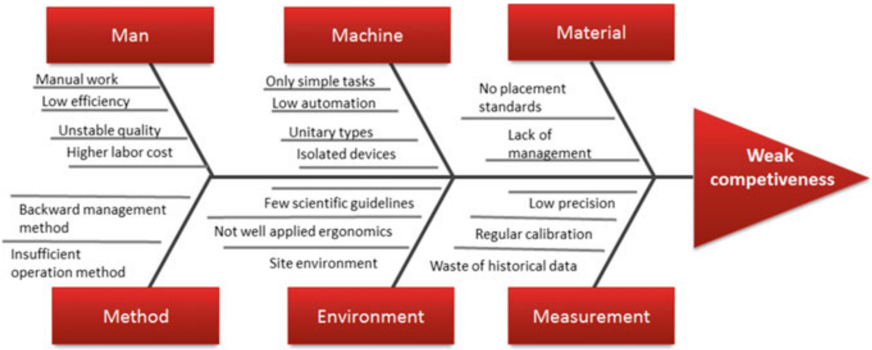


Fig. 5 Drawbacks of current manufacturing companies

but they are unable to deliver the order within time window at last. The occurrence of such a situation will lead to a loss of both companies and customers, which is something that people do not want.

In addition to Information Island, there are also many other problems with current manufacturing factories, as shown in Fig. 5.

These drawbacks will be discussed from six aspects and shown in the Fishbone diagram. (1) Man: in today's manufacturing companies, many processing operations are completed by manual work. However, the efficiency is well below the throughput of machines. Besides, the quality is unstable and hard to control, since the man is subject to various interferences usually, such as emotions, fatigue, stress and temperature. What's more, as the government launched updated labor laws and people have higher life pursuit, the labor cost is higher and higher these days. The companies based on cheap labor force have to find out the new development model. (2) Machine: currently, many machines are designed in a straightforward way and are only able to carry on simple tasks. The degree of automation is low and the type of machines is unitary. What's worse, the devices within the same plant are not connected to each other. Instead, they solely do their own processing but are not well collaborative. (3) Materials: there are no standards for materials placement in many factories. Very often, the raw materials or tools are placed aside very freely. This habit leads to excessive stock of unnecessary materials and a waste in time to find the one needed (Wang et al. 2013). (4) Methods: the 15 present management approach and operation method do not match with the market demands. Companies now are short of management on data and there is no systematic management on materials. Some operation modes such as assembly methods of low efficiency are not able to fulfill the needs of market. (5) Environment: there are few scientific guidelines to tell the influence of plant environment on devices or workers in Chinese factories. Ergonomics have not been well applied into practice. In many production sites, the temperature, humidity, illumination, sound intensity and cleanliness are not well controlled and determined since they don't have a clear mind about the impact of these environmental factors on workers' affective status and machines' operation. There is not enough stress on the management of the site environment. For example, few companies in China learn experience from 6S management method of Japan. (6) Measurement: the available devices, technologies and operant level are not enough to achieve high precision in measurement. Workers are required to calibrate the devices regularly, since the devices are not able to do self-checking and self-adjustment in real time. In addition, the historical data has not been made best of and acted as the reference for measurements, which wastes these data sources to some extent.

With a view to all the above shortcoming of the factories today, scholars and enterprises started to explore a new generation of manufacturing mode. Hence, the concept of smart factories is proposed to solve the problem of Information Island as well as get rid of other drawbacks as stated above.

2.2.2 Introduction to Smart Factories

In a smart factory, CPS is the major technical support. There are two sets of systems that are operating simultaneously. One is the physical factory and the other is a virtual one. All of the devices, materials, WIP, products, people and operation process have virtual counterparts in the virtual factory. This is basically realized through real-time simulation. Any processes are shown in the virtual factory, which can be observed by the eligible engineers. On the other hand, any change that engineers make on the virtual factory will be implemented in the actual factory automatically. This section will only basically introduce the components and functions of smart factories. The approach describing how to build such a smart

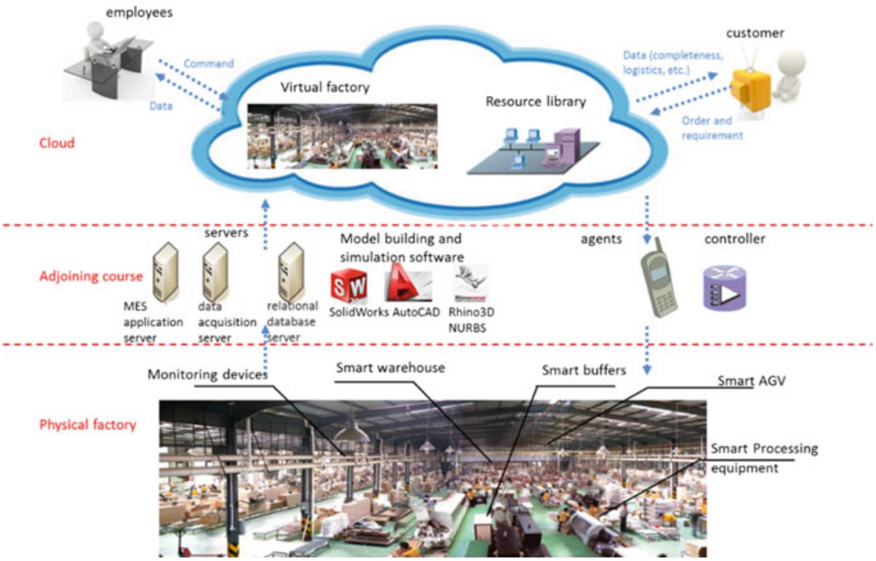


Fig. 6 Architecture of smart factories

factory will be talked about later in Sect. 4.1. A better insight over smart factories is shown in Fig. 6.

Physical Factory

As shown in Fig. 6, there is a physical factory operating in the whole system. In a smart physical factory of Industry 4.0, all of the materials, devices and process are intelligent. There are smart AGV, warehouses, processing equipment, buffers and monitoring device.

(1) Smart AGV: In the present factories, the main functions of the Automated Guided Vehicle (AGV) are to move automatically along the prescribed path. However, the starting point, end point and the route have to be laid down by people in advance. In smart factories, AGV will more much more intelligent. They will receive the instructions from the cloud and calculate the optimal path to complete the task. Positioning devices are installed on the AGV so that the location and status of AGV can be tracked and corrected. Automatically, the AGV will operate among smart warehouses, processing devices and buffers.

(2) Warehouse: There are stereoscopic warehouses of various forms and for various purposes. The temperatures and humidity are intelligently controlled to keep the stock in good state. For example, the processed foods like canned chicken will be stored in their specialized warehouses, which will regulate the temperature to a relatively low degree and monitor the quality of those foods in

real time. Smart warehouses hold inventory that is used to buffer the variation between production schedules and demand. They are able to automatically accumulate and consolidate products from various points of manufacture within the firm. By sensible planning of the stocks, the travel times of AGV for order receipt and order picking are minimized.

(3) Processing equipment: Robots are put into use in the large scale, which can substantially increase the stability of products. Given the quality of products are better guaranteed, the after-sale issue will decline also. What's more, in smart factory, these processing devices are managed according to scientific standards, which can further improve the overall efficiency within the whole factory. Distributed Numerical Control (DNC) machines are appropriately applied to combine the machining tools and computers. They allocate processing tasks to machines dynamically so that the utilization rate is raised. The rate of output over cost will be higher, since the idle time of machines are relatively shorter.

(4) Buffers: Smart buffers are well set between adjacent processing devices. It is used to temporarily store the WIP when there is a difference between processing speeds of the two devices. Smart buffers are able to check the working condition of the next device and send out the WIP when appropriate.

(5) Monitoring devices: The all-around monitoring devices are able to realize the comprehensive monitoring and recording. They are utilized to guarantee the safety of production site and trace back to the past time in case any site failure occurs.

(6) Smart logistics: With the collaboration of all smart facilities, such as the buffers, processing devices, DNC, AGV and waiting platforms, the whole workshop logistics is digitalized and lean designed. The flow of raw materials, spare parts, WIP, waste, information and people are all well controlled. It can be predicted that the overall production efficiency will be improved dramatically in this way.

Adjoining Course

Between the physical factory and the virtual one, there is an adjoining course, of which simulation is a key method to connect them. It is noteworthy that this is a two-way interaction between the two factories.

The realization of interaction from physical factory to virtual factory is achieved as follows. The models of all devices and materials are built in this stage for the convenience of simulation. The available software for building models and simulation include Solid Works, UG, Tinker CAD, 3DSlash, etc. There is some difference between the current simulation and the new generation of simulation. The current simulation method is to build models and asks the virtual system to run so as to have a look at the possible results of this layout. While, in the simulation of smart factories, this is a kind of real-time simulation. In addition to modeling software, many servers are coming in handy. The servers consist of MES application server, data acquisition server, relational database server (RDBS) and real-time database server. They will help collect and analyze the data in physical factory operation and modify the virtual one in real time. Thus, the virtual factory is allowed to run almost simultaneously with the physical one.

The interaction from virtual factory to physical factory is realized in this way. Some agents and controllers are working to realize the functions to control the physical factory by modifying the virtual factory. The agents will detect and receive the signals sent from the virtual factory and quickly find the counterparts in the physical one. Then, instructions will be sent to the physical devices or materials and they will be adjusted accordingly with the help of controllers.

Cloud

There are two parts in the cloud, of which one is the virtual factory and the other is resource library. Virtual factory is the cyber world corresponding to the actual factory, as stated above. Hence, the resource library is highlighted here.

Resource library is pool that stores all the information of the factory, historical data, standard sizes, users' requirements, the failures and remedial measures included. These resources can provide great convenience to fulfill the orders and maintain the factory. For instance, when a virtual processing device is working on a virtual part, the parameters of the virtual device are exactly with its counterpart. Then, the virtual system will compare these parameters with the historical data in the resource library. Provided that there are any outlier data, the virtual system will quickly predict the potential problem and risk, after which remedial steps are taken at once. Moreover, there are many standard models stored in the resource library, which are ready to be invoked when needed. This kind of function will bring engineers great convenience.

This cloud is accessible to eligible employees within the company. Even customers have partial access to a tiny subset of the cloud. Employees observe the status of virtual factory and retrieve data from the cloud, while they could also input specified command into the cloud to control the factory indirectly and manage the resource library. The customers' order and detailed requirements are also recorded in the cloud. Since there is a tag on the materials all the time, the status of products can be checked and tracked any time. Hence, the customer is informed of the degree of completion and delivery performance of his or her ordered item. What's more, he or she can even have a connection with the cloud after the ownership has been transferred to him or her from the company.

To give a brief conclusion to this subsection, the smart factory consists of a physical factory and a cloud. They are connected by advanced technologies or devices such as real-time simulation and servers. The cloud consists of virtual factory and resource library, which is accessible to qualified users.

Effect

It can be seen from the above introduction that all devices have counterparts in the virtual factory and are connected with the cloud. Employees of different departments have access to the cloud so that they are informed of the order at the same time. Production department don't need to wait for the detailed information from the business sector. Similarly, the adjustment of plan made by the production department is transparent to business sector and logistics department. Therefore, diverse departments are connected by the cloud and numerous devices are joined together also. The problem of Information Island is resolved is smart factories.

Furthermore, the other drawbacks have also been tackled. (1) Man: smart devices take place of manual work to some extent so that the efficiency is improved and the quality is more stable. The labor cost is also saved. (2) Machine: instead of straightforward-designed machines, the devices are much more intelligent and well controlled via the cloud. They are able to carry out much more complex tasks and cooperate with each other more harmoniously. (3) Materials: the materials are management following the guidelines stored in the cloud, leading to a much cleaner and dapper working environment. (4) Methods: all of the information is managed well in the resource library. The operation modes are of a far higher degree of automation and intelligence, which results in a higher throughput to match the market demand. (5) Environment: the noise reducing devices are in motion. Other devices such as air-conditioners and air humidifiers are regulated according to the instructions coming from the cloud intelligently. The environmental factors such as temperature and humidity are kept at a suitable degree to make people comfortable and machines operating well. (6) Measurement: Because of the cloud, the historical data are taken full advantage of to ensure the devices are functioning well. Self-checking and self-adjustment are both realized so that there is no need for regular check by workers. The smart measuring instruments are of high precision and even are able to upload the measurement data to the cloud. See Fig. 7 for detail.

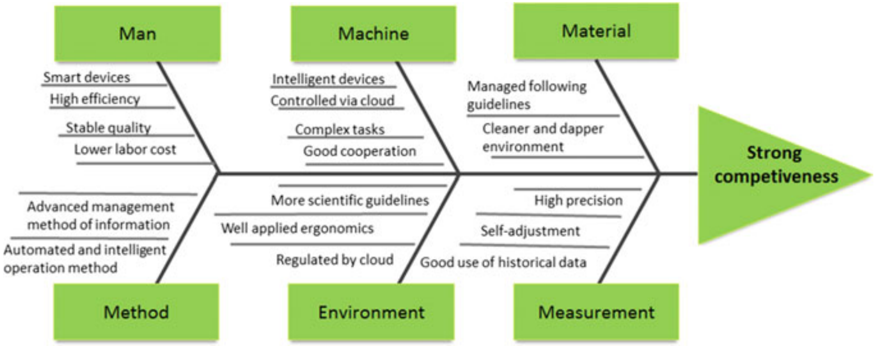


Fig. 7 Advantages of smart manufacturing companies

It can be seen the smart factories have overcome many obstacles in production. Section 2.2 only serves as an introduction to the concept model of smart factories and the idea of cloud.

3 Decentralized Cyber-Physical Systems Agents

In the above, we have talked about the concept model of smart factories and the idea of cloud to tackle the problem of Information System. However, to realize the connection among all the devices and people, there should be a kind of agent to link them to the cloud. Section 3 will discuss the conceptual model, operation mechanism and key technologies needed of the decentralized cyber-physical systems agents.

3.1 Conceptual Model

To find an appropriate conceptual model of the decentralized cyber-physical system agent, the function of it will be expounded first. Then, here comes a biological concept from which we borrow the idea to come up with agents. Last, the appearance and the user interface of the agent for people will be illustrated.

3.1.1 Functions of Agents

To better explain the function of the agent, the composition of the fictitious factory is introduced first, as indicated in Fig. 8. For convenience's sake, the physical factory is simplified here. There are two machines (Machine 1 and Machine 2). The machines can be normal processing machines, DNC, smart AGV, etc. Each machine is holing a workpiece, which are Part 1 and Part 2. Similarly, there are only two people (Person 1 and Person 2) shown here. They can be normal processing workman, assembly worker, supervisor, quality manager, dispatcher, finance officer or anyone else who may appear within the factory. There is an agent installed on each machine and within each workpiece. Each worker is also carrying an agent everywhere. What are the functions of these agents? They are used to connect numerous elements within the factory to the cloud so that the problem of Information Island could be resolved. How can the agents do it?

Firstly, the agent is capable of uploading the information or instructions of machines, work pieces and people to the cloud. The information of machines might be the operation condition, the degree of depreciation, the continuous operation time, the energy consumption, the degree of dexterity, the error of machining, wearing condition of tools and so on. The information of work piece to be uploaded chiefly embraces material sources, material properties, order time, customer

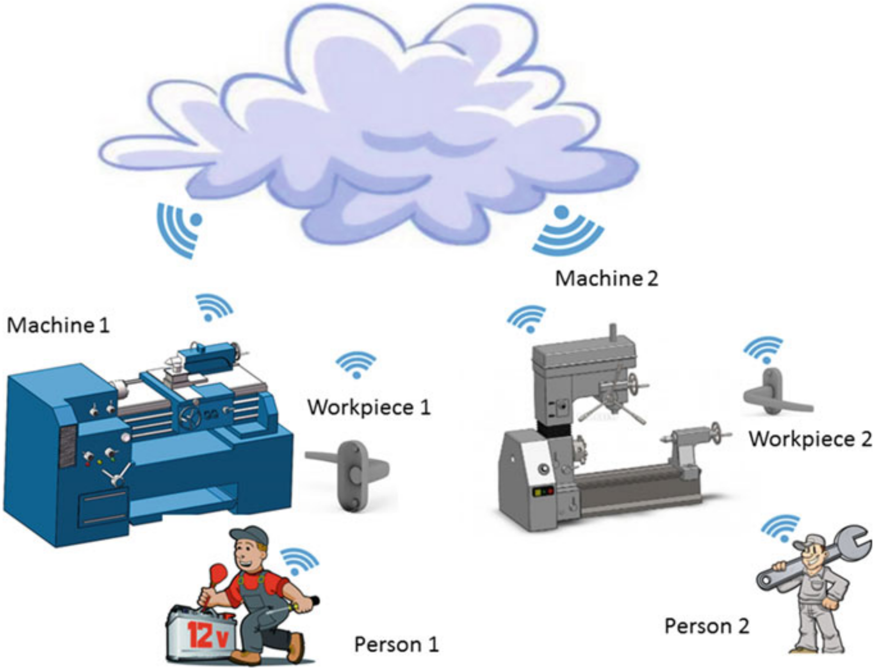


Fig. 8 Functions of agents

requirements, degree of completeness and location. The information or instructions coming from people basically consists of locations, working hours, mission reports such as inspection results and adjustment on the virtual factory in clouds.

Secondly, the agent is a medium for machines, people and work pieces to get information or instructions from the cloud. These kinds of information may be divided into six aspects that are 5 W and 1H: (1) What: Machine 1 may receive instructions telling what work piece it should process on next. Person 1 may receive instructions such as what machines he should check now. Workpiece may acquire the information such as what process it will pass through. (2) Where: this type of information is about the place. The machine 1 may get the dictation from the cloud via the agent to tell where it should send workpiece 1 to. Machine 2 or the warehouse? The workpiece may also acquire information about the route it will pass through. (3) When: this is telling all types of time. Agent can help convey the ideas such as the predicted completion time of a product and the time that workpiece 1 has to wait before departure for Machine 2. (4) Who: people can learn who is in charge of a particular machine or the subsequent step of the process. In this way, Person 1 is in a position to have an idea about Person 2, so they are not isolated from each other but integrated to some extent. (5) Why: this is to explain the reasons, which are particularly useful for people. Workers are given to understand why they have to carry out a specific task, why they need to follow a particular instruction and so on. Only when they are provided a good deal of insight into the essential reasons, can they further guarantee the smooth running of the overall production. Absorbing knowledge from the cloud with the help of agent is a good way for employees to enrich themselves and better serve the customers. (6) How: this is to talk about the ways and means. They are possibly the operating method for Machine 1, inspection method for Person 1, the transportation method for Machine 1 to send workpiece 1 to Machine 2.

It can be seen that the agent serves as a communication channel between the various components with the cloud. The agent can help upload their information and also acquire directives from the cloud. In this manner, people in every department are allowed to have an overall cognition of the factory operation conditions. The devices are also able to react to the ambient conditions. That means the problem of Information Island is tackled.

A small example is given here to better shown the effect of agent for decentralization, as shown in Fig. 9. There is a smart AGV carrying a workpiece. The agent will upload the status of the AGV to the cloud and after very fast computation, the cloud will instruct the AGV to move into the next station. According to the instruction, the AGV will send the workpiece to smart warehouse, or sent it to the appropriate machine. The availability or function of machine A and B will be judged by the servers in the cloud. Possibly, the AGV will send signals to Machine A and B directly to check the availability. What's more, since all parameters of the AGV will be uploaded to the cloud in real time, the computers will compare them to historical data all the time. If there are any abnormal data, the computers will check the similar situation in the past and predict the potential error

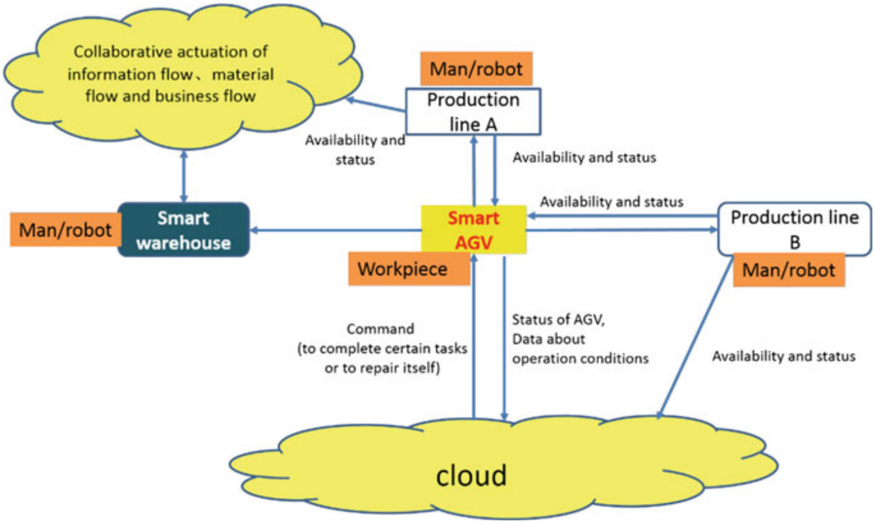


Fig. 9 Example of smart AGV to show functions of agents

with the help of probability distributions or simulation. Accordingly, precautionary measures or remedies will be taken automatically.

It is shown by this example that the agent plays an important role in CPS to realize the five main functions, which are computation, communication, exact control, remote collaboration and self-configuration.

3.1.2 The Biological Concept for Reference

This book chapter puts forward the idea of decentralized CPS agent, because it borrows the concept of synapses in biologics (See Fig. 10). In the living organisms, synapse is a biological part to connect two neurons or one neuron and one effector cell as well as convey information. The presynaptic cell will send neurotransmitters to convey information to the postsynaptic cell, which is called chemical synapse. Alternatively, the presynaptic cell may convey the information with the aid of electrical signals, which is known as electrical synapse. In accordance with the signals sent from the presynaptic cell, the postsynaptic cell will be excited or inhibited. The detailed effect can be complex (Eccles 2013). Hence, the synapse is able to connect two cells, convey information between them and exert some influence on the latter cell.

The CPS model borrows the idea of synapse to build the agent. Synapse is a part on the cell, while the agent is installed in the devices, work pieces or held by people. The synapse assists the cell to get information from the former cell and actuate the latter cell to respond accordingly. Similarly, the agent is able to help the devices to acquire information from the cloud or other devices and guide the device or people to react appropriately.

However, the functions of synapse and agent are not exactly the same. In the sight of the actual needs, the functions of the agent are expanded. To implement the connection and information transmission function of synapse, the two cells have to be in phase contact. On contrast, to connect with another device or the cloud, one

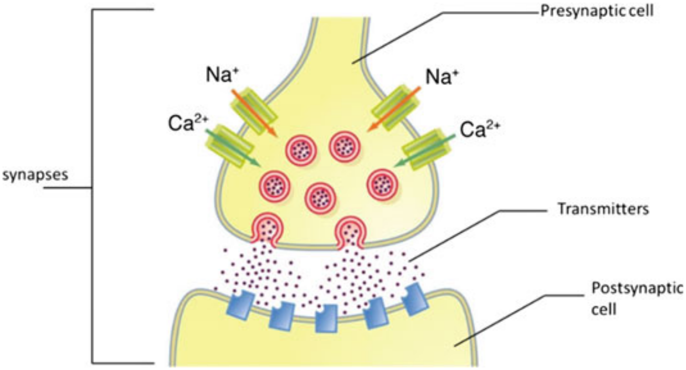


Fig. 10 Synapses concept for reference to propose the idea of agent

device doesn't need to contact them, since the information transmission medium is WIFI or some other wireless signals. The second difference is the directionality. The direction of information transmission is one-way between the two cells via synapse, but there is no such limitation on the agent in CPS. It is able to upload the information to the cloud, acquire the information from the cloud and even disseminate the information to all the devices nearby directly. According to the instructions given by the cloud, the devices will carry out the designated tasks.

To briefly summarize, the idea of the agent is borrowed from synapse, but the functions of agents are far more powerful.

3.1.3 Appearance and User Interface of Agents

The appearance interface of agents for devices or work pieces is not that important, since they only needed to handle the information internally. However, the appearance and interface of agents for people should be well devices, because people need to read it clearly so as to digest the information.

The agents should be compact in size so that it is portable. Currently, it can be a smart phone or a smart watch. In the future, a glove, a ring, an earphone, or a pair of smart glasses even act as the agent. The smart glasses in the future can even display the cyber factory or the information needed in front of the people virtually, similarly with the Google Glasses proposed these days (Paletta et al. 2013).

What's more, the interface design should be humanized and user-friendly. The rough sketch over the interface is shown as below (Fig. 11).

The main functions are displayed in the homepage. They are acquiring data, observing factory, issuing commands and viewing virtual factory. The icons standing for them should be beautiful and metaphorical, so that users can grasp the meaning of them as well as a pleasant user experience.

After clicking different icons, users are able to see their sub-functions. The icon of acquiring data is to help users to retrieve data of all types in the factory, including all historical data, the user data, the national profession standard, the parameter settings of devices, etc. The observing factory means to learn about the status of any element of the company. The element is probably a device, a WIP or a worker. Not only could the present condition be retrieved, but also the historical status and the changes could be tracked and reproduced. Thirdly, the issuing commands button enables employees to release decrees to the cloud or to the devices directly. This function allows remote manipulation that could help to improve the working efficiency. The last button of viewing virtual factory is help people to have an overall look at the whole factory. They can choose to observe the cyber factory which runs simultaneously with the physical factory. Alternatively, they can also comprehend the operating conditions by watch the surveillance videos recorded by all-around monitoring equipment.

This handy agent is quite functional and greatly facilitates people's work. All eligible employees of the company are accessible to the cloud via such an agent, including the people of production departments and other departments. Even some

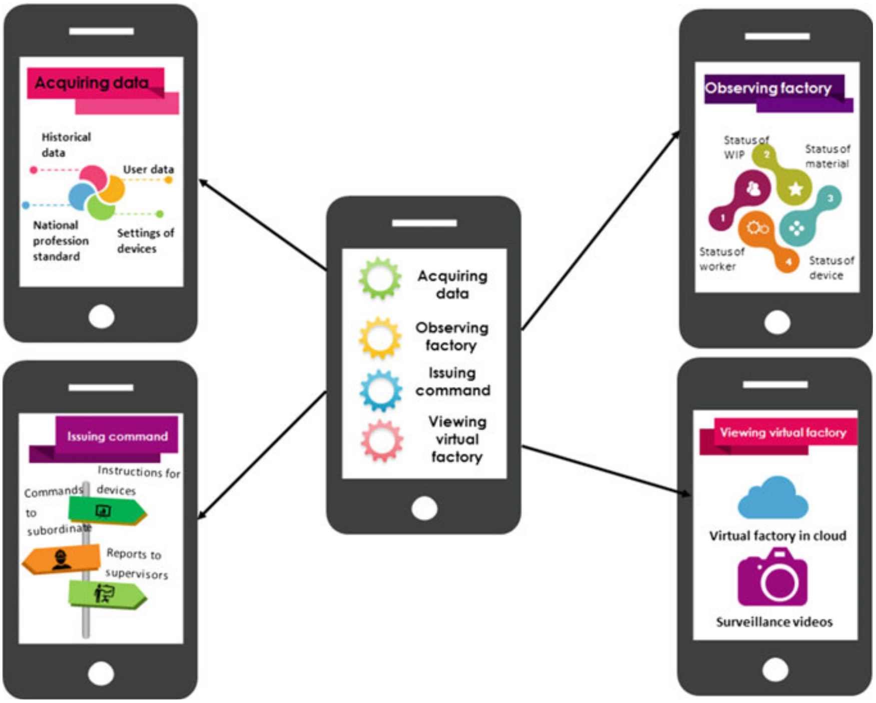


Fig. 11 User interface of the agents

organizations outside the company are allowed to hold such an agent, but only partial information can be obtained by them. For instance, the suppliers of the company may have an idea about the existing inventory of the company to decide a better delivery time. The customers are allowed to learn about the current location and status of their ordered items.

3.2 Operation Mechanism

In Sect. 3.1, the conceptual model of decentralized CPS agent is introduced, which consists of functionalities, the idea source, the appearance and user interface of the agents. However, the above section does not tell how the agent is able to realize those functions to bring convenience to people. Hence, this section will mainly stress the operation mechanism of the agent. An internal view of cloud and agent is shown in Fig. 12 to clearly interpret the operation mechanism.

The cloud is a vital part in CPS and it works with organic integration of computing, communication and controlling. First, there are many computers and servers equipped with high-end technologies. Their speed of computation and information

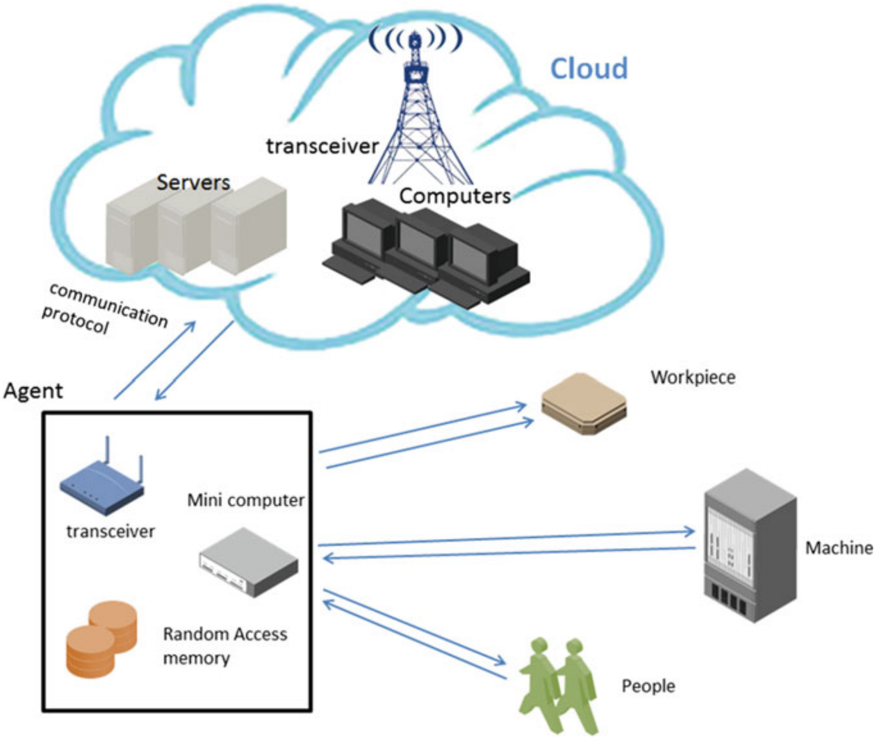


Fig. 12 Operation mechanism of agents

retrieval, the storage capabilities, and the speed of data handling is far beyond those of current computers. They are set to help computation, checking historical data, searching for solutions and generating instructions. These computers play a stronger role with the application of advanced management approaches such as ERP, MES, etc. There is also a beacon with antennas to send and receive signals. It is able to receive the signals sent by the agents of users, devices or work pieces. In return, it will also convey information to them through the signals. This can be achieved by WIFI or other similar methods. These sent information is generated from the computers.

The agent mainly consists of a signal receiver to receive signals, a transmitter to send out signals, a microcomputer. The microcomputer is used to do some computation work and store some relative data. The microcomputer in the agent for devices or people is more complex, since it will handle some demands and deal with multiple types of information. The people will read the information or demand directly, and then follow the directions to complete their task. The machines will have a controller corresponding to the agent. The controllers will control the machine to carry on specified tasks transmitted by the agent. On the other hand, the microcomputer in the agent for workpiece or the end product has a lower requirement for the computation function. What's important is the storage capability of a certain degree, because it needs to hold some information about this work piece. Hence, these microcomputers can be a combination of a simple processor and a chip to store the memory.

The most challenge now is to find a communication protocol. This should be applicable to all the things within CPS, including the computers and processing devices. It is like looking for a common type of neural signals which is applicable to all types of cells and setting standard regulations for their activities. Only when such a communication protocol is settled, can the speed, security, accuracy and reliability of communication be guaranteed.

3.3 Key Technologies

To make the agent working as stated above, the support of state-of-art technologies is needed. Some key technologies are listed here (Fig. 13).

(1) Computer technology: the biggest challenge is to compress the volume of the microcomputer while keeping complete functions, since it needs to be installed within the agent. While the agent has to be fixed onto devices or even work piece. Given it is too large, it might bring negative impact on user experience, especially when it is installed in the product.

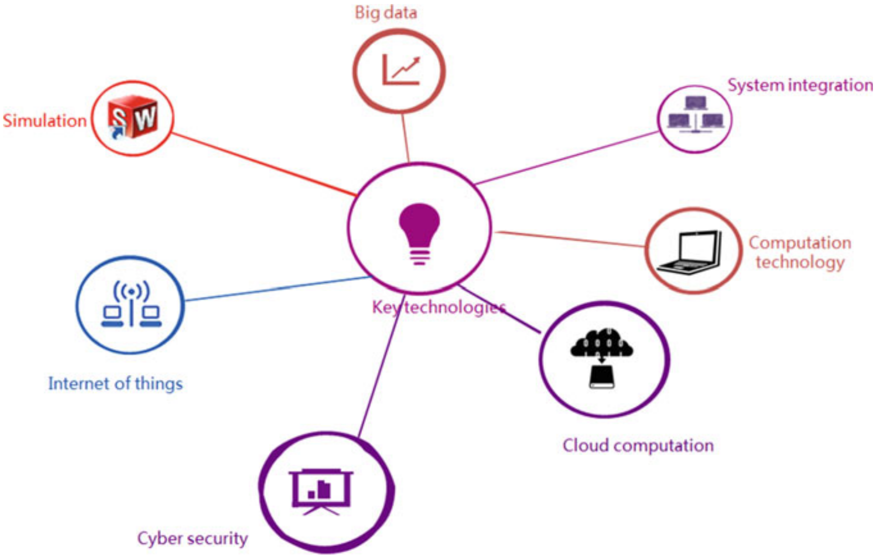


Fig. 13 Key technologies to support agents

(2) Simulation: In addition to building models of all devices and simulate their operation process in the virtual factory, the technology should be able to synchronize the virtual factory almost in real time through simulation. The key points of simulation are the reproducibility, precision and validity.

(3) System integration: the agent acts as a bridge between the components of the factory and the cloud. In addition, it can also assist the communication between two devices or between a device and a person. Thus, it plays a role in system integration for ease of concentrated, efficient and convenient management. It is not enough to only put the agent into use. This application has to be combined with structured cabling system and computer network technologies.

(4) Internet of things (IoT): it is a set of networks in which each object is connected. This technology is able to create an environment in which the agent can work normally. IoT is t connect all the things with the internet with the help of RFID, infrared sensors, laser scanners and other information sensing device. This is a kind of Internet to realize smart identification, tracking and positioning, monitoring and management.

(5) Cyber security: Since all of the things are connected with the cloud through agent, the loss can be substantial economically given the cloud is attacked. With the improvement of connection ability and circulation ability, the security problem is also increasingly prominent. Great care has to be taken to ensure the network security. First, confidentiality is required. The information should be completely inaccessible to unauthorized users. Second, integrity is another foundation of cyber security, which means the information cannot be modified or damaged and won't be missing within the stored or transfer procedures, given these behaviors are not authorized. The third meaning of cyber security is usability, i.e. when one device or user is authorized, they are able to acquire the required information. The fourth one is controllability on the dissemination of information and its content. Last but not least, the auditability is also vital to ensure the security. Supposing any security problem occurs, the engineers should be allowed to audit and find the networks' settings, historical records and so on. These can supply evidences and suggest remedies in the face of the security problems.

(6) Cloud computation: cloud computing is a computing method of a new generation based on the Internet. The Internet provides dynamically scalable and virtualized resources to users in order to complete sophisticated computing. These resources consist of networks, various servers, storage space, applications and other services. The cloud computing should be highly reliable, large in scale, virtualized and conveniently applicable.

(7) Big data: The diversified information assets of companies are now of tremendous amount and have a strong growth rate. Conventional software is not able to capture, manage and handle these information assets. Only the new processing mode can adapt to the considerable amount of information and the new processing mode is Big Data. The 5 V features of Big Data is volume, velocity, variety, value and veracity (Lohr 2012). The strategic significance of

Big Data is not to store the massive information. Instead, it emphasizes the specialized treatment on these data. For example, the cloud may store all the historical data about a machine's failure. Then the Big Data technology will analyze these data and help compare these data to the current running state of the machine in real time. In this way, it can help predict or discover problems of the machine and even suggest solutions. It is a key technology for self-maintenance of devices.

There are also other technologies which are important for the realization of CPS and the function of agent, such as augmented reality, autonomous robots, additive manufacturing, etc. Many of them are not quite mature but they are indispensable in a decentralized smart factory. They needs to be further developed to match the needs of industry.

4 A Cloud-Based Smart Manufacturing Paradigm

The above three sections basically introduce the idea of a decentralized smart factory, including its advantages over traditional manufacturing factories, its constituent parts, the conceptual models and operation mechanism of agent and cloud, and key supporting technologies. However, the way to build such a factory and the subsequent business model is still unknown to readers. Hence, this section will first come up with a general implementation approach to build a smart factory. Then, the new business model of manufacturing industry will be discussed.

4.1 Implementation Approach

The implementation approach is proposed by borrowing idea from engineering design (Dieter and Schmidt 2013). The basic steps include defining problem, gather information, generating concepts, evaluating concepts, detailed design of factory and implementation, as shown in Fig. 14.

Defining Problems is the first step, which is to analyze the existing problems and define the requirements. To give a comprehensive problem statement, the decision makers can analyze the operation performance from five aspects, which are quality, cost, delivery, safety and service. The narrow sense of quality refers to the product quality. Here, the quality should also include the quality of corporate environment, manufacturing equipment, working personnel and production flow. Some examples of the possible quality indexes are the number of defects, the ratio of first run acceptance, the ratio of units returned to units shipped out. Then, the cost refers to all the fixed cost and variable cost. The fixed cost includes the rent cost, administration cost, depreciation cost, etc. The variable cost include materials cost, labor cost, stock keeping cost, etc. Companies are required to reassess the waste or loss in

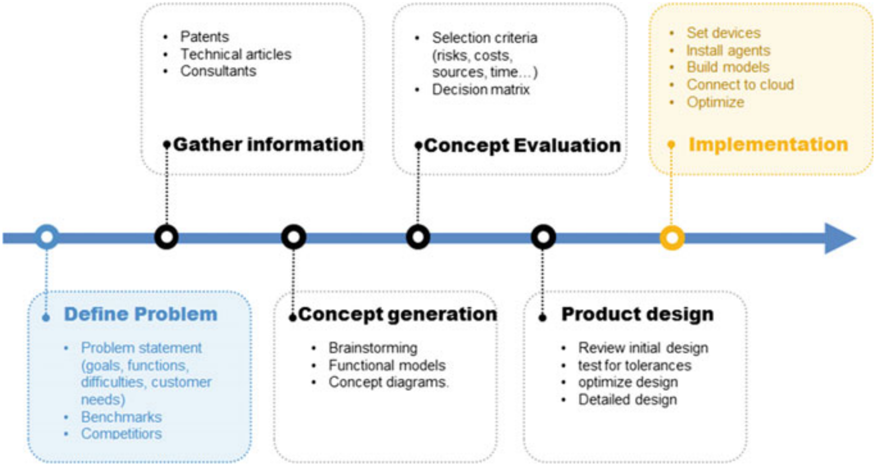
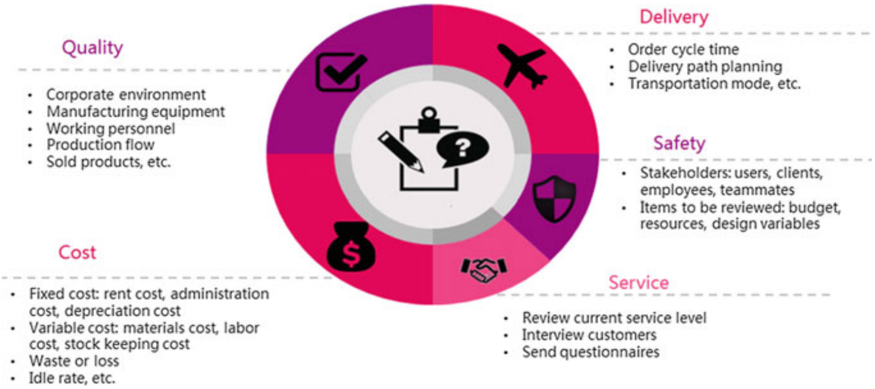


Fig. 14 Implementation approach to build CPS

production, the idle rate, the energy consumed, etc. Delivery focuses primarily on the order cycle time, which is time elapsed from the time when customer places an order to the time when the customer receives the product. In addition to the order cycle time, there are some other indexes to be considered, such as the travel distance, the transportation mode, the delivery path planning, order fulfillment degree, etc. The fourth aspect to consider is safety, which is extremely important for a company. It's engineer's social responsibility to ensure the safety of the users and clients of products, the employees within the whole factory and his or her teammates. Hence, employees are required to ensure the budget and resources available are sufficient to produce safe products. Also, they need to review all the design variables are accurate in order to guarantee the design s are safe. The last factor to analyze is the service. The employees of the company are expected to review their current service level. To make the survey results closer to reality, they can interview some customers to learn whether their service meets their expectation.

To have a more comprehensive and accurate picture about the problems, companies are suggested to look for some comparison standards. The first is the performance of benchmarking enterprises, since they usually adopt more premium technologies and apply more sophisticated management approaches. Then, the company could compare itself with its competitors, because this comparison will help point out more targeted improvement aspects to win the competition. The third comparison standard is the industry average level. The statistical data or the industry mandates could be referred to as reference. This is to help companies have knowledge of their level in the industry (Fig. 15).

The second step is information gathering. There are various information sources. For instance, the engineers could scan the patents available on the internet to see what software, hardware or devices are suitable. They can also search for technical articles on the Internet or in the library to find practical solutions, which may of



Quality
Corporate environment
Manufacturing equipment
Working personnel
Production flow
Sold products, etc.
Delivery
Order cycle time
Delivery path planning
Transportation mode, etc.
Safety
Stakeholders: users, clients, employees, teammates
Items to be reviewed: budget, resources, design variables
Cost
Fixed cost: rent cost, administration cost, depreciation cost
Variable cost: materials cost, labor cost, stock keeping cost
Waste or loss
Idle rate, etc.
Service
Review current service level
Interview customers
Send questionnaires

Fig. 15 Aspects of problems to be defined

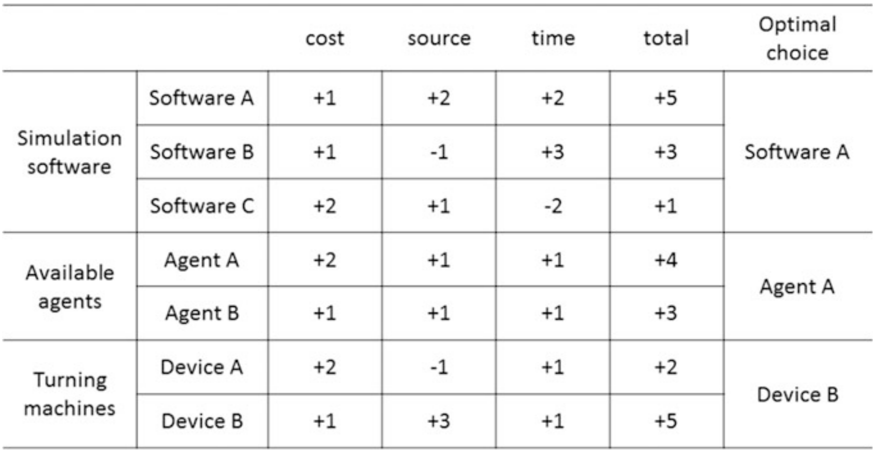
help to solve their problems. Then, they are also to employ some consultants to give a systematic evaluation as well as come up with some suggestions.

The third step is concept generation. In the light of their problems and available information, experts of the company may have a brainstorm, through which many novel ideas may be generated. These ideas should be different methods to realize CPS and build a smart factory that is up to their expectation. To better present the ideas to other teammates, they are advised to offer functional models and concept drafts.

What follows is concept evaluation. Experts are required to have a comprehensive evaluation on all of the ideas generated in the last step. It may help to first lay down some selection criteria, such as the investment, the availability of source, the time needed, the estimated annual production capacity, etc. A decision matrix could be given, which is meant to show the evaluation process and result more clearly. The matrix will be some table like Fig. 16. Every suggestion will be evaluated against the criteria point by point and scores will be given. The one with highest score will be the final choice.

The 5th step is to give detailed design of factory. To select the optimal design, decision-makers are expected to review the designs according to the evaluation again and test for the tolerances. After getting the best rough design, further detailed design is needed in this stage. The concrete layout, the parameters setting, the initial state and any other details should be settled down as much as possible.

Then, the final stage is implementation, in which the people of the factory will perform their design. The basic procedures can be as Fig. 17. They will first move the devices and work pieces to the exact locations according to plan and set this arrangement as initial layout. Then, they will make sure every device is equipped with the agent, since the agent is the most important communication medium between things and the cloud. After that, they will build models and simulate the actual operating conditions of the physical factory that will be uploaded to the cloud later. To prepare the cloud well, the computers, servers as well as the beacon should



		cost	source	time	total	Optimal choice
Simulation software	Software A	+1	+2	+2	+5	Software A
	Software B	+1	-1	+3	+3	
	Software C	+2	+1	-2	+1	
Available agents	Agent A	+2	+1	+1	+4	Agent A
	Agent B	+1	+1	+1	+3	
Turning machines	Device A	+2	-1	+1	+2	Device B
	Device B	+1	+3	+1	+5	

Fig. 16 Decision matrix example

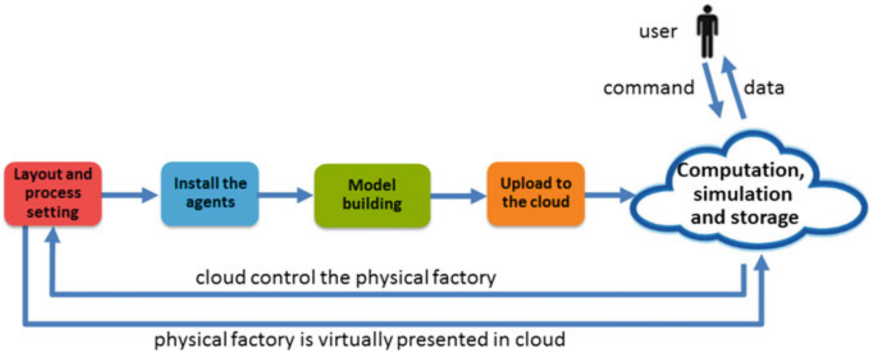

user
command
data
Layout and process setting
Install the agents
Model building
Upload to the cloud
Computation, simulation and storage
cloud control the physical factory
physical factory is virtually presented in cloud

Fig. 17 Implementation procedures

be in place ahead of schedule. By doing that, the physical factory in the CPS is connected to the cloud and every device is able to be integrated with other facilities. The cloud will carry out large amounts of computation work and simulation work, based on which the cloud will present the operation of virtual factory as well as exercise real-time control on the physical factory. At the same time, the users such as the workers, engineers or the financial staff will also have an access to the cloud. Through the agent, the users are able to acquire the data they need. Alternatively, they can also give the cloud a command to control the physical factory indirectly. In this whole implementation process, the layout or process method of the physical factory may be adjusted at any time according to the actual requirements and the computation result of the cloud.

The above is a simplified paradigm to implement the concept of a cloud-based smart manufacturing. As for the specified approach, the factory could make some adjustments and apply the idea according to their actual conditions. A real application case of a company in Shanghai will be given in Sect. 5.

4.2 Business Model

As stated above, the problem of Information Island exists within the company. So is the case among different companies. For instance, the manufacturing company usually has to place an order to its supplier, but the supplier knows nothing about its inventory, which results in the existence of a lead time in delivery process. What's more, the manufacturer mainly pays attention to selling products to its customers. When there is any problem with the product afterwards within the maintenance period, they will send people out to help for free. However, few manufacturing companies are considering charging a fee for service.

Nevertheless, after applying the idea of smart manufacturing to practice, the business model of the enterprise will be largely different from the current one. The internal integration and external integration will be achieved with the help of CPS in the new era. Furthermore, by making use of the cloud, the product-oriented manufacturing companies will possibly turn into service-oriented ones to cater to the market demands.

4.2.1 Internal Integration Within the Company

The internal integration within a company is achieved as shown in Fig. 18. It is a kind of vertical integration in the company.

The first integration is within the production department. All the production personnel have a connection to the cloud, including the research staff, the designer, the supervisor, the assembly worker and the dispatcher. Hence, they will know any changes in the design process or on the production field at the same time. There is no deviation of the content of the information or the time to be informed. Thus, the information flow is integrated in the manufacturing process. What's more, since all the devices are connected to the cloud also, the man-man, man-machine and machine-machine interactions will be much easier. The workpiece with the agent will be passed on to become the end product without obstacles.

The second internal integration is among different departments. Since every department such as the finance department, procurement department, production department and logistics department is allowed to obtain any data they need from the cloud, they all can learn about the process in due course. For instance, given the production department finds the material is not enough to manufacture the products, both the procurement department and the finance department will be informed of this immediately by the cloud. The procurement will purchase the raw materials

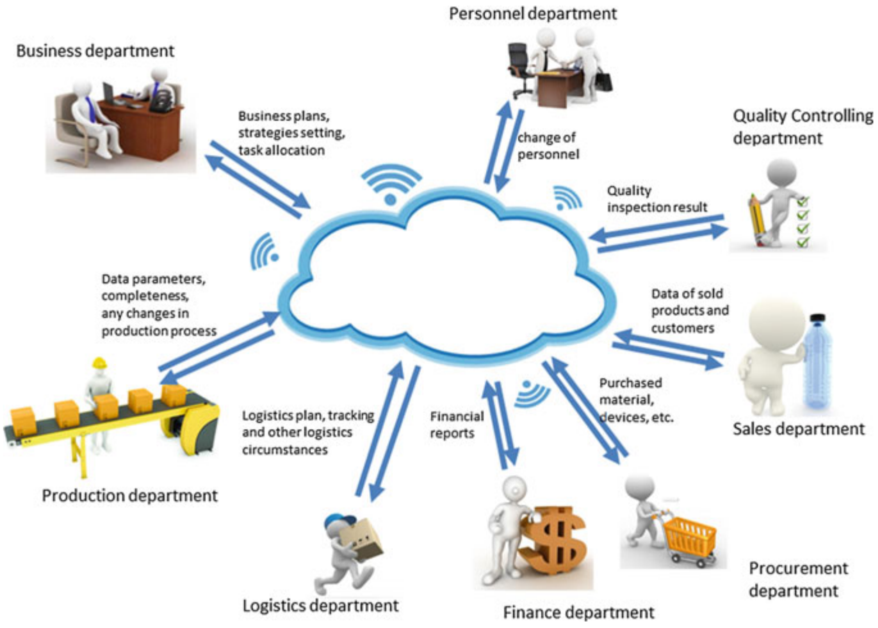

Personnel department
Business department
Business plans, strategies setting, task allocation
change of personnel
Quality Controlling department
Quality inspection result
Data parameters, completeness, any changes in production process
Data of sold products and customers
Purchased material, devices, etc.
Logistics plan, tracking and other logistics circumstances
Financial reports
Sales department
Production department
Procurement department
Logistics department
Finance department

Fig. 18 Internal vertical integration within the company

needed without the message sent from the production department. The finance department will alter their financial reports by reviewing the data retrieved from the cloud also.

It can be seen within a cloud-based manufacturing company, all of the information, logistics and capital are integrated. The problem of Information Island is resolved, which means all departments are linked together with the help of cloud in a cyber-physical system, so that seamless connection and coordination is realized.

4.2.2 External Integration Among the Companies

In addition to the internal integration, a smart manufacturing company in the future will possibly achieve external integration with other companies.

Some related companies have varying degrees of access to the same cloud, as a consequence of which they are able to get useful information in a timely manner. Hence, there is no need to wait for the notice from another stakeholder so that much time or cost will be saved in the cooperation. Two kinds of integration of companies will be discussed in the following, which are horizontal integration along a supply chain and cloud factory.

Horizontal Integration Along a Supply Chain

This kind of integration emphasizes the cooperation among companies along the same supply chain. The stakeholders chiefly consists contains supplier, manufacturer, distributer, retailer and customer. Sometimes, the third-party logistics is also involved. All of them are connected to the cloud mainly owned by the manufacturer, as shown in Fig. 19.

After such integration, the whole process is customer-oriented and the cooperative degree of the manufacturers with other organizations is increased dramatically. The supplier is able to read the material inventory of manufacturers. As soon as the inventory level reaches the re-order point, the supplier will deliver their goods to the manufacturer at once. With the cloud, the factory is also able to learn about the detailed requirement of customers immediately and directly, while in the past they have to predict the market demands by reviewing the orders from retailers. According to the customer requirement, they will further process on their WIP and produce the item which exactly meets the expectation. The distributer is also able to get the degree of completeness of the product in real time, so it will be much more convenient for the distributer to decide when to get goods from the manufacturer. Similarly, the retailer will also have an idea about the exact needs of customers and the inventory conditions of distributer, so that it will replenish its stock at the most appropriate time. If any third-party logistics will be hired, they are also authorized

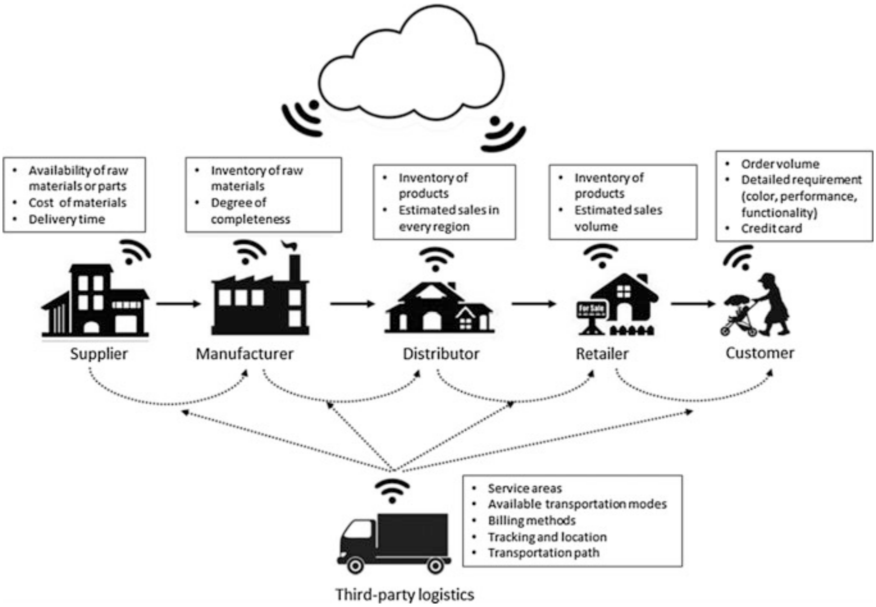


Fig. 19 Horizontal integration along a supply chain

to be informed of the completeness of products and the inventory of different parties.

It can be concluded that with the aid of the cloud, it's easier for manufacturers to achieve smart manufacturing, since they have a clearer mind about the customer needs and develop a better cooperation with other organizations along the value chain. As a result, just-in-time (JIT) manufacturing and delivery are able to be achieved. Also, the inventories stored by manufacturers, distributers and retailers will all be reduced, which will lead to a reduction in inventory holding cost. Also, the service level will be improved, since the requirements of customers are well taken care of during the whole process, and the delivery time is also cut in length. To briefly summarize, the horizontal integration of companies will lead to a new pattern of production, which features wide varieties, small batch and customized production with flexible manufacturing.

Cloud Factory

The cloud factory refers to the integration between companies of the same type. With this form of cooperation, the utilization rate of resource will be increased and companies will probably better meet the market demand. To illustrate better, an example case is shown as below (Fig. 20).

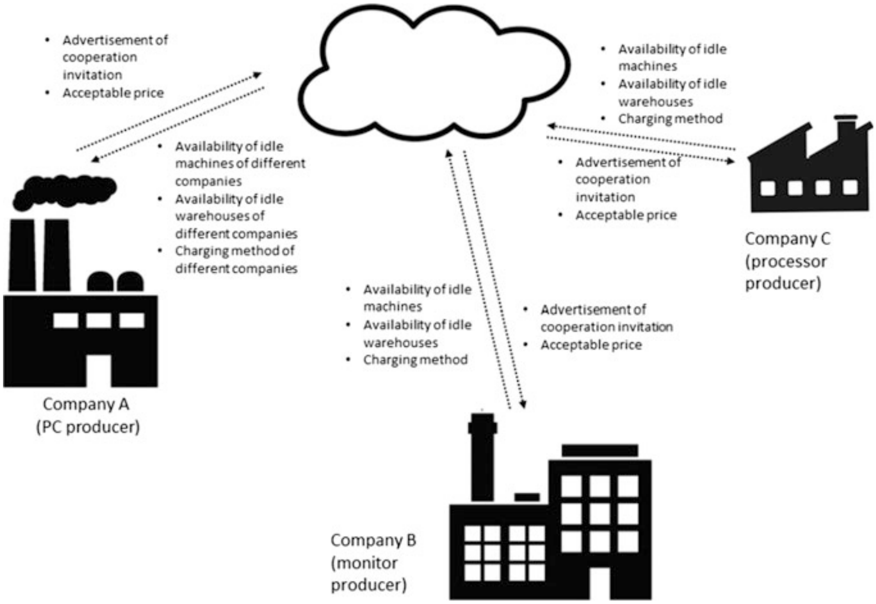

• Advertisement of cooperation invitation
• Acceptable price
• Availability of idle machines of different companies
• Availability of idle warehouses of different companies
• Charging method of different companies
Company A (PC producer)
• Availability of idle machines
• Availability of idle warehouses
• Charging method
• Advertisement of cooperation invitation
• Acceptable price
Company C (processor producer)
• Availability of idle machines
• Availability of idle warehouses
• Charging method
• Advertisement of cooperation invitation
• Acceptable price
Company B (monitor producer)

Fig. 20 Cloud factory

Company A is a PC manufacturer and it receives an urgent order these days. However, with some orders at hand, it is not possible for it to finish this stock of goods within the required time window. Then company A can propose some cooperation invitation on the cloud for help. Company B is a company to produce monitors and Company C's major products are processors. As it happens, when Company A proposes the advertisement, B and C have idle machines and surplus productively. In this condition, it's likely that Company A will outsource some work to Company B and C.

In this mode of cooperation, company A is assisted to meet the urgent demand of customers so that its corporate reputation is guaranteed. What's more, it can even outsource some work regularly in order to concentrate on its core task to win core competition. On the other hand, Company B and C are allowed to make the best of their resources. Instead of leaving the machines idle, they can charge for their service to Company A. It can be judged the form of cloud factory is a win-win cooperation method. Last but not least, the customers are also able to receive their orders in a shorter time.

4.2.3 Service-Oriented Trend of Manufacturing

As mentioned in the above sections, manufacturing companies now rely primarily on products to make a profit, but the good service is in short. However, in the new generation, it is predicted that there will be a service-oriented trend of manufacturing with the help of cloud-based CPS. Customer service mainly includes three elements that are pre-transaction elements, transaction elements and post-transaction elements. Currently, transaction elements have drawn attention of the manufacturers, such as the ability to back order, the transship, hey system accuracy, the product substitution, etc. (Stadtler 2015). In the future, manufacturers will pay more attention to pre-transaction elements and post-transaction elements as well, as shown in Fig. 21.

Before the transaction, companies will better take care of the personalized requirements of customers and inform the customers of more information. First, the customer will place an order to the company with his agent. Then the detailed requirement will be stored in the cloud, including his preferred color, the functions, size, configuration, etc. Then the company will retrieve the data and assign the jobs to different departments. The products to produce will exactly be personalized for customers. During production, the degree of completeness and the logistics process, the product condition and accurate documentation will all be uploaded to the cloud so that the customer is able to learn about it. Being informed of more information during the process, the negative emotions of customers such as anxiety will be relieved to a certain extent. The customer service satisfaction will be possibly improved significantly.

After the transaction, service is still continuing. The data of the product operation conditions and the customer will be transmitted to the company cloud in real time so that the company can predict or find any abnormal conditions in time. For

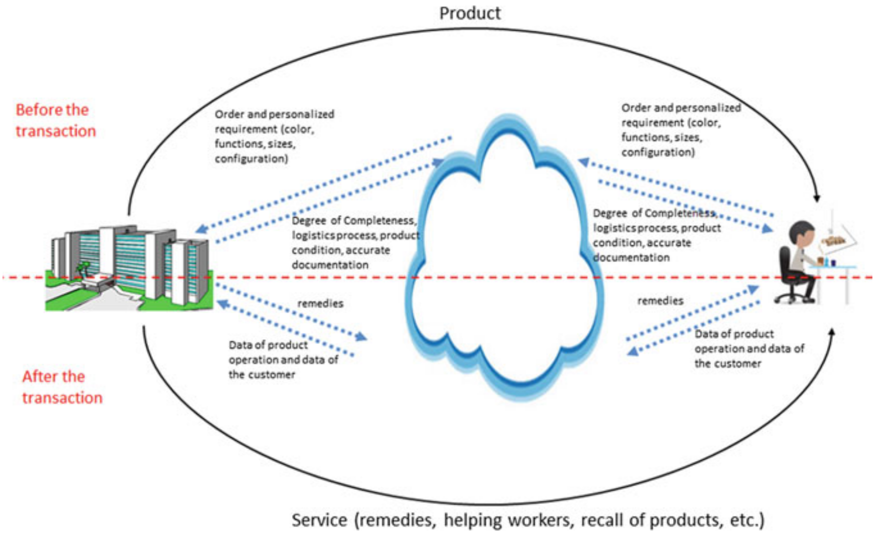

Product
Before the transaction
Order and personalized requirement (color, functions, sizes, configuration)
Order and personalized requirement (color, functions, sizes, configuration)
Degree of Completeness, logistics process, product condition, accurate documentation
Degree of Completeness, logistics process, product condition, accurate documentation
remedies
remedies
Data of product operation and data of the customer
Data of product operation and data of the customer
After the transaction
Service (remedies, helping workers, recall of products, etc.)

Fig. 21 Service-oriented business model

example, a watch company may get the operation data of the sold watch. The company may find the watch is dislocated even before the customer is aware of that. Accordingly, the company may suggest remedies to customers for repairing it, send out workers to help or even call back the watch. In addition to detecting the failure of the products, the company may also collect the data of customers and provide service accordingly. For instance, the smart watch may record the health indexes of the customer and upload it to the cloud. As long as there are any abnormal data, the company will give a warning and even help to inform his private doctor. For another example, the customer may take the watch to make explorations. The watch is recording and uploading his locations and tracks all the time. Assuming the customer meets any danger, the watch will play a big role for the salvage teams to rescue him.

The service after transaction is not merely solving quality problem or reflect customers' data. It may also include the inverse logistics of recycled packages, in which the location will be stored in the cloud. The service also includes handling customer claims and complaint. In this kind of process, all the departments will be informed of the claim and review their handling process so that it will take only a short time to find which department accounts for the problem.

To give a brief summary of this subsection, the customer service of a manufacturer will become more and more complete. Rather than only emphasizing the product quality in a one-time transaction, smart manufacturing companies will pay more attention to offer service with the help of their cloud in CPS.

5 Application Case

There is a manufacturing company in Shanghai that has tried to implement the proposed cloud-based smart manufacturing paradigm and achieved some results. This section will briefly introduce the background for the company to transform to smart manufacturing mode, and then illustrate how they are applying CPS to improve their overall performance. Out of consideration of commercial secrets, the name of the company is abbreviated as BY.

5.1 Background

In the wake of richer material life, customers are more and more demanding. People prefer customized items instead of standard products. What's more, the orders volume is also increasing due to the stronger purchasing power of people. Hence, the company is required to have a more flexible and efficient production system to meet the market demands. The sub-objectives can be listed as follows.

The first sub-objective is to dispose of the problem of Information Island. As stated above, departments within BY usually have no ideas about the alterations made by another department, since the information or material flow is unidirectional. Without the existence of an efficient communication channel, it is usually the case that one department only has a part of information about one order. With the deviation in the different departments' knowledge about the same case, some problems in finance, production or logistics might be unavoidable, which will cause the reduction in service level. It's hoped by Company BY that the application of CPS, it will have a better internal vertical integration across departments, because they will all be authorized to acquire data they need from the cloud or publish some commands or changes through the cloud. Within the production department, it is also expected people are allowed to have a more comprehensive idea about the whole section, instead only focusing on their own devices, materials and operation conditions.

Secondly, digital simulation and cloud computation could be utilized to optimize their factory design, such as the device layout, the machine parameters, material arrival rate, etc. The cost in money and time for reconstructing a production line is high for a company. Hence, it is not practical for it to try every design, compare the corresponding yield and then choose the optimal one. However, if a mode of cloud-based smart manufacturing is achieved, the cloud is able to help collect the information, compare the data with historical ones or industry standards, make simulations, etc. In this way, the cloud may send orders to the physical factory and guild the devices to re-configure themselves. As a consequence, the design of BY factory will be constantly improved so that the overall efficiency is also improved.

Last but not least, it's hoped by Factory BY to facilitate control on the machines and to improve the production efficiency. In the past, machines have to be manipulated by people, which increases the labor cost and limits the number of devices. Assuming remote operation is allowed, more devices will be introduced so that the overall efficiency will be improved. It will also be easier for the workers to view the global process to decide the operation on a certain machine.

To summarize briefly, Company BY tried to employ smart manufacturing mode and implement CPS, in the hope of optimizing their design, solving Information Island problem and facilitate the control. The ultimate goal was to improve the production flexibility as well as capacity.

5.2 *Application Situations*

After giving the background to implement CPS, this section will briefly how they are using this system now and the results that they have achieved.

With the CPS it has built, Company BY now has a new corporate structure as shown in Fig. 22 and achieved its objectives one by one.

First, the problem of Information Island is tackled within this company. After receiving an order placed by a customer, the business department will handle it and assign the sub-tasks via ERP system to different departments. For example, the manufacturing department will receive the production task and the logistics department should begin to plan the transportation route as well as select appropriate delivery mode. Especially within the production department, the material preparation station will get ready to acquire materials from the procurement

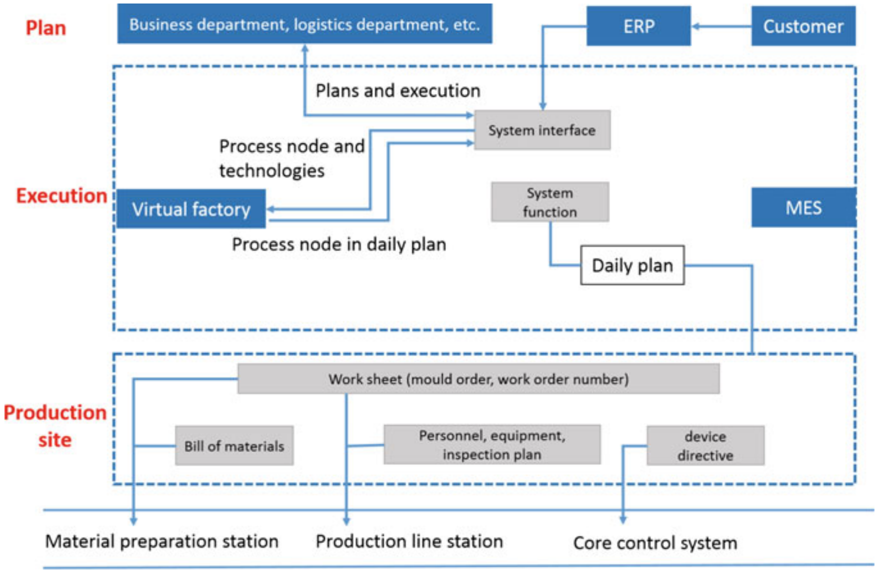
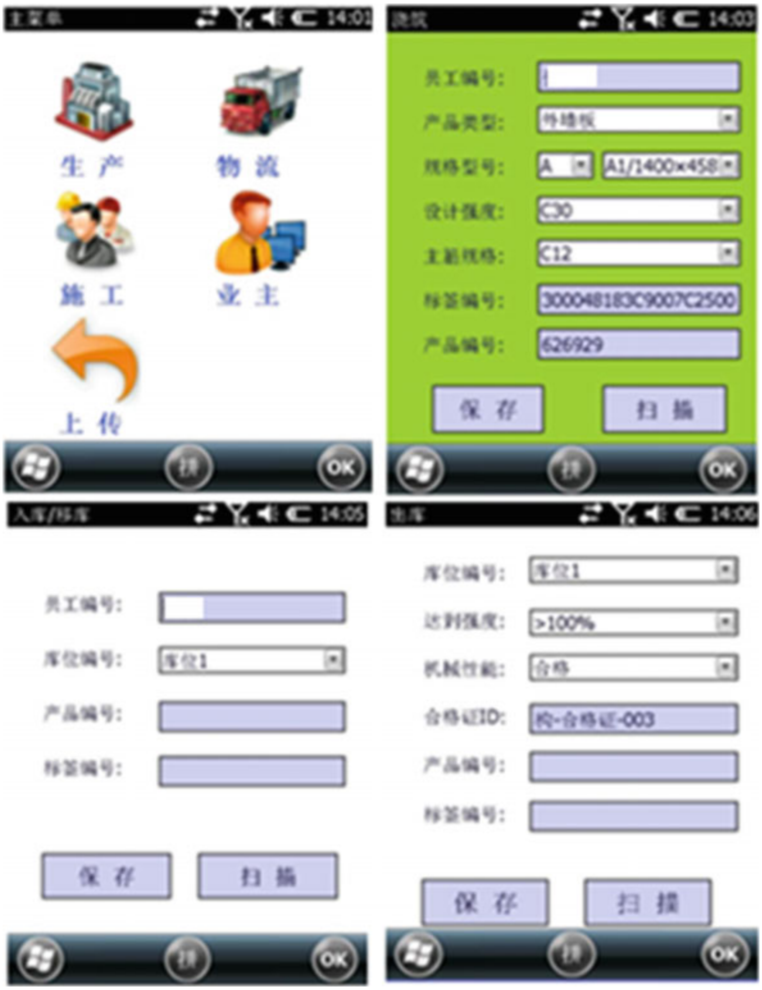

Plan
Business department, logistics department, etc.
ERP
Customer
Plans and execution
System interface
Process node and technologies
Execution
Virtual factory
System function
MES
Process node in daily plan
Daily plan
Work sheet (mould order, work order number)
Production site
Bill of materials
Personnel, equipment, inspection plan
device directive
Material preparation station
Production line station
Core control system

Fig. 22 Architecture of the smart company BY

department, while various production stations will check their equipment status, available technologies and skilled workers. All of these details including the customer requirements and task allocation will be stored in the cloud automatically and can be obtained via an Application (APP) as is shown in Fig. 23. The APP is their agent that can help to connect them with the cloud. For example, authorized employees can start this APP to view or alter the data about production, logistics and clients. The other three pictures show the information about employee ID, product type, specifications, stock number, certificate ID, etc. In this way, every department will have an idea about the responsibilities of every department and they will all be informed of any changes during the process. As the consequence, it is likely that the departments are able to work much more collaboratively.



员工编号:
产品类型: 外墙板
规格型号: A A1/1400×458
设计强度: C30
主筋规格: C12
标签编号: 300048183C9007C2500
产品编号: 626929

员工编号:
库位编号: 库位1
产品编号:
标签编号:

库位编号: 库位1
达到强度: >100%
机械性能: 合格
合格证ID: 检-合格证-003
产品编号:
标签编号:

Fig. 23 User interface of Company BY’s agent

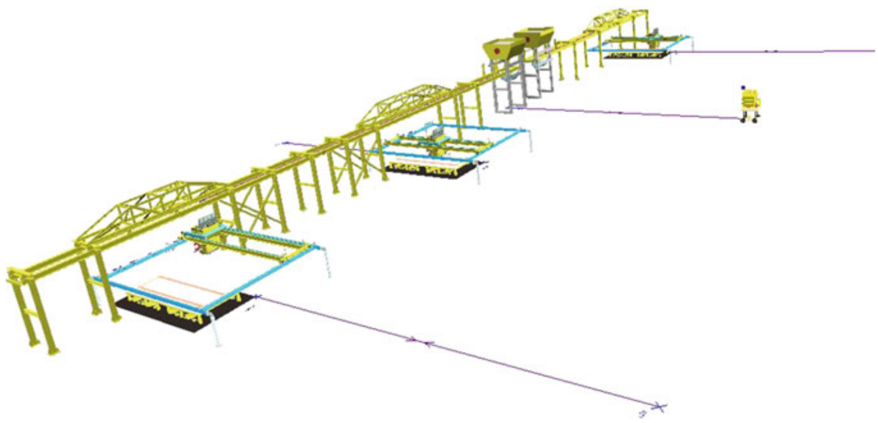


Fig. 24 A part of the virtual factory of BY

Secondly, they are able to optimize their design by simulation in the virtual factory. As shown in Fig. 24. They firstly build 3D models of various devices, which mainly consist of rails for trolley frames, the feeding trolley, the trolley rail, the walking placing boom, the lifting placing boom, vibrator, etc. Then, they will import this to simulation software, following which they will define the initial layout as shown and define the parameters of those facilities. By modifying the parameters and allowing the virtual factory to run for a certain period of time, engineers of Company BY could see different outputs accordingly. In the light of the outputs corresponding to various settings, engineers are allowed to obtain the optimized grouping method and the design of highest efficiency.

In addition, the plan will be keeping modified for higher efficiency even during the production process with the help of virtual factory. This modification mechanism is shown in Fig. 25. Every worker will have a Finish button on his or her agent. They are required to press the button when they complete their operation. The production cycle is set as 10 min in the virtual factory. Given that any worker does not complete his sub task within ten minutes, the extra time will be collected by the Manufacturing Execution System (MES) and then sent to the virtual factory. Then the virtual factory will make a quick analysis on the time delay and reenact the production schedule. Then the updated plan will be pushed to every station in site again so that the system accommodates the flexible and stochastic production process. In this manner, the operation method and schedule will be keeping modified to be suitable to actual circumstances.

The objective of remote control is achieved as well. An example to remotely manipulate the placing boom will be given to illustrate better. As shown in Fig. 26, the pictures on the right are the models of different placing booms, which are shown on the left. By viewing the operation condition of the model in the virtual factory, the workers are given an opportunity to learn about the actual operation status of its

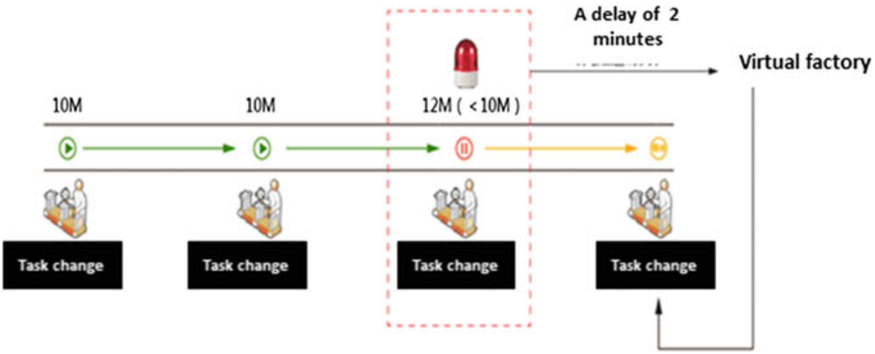


Fig. 25 Optimization in the production process via virtual factory

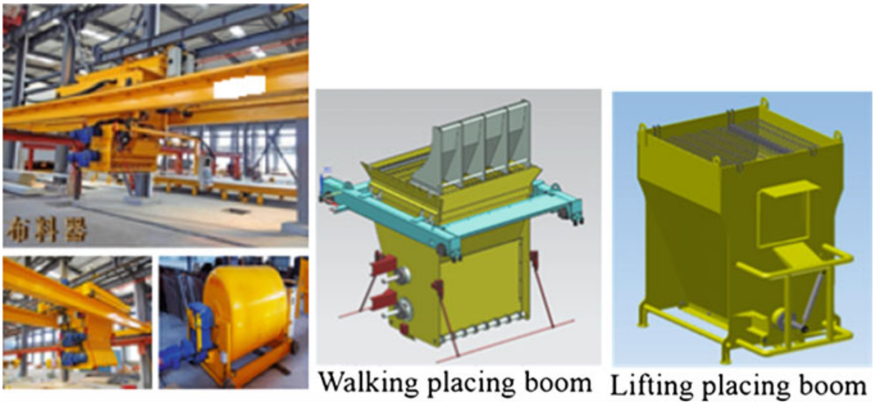
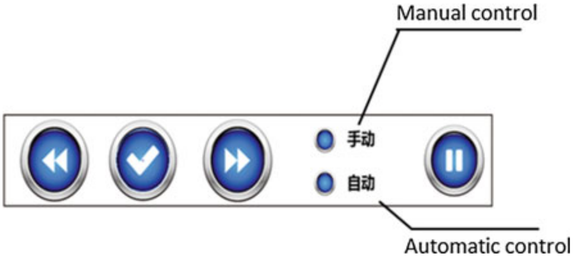


Fig. 26 Physical placing boom and its virtual counterparts

Fig. 27 User interface to manipulate machines remotely



counterparts in the actual factory. Then they will manipulate the placing boom remotely by clicking the buttons on their APP user interface, as shown in Fig. 27.

There are mainly 4 buttons for device manipulation. The first is back button. After clicking it, the placing boom will move back along its track. The second button is a tick, which indicates completion of the task. After the worker clicks the

Finish button, the core control system of the MES will receive the completion signal, and waits for the signals from other stations to achieve information linkage. The third is forward button that will make the placing boom to go forward along the track. The last button is stop button. By pressing this button, the device will stop any action at once. This button will be especially useful when there is an emergency. The two indicator lights are to show whether the production line is now in automatic mode or manual mode. This is set by the core control system. Since these operations are completed by using the APP, the workers are able to manipulate the machines remotely. This will definitely bring a lot of convenience to them.

Although the real-time simulation and external integration has not been achieved by Company BY, it can be seen the implementation of CPS has already enabled BY to tackle the problem of Information Island and optimize their design. Remote control is also realized to help BY to improve the operation efficiency.

6 Conclusion

This paper firstly introduces the concepts of Industry 4.0 and smart factories, and points out their superiority over the current manufacturing modes. Then, the idea of decentralized cyber-physical agents is illustrated, including its conceptual model, operation mechanism and its supporting technologies. This agent is to connect all the physical things with the cloud and will possibly play an important role in future's cloud-based smart manufacturing. The smart manufacturing company in the era of Industry 4.0 will have a totally different business model as discussed in this chapter and the implementation approach is also given. An authentic case of the Company BY proves that companies can take this methodology as a reference and follow this framework so as to improve the overall performance. To be specific, the company resolves the Information Island problem, realizes remote control and becomes much more flexible when dealing with customized orders.

This chapter borrows the synapse concept from biology to come up with the idea of agent, so that the connection between the devices/people/WIP and the cloud is realized. Compared to previous literature, in addition to discussing smart manufacturing theory, this chapter also specifically talked about the business model of the new generation of company and the application applicable approach to implement the method. It is speculated that this framework will have referential significance to many companies when they plan to turn into a smart manufacturer and improve their profit accordingly. However, some supporting technologies are not very mature currently, such as the internet of things and big data. Besides, the cyber security will also be a potential risk to a company if it is not well handled. It's advised the future works of scholars and engineers make efforts to enhance these aspects.

Acknowledgements The research presented in this paper was partially funded by the Ministry of Industry and Information Technology of the People's Republic of China (2016ZXFM03002), and the Shanghai Academy of Space Technology-Shanghai Jiao Tong University Joint Research

Center of Advanced Aerospace Technology (USCAST2016-16). Special thanks to Dr. Gang Liu and Mr. Zongkai Dai for the help of the case study.

References

Baheti R, Gill H (2011) Cyber-physical systems. Impact Control Technol 12:161–166

Davis J, Edgar T, Porter J, Bernaden J, Sarli M (2012) Smart manufacturing, manufacturing intelligence and demand-dynamic performance. Comput Chem Eng 47:145–156

Dieter GE, Schmidt LC (2013) Engineering design, vol 3. McGraw-Hill, New York

Eccles JC (2013) The physiology of synapses. Academic Press

Edgar TF, Davis JF (2008) Smart process manufacturing–a vision of the future. Ind Eng Chem Res Dev Centen Issue

Ghonaim W, Ghenniwa H, Shen W (2011) June. Towards an agent oriented smart manufacturing system. In: 2011 15th international conference on computer supported cooperative work in design (CSCWD). IEEE, pp 636–642

Lee J, Bagheri B, Kao HA (2015) A cyber-physical systems architecture for industry 4.0-based manufacturing systems. Manuf Lett 3:18–23

Lohr S (2012) The age of big data. New York Times, p 11

Lucke D, Constantinescu C, Westkämper E (2008a) Smart factory-a step towards the next generation of manufacturing. In: Manufacturing systems and technologies for the new frontier. Springer London, pp 115–118

Lucke D, Constantinescu C, Westkämper E (2008b) Smart factory-a step towards the next generation of manufacturing. In: Manufacturing systems and technologies for the new frontier. Springer London, pp 115–118

Lukasiewycz M, Steinhorst S, Sagstetter F, Chang W, Waszecki P, Kauer M, Chakraborty S (2012) September. Cyber-physical systems design for electric vehicles. In: 2012 15th euromicro conference on digital system design (DSD). IEEE, pp 477–484

Munir S, Stankovic JA, Liang CJM, Lin S (2013) Cyber physical system challenges for human-in-the-loop control. In: Presented as part of the 8th international workshop on feedback computing

Paletta L, Santner K, Fritz G, Mayer H, Schrammel J (2013) April. 3D attention: measurement of visual saliency using eye tracking glasses. In: CHI'13 extended abstracts on human factors in computing systems. ACM, pp 199–204

Song H (ed) (2009) Handbook of research on human performance and instructional technology. IGI Global

Sridhar S, Hahn A, Govindarasu M (2012) Cyber–physical system security for the electric power grid. Proc IEEE 100(1):210–224

Stadtler H (2015) Supply chain management: an overview. In: Supply chain management and advanced planning. Springer Berlin, pp 3–28

Wang Y, Zhou T, Liu Z (2013) Study on lean management mode of production and operation of enterprise teams. In: Informatics and management science IV. Springer, London, pp 603–610

Xu X (2012) From cloud computing to cloud manufacturing. Robot Comput-integr Manuf. 28 (1):75–86

Zhang Y, Xie F, Dong Y, Yang G, Zhou X (2013) High fidelity virtualization of cyber-physical systems. Int J Model Simul Sci Comput 4(02):1340005

Zhekun L, Gadh R, Prabhu BS (2004) January. Applications of RFID technology and smart parts in manufacturing. In: ASME 2004 international design engineering technical conferences and computers and information in engineering conference. American Society of Mechanical Engineers, pp 123–129

http://news.xinhuanet.com/politics/2015-05/28/c_1115441243.htm (Visit on July 1 2016)

Applying and Assessing Cybersecurity Controls for Direct Digital Manufacturing (DDM) Systems

Dominick Glavach, Julia LaSalle-DeSantis and Scott Zimmerman

Abstract This chapter will address cybersecurity threats to the Direct Digital Manufacturing (DDM) community, including potential attack scenarios and motivations. Many of these insights are the result of direct observation. As an illustrative example, we will discuss the details of a security assessment performed on an Additive Manufacturing (AM) system used for rapid prototyping and complex part production within the defense industry. Protocols and associated recommendations for incorporating security best practices during system installation and subsequent operation will also be presented.

Keywords Additive manufacturing · Direct digital manufacturing · DDM · STL · Cybersecurity

1 Introduction

Applying meaningful and assessing impactful cybersecurity controls for Direct Digital Manufacturing (DDM) is an ongoing and significant challenge for the DDM community. This issue will exponentially grow in significance as DDM technology moves into the mainstream manufacturing supply chain and more businesses and organizations take advantage of the many benefits of producing parts directly from a Computer Aided Design (CAD) drawing.

The power of DDM to enable rapid prototyping and re-design, while decreasing the investment in tooling and re-tooling, is proving to be a means of re-birth in American manufacturing and manufacturing engineering. Further, this combination

D. Glavach · J. LaSalle-DeSantis · S. Zimmerman (✉)
Concurrent Technologies Corporation, Johnstown, PA, USA
e-mail: zimmerms@ctc.com

D. Glavach
e-mail: dg@CyberSN.com

J. LaSalle-DeSantis
e-mail: lasallej@ctc.com

L. Thames and D. Schaefer (eds.), *Cybersecurity for Industry 4.0*,
Springer Series in Advanced Manufacturing, DOI 10.1007/978-3-319-50660-9_7

of benefits is especially attractive to Department of Defense applications where innovative design is required in a more and more constrained budget environment.

Based on the expectation and potential impact in revitalizing the U.S. manufacturing landscape, DDM, including Additive Manufacturing (AM) and other similarly disruptive technologies, will have a significant impact on national security. According to the National Defense University:

> The propagation of this technology has generated a host of national security considerations, which connect to broader economic and policy developments. AM can benefit the national security and defense community largely due to its economic potential. Additionally, the deployment of AM technologies in manufacturing will likely promote greater interaction between the national security community and the private sector, as businesses will be able to produce prototypes and sophisticated components more inexpensively and quickly than before (McNulty and Armes 2012).

The Economist (2014) refers to the potential for DDM to create the third industrial revolution, noting that the disruption to manufacturing will be as significant as digitization was to telecommunication, office equipment, photography and publishing. While DDM creates an incredible growth potential within manufacturing, it also comes with many of the associated cybersecurity risks that threaten other digitized industries.

Due to the potential economic and security implications of DDM, the industry is challenged to address cybersecurity risks in a timely way and develop standards, systems and processes for security before such wide scale adoption of the technology limits, or prohibits, the deployment of protection mechanisms.

While organizations like the National Institute of Standards Technology (NIST) and American Society for Testing and Materials (ASTM) are working to standardize the test products, geometries, and format of .STL files of AM, the industry would be well served to consider the lessons of rapid growth in other industries, such as power and energy, to ensure that security is a consideration right from the start.

1.1 Power and Energy a Case Study: Consequence of not Addressing Security Before a Technology Infrastructure Is at a National Level

The negative impacts of failing to include security processes and protocols at start-up can be seen within the power and energy sector. In this sector there are large deployments of programmable logic controllers (PLC) and supervisory control and data acquisition (SCADA) systems. At the time of design and deployment, these systems were not equipped with adequate security mechanisms and reliability protocols and methodologies simply did not exist.

Subsequently, in 2003, North America experienced its worst blackout to date, as 50 million people lost power in the northeastern and midwestern United States and Ontario. In some areas, power was not restored for nearly a week.

The Canada Power System Outage Task Force was formed to investigate how to prevent future blackouts and reduce the scope of those that occur. They concluded in a 2004 Final report that their single-most important recommendation is for the U. S. government to make Reliability Standards mandatory and enforceable. And so, in the Energy Policy Act of 2005 bulk electric providers were tasked to comply with the audits of a self-regulatory "electric reliability organization" called the North American Electric Reliability Council (NERC) and associated Critical Infrastructure Protection (CIP) 002-009 guidelines.

Complying with these energy and power security guidelines, after the control and data systems had become so tightly woven into the fabric of the power grid, and retrofitting security, became a much larger and more costly endeavor, than if the task of creating robust auditable security mechanisms and protocols had been tackled in the beginning. And while it's impossible to determine exactly, the costs and dangers associated with the 2003 prolonged blackout may have been mitigated if security mechanisms and reliability protocols and methodologies had been in place before the SCADA-based grid was allowed to blossom (US-Canada Power System Outage Task Force 2003).

The DDM community now stands on a similar precipice as the power and energy community did in the early 2000s. The emerging infrastructure for a technology so clearly in demand in both private and defense markets needs to define security guidelines, methodologies, and protocols before its reliability is compromised, security is breached, and a blackout-like incident occurs.

2 Defining Direct Digital Manufacturing

In a 2011 Brooking Institute web article, DDM was defined as "the fabrication of components in a seamless manner from computer design to actual part in hand. Also known as "3D printing" or "additive," "rapid," "instant," and "on-demand" manufacturing, DDM uses 3D computer-aided design files to drive the computer-controlled fabrication of parts. This next evolutionary move within manufacturing is driven by new hardware and software driven systems that use a variety of components and ingredients to build up layers of materials to create complex three-dimensional structures. These structures are designed, modeled and tested entirely within the cyber world prior to manufacturing. The Brooking Institute article details the process further:

> Unlike traditional machining methods, which involve working from a rough mold and then cutting away to achieve the desired complex shape, direct digital manufacturing creates the shape precisely and instantly, using additive fabrication. This new approach to manufacturing is a disruptive and potentially game changing technology (Schuette and Singer 2016).

With applications of the DDM technology rapidly evolving into the mainstream and defense pipeline, the importance of relevant and meaningful cybersecurity controls and reliability is also increasing. Imagine the impact to DDM pace-makers, or custom hip replacements if the supporting systems become unstable or unreliable. Imagine the impact if a nation-state actor or terrorist is able to modify the digital representation of a jet engine nozzle or if the DDM components in a counter-improvised explosive device (IED) cannot be deployed.

2.1 Installing a "New Printer"

The problems of applying rigorous cybersecurity at the onset, are compounded by the 'wild west' feeling of innovation. Opportunities to apply the DDM manufacturing technique to solve pressing problems for economic gain, are so dazzling that a slapdash security approach to incorporating DDM can occur. As an example, our involvement and interest in DDM cybersecurity began one day after a help desk call was placed asking if a technician could assist in attaching a new printer on the shop floor to the network. This task was originally assigned to a desktop technician whose principal responsibility is to perform basic break/fix activities of desktop software and hardware. Their tasking also includes installation and management of network printers and associated queues. So the technician dutifully found the appropriate Ethernet cable to attach it to the shop floor network, performed some basic configuration of the "printer" and let Dynamic Host Configuration Protocol (DHCP) do the rest.

Little did the technician and the rest of the internal information system management office know that this printer wasn't just a printer but a highly calibrated $750,000, dual-laser melting additive manufacturing system, or 3D printer. The importance, complexity and cost of the system would've been nice to know.

In this particular case, the AM equipment was delivered to the 'manufacturing' floor, unboxed and set up all without the awareness of the IT department. Once installed, the AM engineering team connected with the Enterprise Help Desk and requested "can you help connect our new printer to the network?" Unwittingly, the request was executed. Needless to say, the original equipment manufacturer (OEM) was unable to connect to the AM equipment, since it was behind the corporate firewall. Subsequent requests were submitted to the Enterprise Help Desk requesting that the OEM be given access to the equipment through the Internet for fine tuning. The printer was transferred to an open Internet connection normally provided to corporate guests. This channel is monitored, yet it has minimal shielding. It was only after subsequent investigation by the information security team that it became clear that the "printer" was in fact a metal DDM printer, not a typical office document printer. Following this discovery, the security team has moved the printer to a more secure and scrutinized subnet on the network where additional security controls and enhanced logging occur routinely and where it is still possible for the engineering team to work directly through the network with the manufacturer.

After this original connectivity was made, the materials engineers contacted the AM system manufacturers, a German owned and operated firm, and began to attempt to connect to the system over the Internet. What we later found was that this remote access to the system from the manufacturer is commonplace for the initial setup and calibration of the system, as well as for ongoing periodic access for maintenance and build troubleshooting. In this case, the printer in question could not initially be accessed directly from the Internet, as it was deep within the organizational security perimeter. So a request was made to create a hole into the company's security perimeter to allow access to the printer. This is when the security team was finally brought onboard, the threat profile and security assessment were performed, and mitigation steps taken.

To describe this phenomenon of bolting security on to a system post implementation we coined the term "the stagecoach principal." The stagecoach changed how goods got from point A to point B. It all worked well until someone noticed that there was something on the stagecoach of value and something they would want. So the robbers started to ride down from the hillside with weapons and take what they wanted. This happened because there was no active defense. So what did the stagecoach owners do? They put a marshal or person with a weapon on the stagecoach to protect it. The next time around, when the robber brought a stronger force, bringing his buddy and another horse, what does the stagecoach company do? They put a few extra horses in the rig and so the spiral continues. If they would have thought of their vulnerabilities up front the stage coaches could have avoided all of those evolutionarily mistakes.

Similarly, we continually make these types of mistakes in our push to get new technology into the mainstream market prior to developing mechanisms to update and secure them. Today is the time to think about inserting security into the digital thread, before it's too late.

3 Security Lessons from Past Industry Digitization

Digitization is as disruptive to manufacturing as it was to telecommunications, photography, and publishing. While there are many other examples, it's informative to look at the impact of digitization on security in the telecom and the previously introduced power and energy industry. Each of these industries experienced extra-ordinary fast paced growth that did or could outpace security.

3.1 Telecommunication: An Organizational and Policy Approach to Security

As privileged enablers of the digitization mega-trend, telecom companies are scrambling to find ways to monetize the infrastructure they already have in place.

The world is becoming more and more connected. Sometimes called the Internet of Things (IoT), all of our devices, more and more can communicate with each other over—with even our home thermostat connected to our watches—and the telecom industry is struggling with how to keep up with this ever increasing demand. Further, the growth of many services, like Netflix and Pandora, leverage what the telecom industry has built through 4G and 5G s, without giving much (if anything) back to sustaining the data infrastructure.

> Because many of these new services are managed in cloud-based systems, the digital environment will require a higher level of security and privacy protection than currently exists. That potentially presents yet another opportunity—it could be called a duty—for telecoms to set the benchmarks and standards for safeguarding the sensitive personal information shared by consumers, companies, and machines over these ubiquitous networks (Friedrich 2015).

As custodians of the networks, telecom carriers are charged with fighting the new threats. To address this, as well as many issues, many telecom providers are now appointing Chief Digitization Officers (CDO). CDOs for telecom networks will need to identify strategies to build features and security parameters that will ultimately end up largely shaping the future of the IoT and complementary applications. Like the power and energy sector, telecom networks are an integral part of a country's critical infrastructure and act as a backbone in enabling and linking the other critical components.

3.2 Power and Energy: A Lesson About the False Separation of Operational Technology Versus Information Technology

In some traditional security approaches, a distinction is made operational technology (OT) and information technology (IT). We have found this OT versus IT approach to be problematic, because currently the DDM "digital thread" spans both the OT and IT realms. As such, it inherits organic risks from each. For DDM, this means the lines between OT and IT, as traditionally understood, are blurring rapidly. Again, we can gain insight by looking at the lessons learned in power and energy.

Gartner, one of the world's leading information technology research and advisory company, defines **Operational Technology** (OT) as hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes, and events in the enterprise. **Information Technology** (IT) is the common term for the entire spectrum of technologies for information processing, including software, hardware, communications technologies and related services (Gartner 2016).

One common strategy of securing the IT side of the network from the operational side is to implement what is known as an "air gap." This air gap simply means that the networks have no direct connections between them. This approach breaks the “digital thread” as files must now be carried by hand from the design network (IT) to the manufacturing floor (OT). However, the “air gap” is rarely a successful security practice, as connections are the inevitable result of fast paced innovation and are bound to be made.

The “air gap” approach to cybersecurity has many other issues resulting in deficiencies, best illustrated in the power and energy case study. According to Sean McGurk, former Director, National Cybersecurity and Communications Integration Center (NCCIC) at the Department of Homeland Security, in a “Right Signals Blog” post:

> In our experience in conducting hundreds of vulnerability assessments in the private sector, in no case have we ever found the operations network, the Supervisory Control and Data Acquisition (SCADA) system or energy management system (EnMS) separated from the enterprise network. On average, we see 11 direct connections between those networks. In some extreme cases, we have identified up to 250 connections between the actual producing network and the enterprise network. (Mackenzie 2016)

For DDM applications, we can leverage this finding. It seems clear that while this approach might be attractive due to its surface simplicity, the air gap no longer works. There are too many interconnected systems between the shop floor, the enterprise network and external partners. In a 2016 Cisco white paper:

> Today manufacturers need “defense-in-depth” strategies that incorporate layers of independent security controls (physical, procedural, and electronic). In an era of converged IT and OT networks, cloud computing, mobility and Internet of Things (IoT) platforms, a holistic approach to data security is required.

Further, analysts say the benefits that come from managing IT and OT convergence, alignment and integration include optimized business processes, enhanced information for better decisions, reduced costs, lower risks and shortened project timelines (Pettey and van der Meulen 2011).

4 Defining the DDM Cybersecurity Threats, Vulnerabilities, and Risk Management

The potential impacts and damages perpetrated by cyber attacks are well known to businesses and manufacturing operators. The impact can range from physical and environmental damage to intangible impacts such as brand reputation and customer trust. Economic losses can be particularly severe in industrial settings, where an attack can cause losses of millions of dollars in downtime, disrupt production schedules and, in our assessment, damage expensive machines. In the worst case, the health and/or safety of workers may also be at risk, and in the case of a DoD application, even national security.

4.1 Tenants of DDM Cybersecurity

The tenants of cybersecurity are to preserve confidentiality, integrity and availability.

- **Confidentiality** is the tenant of cybersecurity focusing on protecting information from disclosure to unauthorized parties. Confidentiality refers to the need for the secure transfer and storage of information. A DDM example of a security control to protect confidentiality would be encryption of CAD data at rest on a device or data in transit over a communication link.
- **Integrity** is the effort of maintaining and assuring accuracy and consistency of data over its entire life-cycle. Integrity is a critical objective and component within DDM. In our assessment, we saw many examples of mishandling and control of data files including CAD, ".STL", etc.
- **Availability** refers to ensuring that authorized parties are able to access information when needed. This would include the shop's need to communicate with the AM printer OEM. You may not think of availability as a cybersecurity objective but if an adversary can keep you from accessing your systems and data there is a huge competitive advantage.

As you can see in Fig. 1, the three tenants of cybersecurity are tightly integrated.

4.2 DDM Cybersecurity Threats

DDM is advancing at an exponential rate in capability, complexity and speed. As the exponential rate of change increases there is a proportional increase in cybersecurity risks. These risks can compromise the confidentiality, integrity, and integrity of DDM systems. The threats can disrupt information systems, slow operations, halt production, impact product quality, compromise intellectual property or influence company reputation. Understanding DDM cybersecurity risks and developing strategies to manage cyber risk are key factors in DDM cyber resiliency.

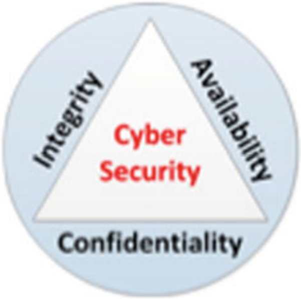


Fig. 1 Tenants of cybersecurity

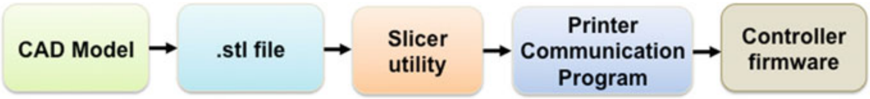


Fig. 2 Additive manufacturing digital thread

A key term used to describe the lifecycle and flow of information within the DDM process is "digital thread." The digital thread describes how the product's design and manufacturing information is authored, exchanged, and processed. A visual representation of the DDM digital thread is presented below, in Fig. 2. The process begins with the CAD 3D file that a draftsman or engineer uses to model and draw the piece. A CAD file can also be producing by scanning an object. An output of almost any mainstream CAD program is the .STL file. The .STL file communicates the details of the piece's surfaces to the hardware that will print/produce it. The slicer utility provides for the interpretation of details associated with printing (such as orientation) and allows for an opportunity to manipulate those details or 'tune' the model. The slicer utility is what cuts the 3D model into tiny digital sections that the 3D printer (firmware) can produce in the next steps of the digital thread.

There are several steps on the additive manufacturing digital thread, as shown in Fig. 2, where an attack could take place: the CAD model, the .STL file, the toolpath file, and the physical machine (controller firmware) itself. All along this digital thread there is an attack surface where the intellectual property or design can be stolen or compromised. In our assessment we saw the risks with poor configuration and data management practices and residual data left at each step on the thread.

4.3 DDM Cyber Vulnerabilities

DDM systems store data, process data with network connectivity and suffer similar cyber risks to corporate networks, laptops and mobile devices. These traditional cyber risks combined with DDM market growth presents attackers with new and potentially valuable targets. New attack opportunities include disrupting processes and facilitating theft, counterfeiting, and enabling sabotage.

Intellectual property is the most valuable target and is often under protected when in the form of an STL file.

Understanding the adversaries approach to attacking DDM systems enables stronger defense priorities and incident response strategies.

Cyber threats to manufacturing enterprises may be motivated by espionage, financial gain or other. These are digital assets so the same cyber controls that are in play to protect your home or business still apply. Things such as firewalls, intrusion detection systems and proxies should not go away.

DDM systems are complex, and so, also are attacks on DDM systems. Sophisticated and funded, competitors, partners, criminals, state actors and terrorist elements must have all the resources needed to accomplish these attacks. Let's take a look at a few of the motivations for attack.

Economic Advantage: The criminal element will get involved, any time there are goods for sale. These attackers are often not be as technically astute but they can have the capacity and resources to employee mercenary attackers as needed. This goes back to our stagecoach principal; the folks who attacked the stagecoach were not after the horses and the coach, they were after the goods, the gold and the money. There are people making significant amounts of money in this space.

Military Advantage: There are strategic and tactical military advantages to sabotaging a DDM system that entices nation state and terrorist actors. These attacks are high reward in that they may have the potential to negatively affect the operation of weapons systems on the battlefield.

Political Activism: Today we are printing products, engine parts, consumer goods and even jewelry. What could be the impact when DDM systems begin to print bio parts at scale? Printing bio parts raises ethical issues of human enhancement, population control, black market trafficking and grabs the attention of political activism (i.e. hacktivism).

DDM is advancing at an exponential rate in capability, complexity and in speed. As the exponential rate of change increases there is a proportion increase in cybersecurity risks. These risks can disrupt information systems, slow operations, halt production, impact product quality, compromise intellectual property or influence company reputation. Understanding DDM cybersecurity risks and developing strategies to manage cyber risk are key factors in DDM cyber resiliency.

4.4 DDM Risk Management Overview

Successful DDM risk management encompasses the traditional risk management processes at each component and along the entire digital thread. Managing risks along the digital thread enables the application of adequate controls to appropriately compensate for specific risk levels. Each element along the digital thread undergoes the following process.

Step 1: Identify the Risk. Identify vulnerabilities and threats with a potential for loss to availability, integrity, confidentiality. Vulnerabilities are defined as a weakness or likely deterioration in security. Threats are defined as an exploitation of a security weakness.

Step 2: Analyze the risk. Determine the likelihood and impact of each risk by developing an understanding of the risk, impact to the specific digital thread and the potential to affect the entire digital thread.

Step 3: Evaluate the Risk. Evaluate the risk by determining the risk magnitude, (the combination of likelihood and impact), technical control to minimize risk or categorized the risk as acceptable.

Step 4: Risk Controls. Risk control is the process of implementing controls or documenting acceptable risk for future evaluations

The technical advances and economic impact associated with the DDM revolution attracts an innovative and entrepreneurial audience. History shows us that new technologies have a tendency to influence a criminal opportunity via unexpected exploitation avenues. From the stagecoach to smart thermostats, security has often been an afterthought in new technology design and implementation.

In Mellissa Hathaway's paper, "Leadership and Responsibility for Cyber Security," Ms. Hathaway submits that corporate and government leadership are reactive in nature to cybersecurity needs and only act to mitigate security issues after a significant event occurs. (Hathaway 2013) She further concludes that additional legislation may be needed to incentivize corporate and government leadership to get serious about cybersecurity. Her point is further validated in the example of security and bulk energy providers described earlier in this chapter. It took a major power blackout that lasted several days for the government to create an energy security standards organization and demand bulk suppliers to comply.

The complexity and critical nature of some products being produced by DDM, ranging from fuel nozzles to human organs, render these systems obvious targets for cyber criminals, espionage actors, or digital activist groups. Regardless of motivation, gaining access to an industrial DDM system is not a trivial action and requires an intricate, but likely, attack scenario, that results in one of the following:

1. Theft (processes and property)
2. Disruption (slowing or stopping the DDM process)
3. Sabotage (inserting unforeseen time-delayed failures)

The combination of system complexity, installation methods and manner in which digital models become manufactured objects create a large attack surface. Within our assessment we focused on a few potential attack scenarios and associated risk evaluations which included:

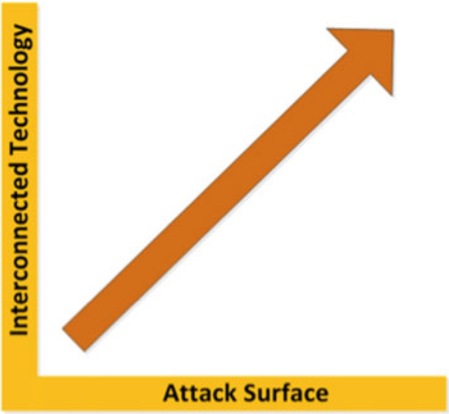
1. Model file formats
2. Data storage and transfers
3. Printer components software and firmware
4. Preproduction software
5. Engineering and production practices

We examine each of these areas in detail later in the chapter.

4.5 DDM Cyber Risks: Theft, Disruption, and Sabotage

We have bucketed what we feel are the current main risks to DDM as: Theft, Disruption and Sabotage. In addition to the new potential risks created by DDM, the traditional cyber breaches such as system compromise, unauthorized logins, viruses and ransomware are still in play. DDM systems are complex with

Fig. 3 Attack surface



potentially large attack surfaces. **Attack surface** refers to the number of things within a system that are vulnerable to attack. Your attack surface could be the STL file, printer or DDM process or model. As these systems become more obtainable to the masses, and organizations can produce goods-on-demand the system attack surface will continue to grow as seen in Fig. 3 below.

Theft—Property theft, in terms of intellectual property loss, refers to attacks that enable an adversary to reproduce physical products. Theft can be thought of in terms of process theft and license theft. Process theft is accomplished when an attacker is able to observe DDM processes in motion or recreate processes through inference by collecting data files on related but not connected systems. License theft is circumventing a right to use control to either extend beyond the intended usage time or duplicate DDM products beyond the intended quantity. License theft has a long history. As an example, not long after CD-ROMs and DVDs were used for movie distribution, someone figured out how to break the license or protection of the system and mass produce copies of the movies and then illegally distribute them.

Disruption—Disruption results in halting or delaying the DDM process through system compromise or data manipulation. For example, disruption can occur by modifying instruction sets to overheat components resulting in temporary or permanent physical damage to DDM printers.

Sabotage—Sabotage attacks impact DDM product reliability in a manner that is unnoticed by quality control processes. Sabotage includes modifications resulting in a reduction in reliability to include: slightly reducing the surface strength, slightly increasing the product size, reducing cooling speed and modifying product-infilling. Sabotage attacks on product reliability have measurable quantifiable costs including the cost to recall or the cost to remanufacture. The impact to reputation may have larger and long-term impacts.

5 Walking the DDM Digital Thread

Weaknesses and vulnerabilities within DDM systems are comparable to those within Industrial Controls Systems (ICS) elsewhere on the manufacturing shop floor. In fact, a good portion of the technical makeup of DDM systems is Programmable Logic Controllers (PLCs), which are embedded systems and actuators. This integration of ICS means that the same security vulnerabilities and weaknesses are inherited in DDM systems. According to a report produced in June of 2016 by the Department of Homeland Security Industrial Control System Computer Emergency Response Team (ICS-CERT 2016) the top six weaknesses that the team found fell into one of six categories.

1. Boundary protection
2. Least functionally
3. Authenticator management
4. Identification and authentication
5. Least privilege
6. Allocation of resources

The ICS Impact: A Case Study of Stuxnet

In August of 2011, a game changing computer worm began to get more and more press and notoriety. Little did the world understand at the time that the computer worm we now call Stuxnet would give rise to a continuously growing cyber war. Stuxnet was a 500 kilobyte computer worm that infected at least 14 industrial sites in Iran. The Stuxnet cyber kill chain operated in distinct stages; first through delivery removable media (USB Drives) and by replicating itself, targeting Microsoft Windows machines and networks, second it sought out Siemens Step7 software, which is used to program Industrial Control Systems (ICS) that operate equipment, and lastly it compromised the programmable logic controllers 11 that controlled the centrifuges. What this process delivered was the ability for the source creator to remotely monitor and spy on industrial control systems and cause the centrifuges they controlled to burst without anyone detecting the worm. This attack replicated itself globally creating many variations of the Stuxnet worm during the past few years. On the heels of the Stuxnet news, the U.S. Defense Secretary warned that the United States was vulnerable to a “cyber Pearl Harbor” that could derail trains, poison water supplies, and cripple power grids. The Secretary also noted that not only was there potential for physical damage to a system, like what was seen in Stuxnet, but also even greater potential of non-physical damage, such as stealing personal or sensitive data (Kushner 2016).

To further enforce how Stuxnet changed so much within the ICS space the FireEye report also stated “The discovery of Stuxnet in 2010 drove interest in industrial control systems (ICS) vulnerability research. FireEye iSIGHT Intelligence counted just 149 ICS vulnerability disclosures that were made between January 2000 and December 2010. Through April 2016, we have counted 1,552. We anticipate this upward trend will continue (Zhou 2016).

5.1 Data Storage and Transfers

During our team's assessment of the additive manufacturing system we observed heavy use of USB drives for data storage and transfer. This was mainly due to the fact that the systems were not networked together and the only means to move the design from the IT network to the OT network was through the use of this technology. There are many inherit risks using this type of media, including configuration management of both the physical device as well as loss or theft of the data on them.

In defense of the designer and material engineers, their first thought isn't: "How I am going to protect this data?" It is: "How am I going to get my job done?" To determine if there is a better way to accomplish this data storage and transfer we contacted the printer vendor. After a bit of discussion they provided two recommendations. The first, is a rather clunky recommendation: connect the printer to the network when printing and, when done, simply disconnect. The second, and vendor-preferred method, was that the client should use the USB drives.

This advice of just use the USB on the surface may seem like a good work-around but as seen within the spread of Stuxnet in the not too distant past, the high-profile attach was born of USBs. Both of these possible strategies are heavily dependent on training and awareness.

5.2 Stereolithography File Attack Research

As mentioned earlier the ".STL" (STereoLithography) is a file format native to CAD software created by 3D Systems. The ".STL" file type is the current defacto standard in AM. The STL file only contains the surface information of the part. At the February 2015 Direct Digital Manufacturing Cybersecurity Symposium hosted by the National Institute of Science and Technology (NIST), Christopher B. Williams Associate Professor, Virginia Tech Department of Mechanical Engineering presented research that he and his research team were able to intercept a job initialization file and decode it, allowing attackers to potentially alter printer parameters mid-print. The STL standard files are especially vulnerable to attacks that alter a design within the digital thread. The VA Tech research presented additional information on the ".STL" file and its makeup as a stored list of triangular elements (specified by the a set of x, y, and z coordinates of three vertices) in ASCII or binary format. An attack that simply edits the STL file could subtly alter the part geometry.

As a part of the research, and to further determine the potential impact of this specific attack, the VA Tech team conducted two experiments.

- **Experiment 1, a Printed Void**: The first experiment evaluated the effect of a "printed void" on the mechanical strength of a printed specimen. Several ASTM Standard D638-10 tensile test specimens with and without voids were printed via Powder Bed Fusion (a Sinterstation 2500 Plus machine) using Nylon 12 powder. Upon testing, all of the specimens containing voids fractured at the void location, while the specimens without voids failed normally. The average reduction in yield load was 14%, from 1085 N to 930 N, and the strain at failure was reduced from 10.4 to 5.8%.

- **Experiment 2, Feasibility of an Attack**: Second, a case study was performed to determine the feasibility of a cyber-attack on a simple AM system and to evaluate the ability of AM operators to detect an attack. In this experiment, upper-level and graduate engineering students were challenged to manufacture and test a tensile test specimen. Unknown to the participants, the computer used was infected with ".STL" attack software that automatically inserted voids into their files before fabrication. Upon completion of the printing, none of the participants detected the presence of the voids in their parts. Upon breaking the part, all participant teams identified that their parts failed prematurely. Two teams detected the presence of a void at the fracture location. However, both of these teams concluded that the placement was due to problems with the machine. Two teams did not notice the voids and attributed the failure to the anisotropic nature of additively manufactured parts.

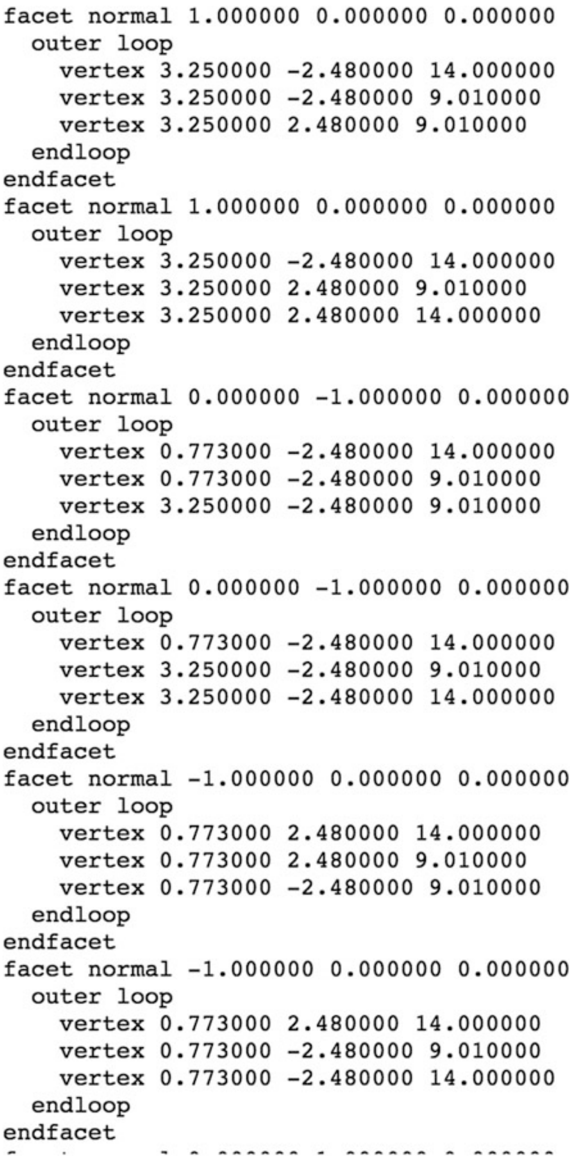
It was the VA Tech team's conclusion that attacks on STL are a viable attack avenue and the STL and other file formats should not be scrapped but that additional security protection should be put in place. These controls and mitigation steps included:

- File hashing that would allow the user to validate the authenticity of the file
- Improved checks within the quality control process
- Improved process monitoring through the development of a "side channel". This method creates a baseline operating parameter so that deviations could be detected
- Operator training (Williams 2015).

This last item, Operator Training, is probably the most impactful. It is the observation of the authors, that, in addition to the six weaknesses identified above by ICS-CERT (boundary protection; least functionally; authenticator management; identification and authentication; least privilege; and allocation of resources) we have also seen another increase in misconfiguration of settings. While the ICS-CERT team has identified the 6 weaknesses, a theme that our assessment teams sees on a regular basis is that of a lack of cybersecurity awareness training. While this is the most "low tech" of the weaknesses it pays the highest dividend in outcome (Fig. 4).

The easy access or wide adoption of a trusted file format like the ".STL" has its pros and cons. Because it is trusted, we are willing to download it and print it without much thought. These files are widely available on the Internet from various websites, both trusted and untrusted. When these files are downloaded off these unknown or potentially untrusted sites there is also no file integrity. The ".STL" files comes in two formats, binary and ascii which is human readable.

Fig. 4 Sample STL file



```
facet normal 1.000000 0.000000 0.000000
  outer loop
    vertex 3.250000 -2.480000 14.000000
    vertex 3.250000 -2.480000 9.010000
    vertex 3.250000 2.480000 9.010000
  endloop
endfacet
facet normal 1.000000 0.000000 0.000000
  outer loop
    vertex 3.250000 -2.480000 14.000000
    vertex 3.250000 2.480000 9.010000
    vertex 3.250000 2.480000 14.000000
  endloop
endfacet
facet normal 0.000000 -1.000000 0.000000
  outer loop
    vertex 0.773000 -2.480000 14.000000
    vertex 0.773000 -2.480000 9.010000
    vertex 3.250000 -2.480000 9.010000
  endloop
endfacet
facet normal 0.000000 -1.000000 0.000000
  outer loop
    vertex 0.773000 -2.480000 14.000000
    vertex 3.250000 -2.480000 9.010000
    vertex 3.250000 -2.480000 14.000000
  endloop
endfacet
facet normal -1.000000 0.000000 0.000000
  outer loop
    vertex 0.773000 2.480000 14.000000
    vertex 0.773000 2.480000 9.010000
    vertex 0.773000 -2.480000 9.010000
  endloop
endfacet
facet normal -1.000000 0.000000 0.000000
  outer loop
    vertex 0.773000 2.480000 14.000000
    vertex 0.773000 -2.480000 9.010000
    vertex 0.773000 -2.480000 14.000000
  endloop
endfacet
```

5.3 Printer Components

Generally once DDM systems are setup, calibrated and optimized, there is minimal continuous monitor and patching of the operating and control systems. A key finding during the assessment was that the operating systems on the printer, both Linux and Windows, were not even close to being up to date with patches and updates. When we spoke to the printer vendor and asked for their recommendation as to the best way to keep them up to date, they said "unplug the printer from the network when you are not using it". They clearly thought about it but a solution was simply not high on their "to do" list. Actually, in defense of the manufacturer, they did have Antivirus software on the printer. The only issue was that it kept interfering with the manufacturer and the material engineer when they were calibrating and troubleshooting, so they turned it off. It also didn't help that the version of the Antivirus software was in the German language.

In addition to operating and control systems, there are network settings within these printers that allow each subsystem to communicate. Each operating system had its own TCP/IP network stack communicating on a non-routable 10.x net.

5.4 Engineering and Production Practices

As a simple illustration of the lack of configuration management of data files, we located an Internet born ".STL" file example and emailed it directly to a material engineer's account. We crafted the email as though it looked like it came from the printer manufacturer as a tool to calibrate the printer. We named the file, printer.stl.exe and included it as an attachment on the email. Sure enough the engineer prepped and sent the ".STL" file to the printer without a second thought. This is not only a problem within the manufacturing space, we see it all the time with specially crafted email asking the recipient for an immediate response to open a Microsoft Word document and before long the system is infected or worse encrypted with ransomware.

Ransomware has become more and prevalent and if our calibration file would have included ransomware the results could be catastrophic.

As previously mentioned, USB drive or removable media use was relied on heavily by the materials engineer to transport data from CAD to a model file to ".STL" file. The revision control or configuration management was non-existent. There were uncontrolled copies of intellectual property in every location along with the residual data that could become extremely valuable to an attacker.

These printers require a lot of continued technical and maintenance support from the manufacturer, especially at initial deployment. To enable this, the German manufacturer installed remote control or remote access software on the printer that is configured to allow them to connect to the printer remotely. This could potentially create International Traffic in Arms Regulation (ITAR) issues. Not only was this software setup to allow for client controlled remote access, it also had a self starting function that enabled it whenever the printer was turned on. So without the client knowing, the manufacturer could remotely access the system at any time.

Not all remote access is bad. If done correctly, remote access for technical support can be powerful and cost effective method. However, that was not the case with the findings in our assessment. All settings were default and the communication protocols were all unencrypted. Overall remote access systems are one of the top three targets for an attacker. Leaving them set in default and wide open was a critical finding.

5.5 Assessment Methodology

AM systems can be complex, consisting of several central processing units (CPU) and PLCs, operating systems, and applications. The list includes both AM-specific components as well as applications that support the user experience, such as web-browsers and Portable Document Format (PDF) readers. The CPU/PLCs communicate via standard network protocols such as TCP/IP within the printer and then to a gateway interface for larger network access. The operating systems and applications on these controllers process design data to produce 3D components.

The assessment team utilized both our company's proprietary security assessment methodology as well as the security risk assessment provided in the NIST Draft NISTIR 8023, "Risk Management for Replication Devices" (Paulsen and Dempsey 2015).

5.6 System Assessment

Our team had the opportunity to conduct a security assessment on a newly installed AM system. The assessment methodology we used was developed by our team over a number of years and included a toolset that was mainly focused on IT systems.

The focus and priority of the materials/manufacturing/engineering staff are installation and operation, which includes connection to the internal and possibly external (OEM) network, so the relevant parts can be produced. Their concerns are usually not about how to make this system secure.

What we found was:

(1) Most applications and OS's unpatched
(2) Factory default install of AV/Host IDS (plus German language)
(3) No process for updating/patching
(4) Residual data left everywhere
(5) Poor authentication (shared/default passwords)

6 Recommendations

- Mandatory scanning (enumeration) of system prior to deploying to the network and disabling of all unneeded communications/system processes

- Review of user accounts/groups on the system including their level of privilege and accordingly adjust
- Removal of all unneeded applications installed on the system (browsers, readers, games, etc.)
- Enable host-based firewall to allow communication via secure ports to know IP addresses for manufacturer communications (disable this connectivity when not in use)
- Develop, document and train for system updates/upgrades processes

According to a 2016 Cisco report:

> To thrive in the new threatscape, manufacturers need to implement new strategies and architectures.

"Defending the edge" with firewalls and access management is as necessary as a strong OT segmentation strategy, both of which are generally lacking in ICS networks today. But this is only part of the solution in today's vulnerable industrial environments, where threats can originate both outside and inside the factory, and may be unintentionally caused by human error." (Cisco 2015)

In addition, manufacturers must also give the task of securing the shop floor to the Chief Information Security Officer and allow him to assemble a team made up of both OT and IT professionals to ensure that the flow of information from the enterprise network (design, modeling, etc.) to the shop floor (toolpath and manufacturing) is uninterrupted and secure.

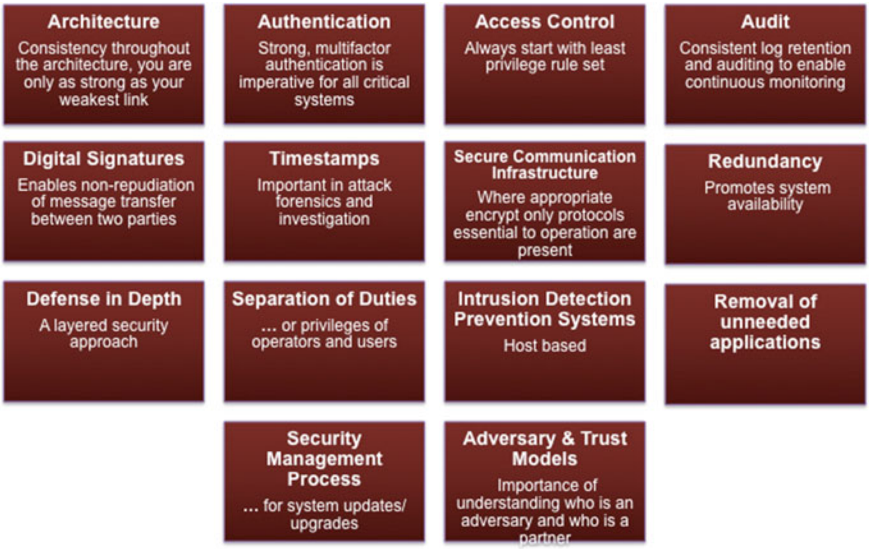
On a broader scale, the DDM community would be well-served to consistently advocate whenever possible for the implementation of security processes and standards, before a black-out incident suffered by the power and energy sector. This could come in the form of advocacy within professional groups, as well as internally promoting awareness all along the chain, from fabricators on the shop floor, to engineers. We recommend that standards, systems and processes be developed before technology is adopted broadly and when it limits or prohibits deployment of protection mechanisms.

7 Conclusion

DDM systems are an innovative and on-demand technology that represents game changing advances to supply chains, consumer goods and economic growth. In the same manner DDM systems are presenting new opportunities for innovation and creation, they are creating new cyber-attack vectors and scenarios that could present potential negative impacts to supply chains, military equipment and consumer confidence. The DDM systems are complex system of systems comprising of multiple Operating Systems, input/output peripherals, networks and process data from media types ranging from CD/DVDs, serial connections and USB thumb drives. The complexity and consistent calibration creates a hesitation from system owners to execute routine cyber hygiene (updates, strict user authentication, screen locking, inactivity timeouts and excessive service removal) activities. The lack of routine cyber hygiene maintenance creates an environment where IT or cybersecurity staffs isolate DDM systems on disconnected or "air gap" networks. The system owner's hesitation to update and operational staff's urge to segregate on another network compounds the cybersecurity risks, further expanding the DDM attack surface.

At a minimum for manufacturers, it is necessary to identify high-impact, quick-mitigation risks by assessing each DDM system as an individual system in the first iteration of the assessment process. Identifying high-impact, quick-mitigation risks increases cyber resiliency removing low effort opportunities to exploit vulnerabilities. Then, do a comprehensive risk assessment with planning for both mitigation and acceptance steps. It is imperative that security be an up-front consideration throughout all aspects of the equipment and process lifecycle, from design through disposal. If this is not the case and the cybersecurity staff does not develop processes and technology to mitigate risks and threats throughout, these systems will become increasingly insecure as the operational staff will find ways to circumvent implemented security controls. The following is a discussion of focus areas for DDM cybersecurity staff (Fig. 5).

Architecture—Cybersecurity consistency throughout the architecture. Identify and address high-impact quick mitigation risks and position DDM systems on networks that preserve integrity, availability, and confidentiality of data.



Architecture
Consistency throughout the architecture, you are only as strong as your weakest link

Authentication
Strong, multifactor authentication is imperative for all critical systems

Access Control
Always start with least privilege rule set

Audit
Consistent log retention and auditing to enable continuous monitoring

Digital Signatures
Enables non-repudiation of message transfer between two parties

Timestamps
Important in attack forensics and investigation

Secure Communication Infrastructure
Where appropriate encrypt only protocols essential to operation are present

Redundancy
Promotes system availability

Defense in Depth
A layered security approach

Separation of Duties
… or privileges of operators and users

Intrusion Detection Prevention Systems
Host based

Removal of unneeded applications

Security Management Process
… for system updates/ upgrades

Adversary & Trust Models
Importance of understanding who is an adversary and who is a partner

Fig. 5 Focus areas for the security team

Authentication—Strong authentication is imperative for DDM cyber resiliency. Each system across the digital thread requires authentication and integrates multifactor authentication or account verification when remote access is used to access DDM systems.

Access Controls—Utilizing the principle of least privilege principles strengthens system integrity and enables access to information and resources necessary to accomplish tasks essential to an operator's workload.

Audit—Consistent logging of successful and unsuccessful system events enables continuous monitoring. Supplementing native logging with a centralized log-server validates log event entries and enables data retention policy compliance.

Digital Signatures—Enables non-repudiation and enables confidentiality of message transfer between two parties or systems.

Timestamps—Consistent correct time configurations on all systems in the digital thread provide critical reference points for digital forensics and breach investigation processes.

Secure Communication Infrastructure—Integrates encryption of data at rest and data in transit. Validating strong cryptographic protocols, appropriate key lengths and hashing as well as enabling Transport Layer Security (TLS) over Secure Sockets Layer (SSL) is recommended.

Redundancy—Promotes system availability. Build redundancy in systems producing products and redundancy in systems providing cybersecurity protection.

Defense in Depth—A layered security approach prevents a single failure in the security architecture to result in DDM system compromise. Defense in depth assists in security update priorities and facilitates risk acceptance.

Separation of Duties—Enables the detection of security control failures that indicate information theft and security breaches.

Intrusion Detection and Prevention systems—Complements security architectures, integrity measures and validates security controls.

Removal of Unneeded Applications—Provides cyber resilience by eliminating a potential attack surface that is not critical to successful DDM operation.

Security Management Process—A security management process allows for thorough testing of patches system updates so that the update doesn't do more harm to the system then good. It also allows for a risk/benefit analysis to be completed before patch implementation. An effective security management process comprises six subprocesses: policy, awareness, access, monitoring, compliance, and strategy.

Adversary and Trust Models—Developing and maintaining understanding adversary tactics, techniques and procedures assist in the cybersecurity priorities and risk acceptance processes. Validating partner cybersecurity controls increases DDM cyber resilience.

Weakest Link—Human error, whether accidental or intentional, can wreak havoc on DDM and bring the functionality and safety of the system to a halt. The most prevalent human threats are untrained operators causing accidental infections and disgruntled insiders.

References

Gartner (n.d.) IT Glossary. http://www.gartner.com/it-glossary. Accessed June 2016, from Gartner

Hathaway ME (2013) Leadership and responsibility for cybersecurity. Georgetown J Int Aff 71–80 (2013)

Kushner D (2016) The real story of Stuxnet, IEEE Spectrum. http://spectrum.ieee.org. Accessed June 2016

McNulty CM, Armas N (2012) Toward the printed world: additive manufacturing and implication for national security. September 2012 Institute for National Strategic Studies, National Defense University, Defense Horizons

National Cybersecurity and Communications Integration Center, ICS-CERT May-June 2016 Monitor. https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_May-Jun2016_S508C.pdf

Paulsen C, Dempsey K (2015) NIST DRAFT NISTIR 8023, Risk Management for Replication Devices, 2015. http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8023.pdf

Pettey C, van der Meulen R (2011) Gartner says the worlds of IT and operational technology are converging, March 16. http://www.gartner.com. Accessed 14 June 2016, from Gartner

Sean McGurk, former Director, National Cybersecurity and Communications Integration Center (NCCIC) at the Department of Homeland Security. http://www.belden.com/blog/industrialsecurity/Goodbye-Air-Gaps-Hello-Improved-ICS-Security.cfm

Schuette L, Singer PW (2016) Direct digital manufacturing: the industrial game-changer you've never heard of. http://www.brookings.edu/research/articles/2011/10/10-digital-manufacturing-singer. Accessed July 2016

The Cisco Connected Factory: Holistic Security for the Factory of Tomorrow, Cisco Manufacturing White Paper. https://abm-website-assets.s3.amazonaws.com/manufacturing.net/s3fs-public/lead_gen_files/

The Economist (2014) A third industrial revolution. http://www.economist.com/node/2155e.2901. Accessed Nov 2014

U.S.-Canada Power System Outage Task Force, Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations. http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf

Williams CB (2015) NISTIR 8041, Proceedings of the Cybersecurity for DDM Symposium, National Institute for Science and Technology. http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8041.pdf

Zhou W (2016) Overload: critical lessons from 15 years of ICS vulnerabilities report. https://www2.fireeye.com/ics-vulnerability-trend-report-2016-em.html

http://www.strategyand.pwc.com/trends/2015-telecommunications-trends, 2015 Telecommunications Trends, Bahjat El-Darwiche, Steven Hall

The Resource Usage Viewpoint of Industrial Control System Security: An Inference-Based Intrusion Detection System

Rahul Nair, Chinmohan Nayak, Lanier Watkins, Kevin D. Fairbanks, Kashif Memon, Pengyuan Wang and William H. Robinson

Abstract Programmable Logic Controllers (PLC) are a part of a broader category of systems commonly known as Industrial Control Systems (ICS). These systems are primarily used to monitor and control various manufacturing and distribution processes, such as switches, pumps, or centrifuges. Since these devices perform relatively the same tasks throughout their lifetime, they likely have a fixed and predictable CPU load or usage for extended periods of time. Our work is primarily based on the premise that we are able to infer CPU load by remotely profiling the network traffic emitted by an ICS device and use that inference to detect potentially malicious modifications to the behavior of the ICS device. This is in stark contrast to traditional (e.g., signature and rule-based) and even other non-traditional (e.g., power fingerprinting and backplane traffic monitoring) intrusion detection mechanisms for ICS networks, since our approach does not require signature or rule

R. Nair · C. Nayak · L. Watkins (✉) · K. Memon
Information Security Institute, Johns Hopkins University, 3400 N Charles Street—Malone 161, Baltimore, MD 21218, USA
e-mail: lanier.watkins@jhuapl.edu

R. Nair
e-mail: rnair8@jhu.edu

C. Nayak
e-mail: cnayak2@jhu.edu

K. Memon
e-mail: kmemon1@jhu.edu

K.D. Fairbanks
Unaffiliated Contributor, Laurel, MD, USA
e-mail: kevin@fairbanksphd.com

P. Wang
ECpE PowerCyber Lab, Iowa State University, 3231 Coover Hall, Ames, IA 50011, USA
e-mail: pywang@iastate.edu

W.H. Robinson
Security and Fault Tolerance (SAF-T) Research Group, Vanderbilt University, PMB 351824, 2301 Vanderbilt Place, Nashville, TN 37235-1824, USA
e-mail: william.h.robinson@vanderbilt.edu

L. Thames and D. Schaefer (eds.), *Cybersecurity for Industry 4.0*,
Springer Series in Advanced Manufacturing, DOI 10.1007/978-3-319-50660-9_8

updates, special access to ICS backplane devices, or additional software to be installed on the ICS device. In previous work, we have demonstrated that it is feasible to use network traffic and machine learning to remotely infer the typical task cycle periods (i.e., CPU load) for an ABB RTU560 (contains a built-in PLC), even on a lightly loaded network one hop away. We now extend this capability to inferring the presence of anomalous CPU load behavior by introducing a Stuxnet-type threat model (i.e., state-sponsored root-kit) to showcase our prototype's detection ability (i.e., the ability to discern normal baseline states from those introduced by a threat). The main benefits of this approach are that: (1) it requires no additional software to be installed on the ICS devices to communicate with the monitor node, (2) the tool is low maintenance, since there are no software updates or signatures to be continuously installed on each ICS device, and (3) the risk of a centralized network-based monitor node being compromised is lower than if it were host-based software on each ICS device due to a reduced attack surface. Our overall prototype tool implements a graphical user interface (GUI) that can be used to monitor and alert on a small-sized to medium-sized ICS network of IP-based RTUs or PLCs similar to the ABB RTU560.

Keywords SCADA • ICS • Resource usage • Network traffic analysis • Inter-packet spacing • Machine learning

1 Introduction

Supervisory Control and Data Acquisition (SCADA) systems are extensively used in industries to automate the control of and enable the remote monitoring of industrial devices. They are commonly used in such systems as: water treatment and distribution, wastewater collection and treatment, oil and natural gas pipelines, electrical power generation and distribution, wind farms, defense systems, or large communication systems. They can send signals to scattered sites in remote locations over communication channels to retrieve the status of the remote equipment. SCADA systems have the capability to reboot, repair, or replace large numbers of geographically dispersed systems. SCADA systems historically distinguished themselves from other ICS systems by supporting large-scale processes that can include multiple sites and large distances. The signals are sent to data conversion devices such as Remote Terminal Units (RTU), Intelligent Electronic Devices (IED), and Programmable Logic Controllers (PLC). The communications are sent from the data conversion tools to the devices, and the responses, which may be rendered in a Human Machine Interface (HMI), are sent to the operator.

SCADA systems were designed to be robust and easily operated but not necessarily secure. Many users assumed SCADA systems were secure due to physical security, and in most cases, by being isolated from the Internet. Early in the history of SCADA systems, the equipment and software were fairly obscure, and network exposure to the world was limited. Over time, a combination of factors drove vendors to adopt standard information technology (IT) platforms, and SCADA system owners connected their systems to other networks. We have come to know that the devices that are connected to the Internet are vulnerable to both network and host-based attacks, and one of the most dangerous of all threats is the Advanced Persistent Threat.

Advanced Persistent Threat (APT) describes a scenario where well-trained and well-funded hackers develop software that uses multiple attack vectors in order to compromise and control a targeted system while being unnoticed for long periods of time (Tankard 2011). APTs are usually nation-state adversaries. According to (Marble Security 2013), the APT attacks of today are more damaging and stealthier than ever, as evidenced by the theft of advanced U.S. weapons designs (e.g., Patriot missile), money from banks (e.g., $45 M from ATMs in 27 countries), and personal information (e.g., 50 million user passwords). They have the ability to evade many of the tools employed by the defense-in-depth concept such as, firewalls, traditional intrusion detection systems, and anti-virus software.

Due to many major critical infrastructures (CI) being operated through SCADA systems and the recent trend of using open TCP/IP-based networking equipment, APT attacks have become a very relevant threat for cyber-physical networks (Kim et al. 2014). Some of the major managerial weak points in SCADA networks are the connections to vulnerable information technology (IT) systems and the impossibility of determining when an attack has occurred. Malicous software such as Stuxnet and Flame, have demonstrated the validity of this assessment (Kim et al. 2014).

Early on, many network owners were unaware or denied the critical importance of securing SCADA devices. Attacks on SCADA systems have the potential to cause huge losses to the government and private sectors. They can also increase the chances of human fatality, especially the employees who are working in the industrial environments. As government conflicts are slowly moving from traditional (i.e., kinetic) to cyber form, SCADA systems are the primary targets to bring all of the government and industry operated infrastructures down. We have already seen well-known SCADA system attacks in the cases of Stuxnet and BlackEnergy (ICS-CERT 2016-1, ICS-CERT 2016-2).

Stuxnet was one of the most sophisticated and stealthiest worms in existence at the time of its discovery. It specifically targeted the Microsoft Windows operating system and Siemens Step 7 software. It exploited four zero day vulnerabilities to silently sabotage the centrifuges at Natanz nuclear facility in Iran for more than a year. The devices in the power plant were not connected to the Internet, and hence the attackers decided to spread the worms through infected USB drives (Langer 2011). They initially targeted a few companies that were directly related to nuclear power plants. Once the infected USB drives were used, the worms slowly propagated into the network of the nuclear infrastructure and then infected specific cyber physical devices. Stuxnet loaded the malicious payload onto the PLC, but the

PLC's operation seemed to display normal results to the operator via the HMI. This process completely destroyed the centrifuges in the Iranian nuclear infrastructure. The BlackEnergy malware attacked GE's Cimplicity HMI and targeted Ukrainian power companies. It was used in a coordinated attack that caused power outages affecting approximately 225,000 people. Furthermore, the BlackEnergy attacks employed the KillDisk malware to erase and corrupt files on several systems.

Our work focuses on the detection of anomalous behavior in cyber physical devices as caused by threat models based on Stuxnet-like and BlackEnergy-like malware. It implements an inference-based method used to detect anomalous activities in an industrial control system (ICS). To demonstrate the feasibility of our work, we developed an intrusion detection system for ICS, which is essentially a computer (i.e., monitor node) in the network that takes active measurements from each ICS compute node (i.e., RTU, PLC, or IED) connected to the ICS. Currently, the prototype supports active measurements, which are taken by analyzing the ICMP replies from each ICS compute node that results from ICMP pings from the monitor node. The main contributions of our work are: (1) the introduction of a new approach to security for ICS, namely the resource-usage viewpoint of ICS security, (2) the development of a Stuxnet-type threat model for the ABB RTU560, and (3) the development of a working prototype to demonstrate that the resource usage viewpoint of ICS security can be used to detect anomalous behavior in ICS without the use of rules or signatures.

The rest of this chapter explains: advanced persistent threat (Sect. 2), other works that are related to our work (Sect. 3), the resource usage viewpoint of security (Sect. 4), how the ICS device's real-time operating system (RTOS) and CPU are correlated with ICMP network traffic via machine learning (Sect. 5), our threat model (Sect. 6), our test bed (Sect. 7), our experimental evaluation (Sect. 8), a real world case study (Sect. 9), our results (Sect. 10), and our future work (Sect. 11).

2 Advanced Persistent Threat

APTs have a well-defined methodology after the initial reconnaissance (Fig. 1 Mandiant's Attack Lifecycle Model). We list the phases of the Mandiant's Attack Lifecycle Model (Mandiant 2013) as follows: (1) **initial compromise**, (2) **establish foothold**, (3) **escalate privilege**, (4) **internal reconnaissance**, (5) **move laterally**, (6) **maintain presence**, (7) **complete mission**. The initial compromise begins with an initial penetration of the enterprise, most likely via a spear-phishing email that employs a social engineering message, malicious hyperlinks, or infected files. The establish foothold phase starts once the spear-phishing email has resulted in a malicious file being executed and a backdoor being established (i.e., a way for an intruder to send commands remotely). Network traffic may be encrypted or obfuscated to hide potential malicious network traffic signatures. Covert channels

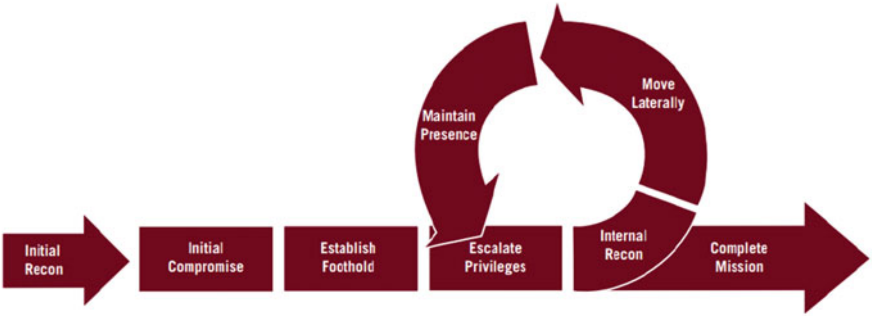


Fig. 1 Mandiant's attack lifecycle model

(Zander et al. 2007) could also be employed. In the next phase (i.e., escalate privilege), attackers try to acquire passwords or other credentials that will provide greater access to the system. Next is the internal reconnaissance phase, where the malware attempts to find potentially interesting targets. The malware attempts to move laterally around the network by using its amassed credentials. It maintains its presence by establishing multiple backdoors and using gathered or manufactured credentials to establish legitimate entry and exit points for the network. Finally, after completing the mission, the attacker archives any files of interest and exfiltrates them.

The Stuxnet and BlackEnergy attacks are good examples of APT malware affecting cyber physical devices. The Stuxnet malware (Langer 2011) sabotaged the Iranian Nuclear Program activities at the Natanz uranium enrichment plant. Most analysts speculate that the initial compromise occurred via an infected removable drive. A foothold was established via multiple exploits, including a Windows Server Service exploit (MS08-073), a Print Spooler Zero Day (MS10-061), and an auto-execute zero-day vulnerability (MS10-046). Privilege escalations occurred using vulnerabilities MS10-073 and MS10-092. Stuxnet was designed to detect and evade anti-virus software using different techniques and to defeat network intrusion detection systems by encrypting and obfuscating its network traffic. The malware then accomplished the lateral movement phase by copying itself to accessible network shares and infecting the WinCC database server using a hardcoded database password. It was able to maintain a presence by infecting the Siemens Step 7 software project files; these files would infect other systems that opened them. Finally, when the malware was able to gain access to a Windows system with access to a Siemens Step 7 PLC, it would install a rootkit to reprogram the software to make the centrifuges operate outside of the acceptable limits and eventually destroy them; this activity allowed the malware to complete its mission (Virvilis et al. 2013), (Falliere et al. 2011). Our Stuxnet-type threat model only emulates the compromised PLC's resource usage aspect of the Complete Mission stage and not the other stages in the APT attack lifecycle.

3 Resource Usage View Point of Security

Generally speaking, the resource usage viewpoint (RUVi) is the concept that information about the resource usage (and thus running processes) of computing devices, with operating systems (OS) that manage shared resources, can be inferred by analyzing the network traffic emitted by the device. In this chapter, we explain how this general concept was leveraged to develop a security paradigm. Further, we illustrate how this security paradigm was used to develop a working prototype, the RUVi of ICS Security. The concepts that birthed this security paradigm were motivated by our previous works with inferring resource usage in: (1) general-purpose nodes (Watkins et al. 2010, 2011 and 2015), (2) mobile devices (Watkins et al. 2013, 2014), and (3) ICS nodes (Lontorfos et al. 2015). The concept of using information leakage extracted from network traffic to remotely ascertain the state of a compute node's hardware (i.e., CPU and memory load, CPU speed, or battery power level) is thoroughly explained in these previous works.

To further illustrate the RUVi, consider Figs. 2 and 3, once the CPU load of a general purpose node reaches approximately 70%, the node becomes too busy, and its network traffic begins to exhibit noticeable delays. This point is evident from the probability distribution function (PDF) for 70%. At this point, the longer tails would dominate in an average of the CPU loads per task and would allow for easy identification of the busy state of the compute node. Note this phenomenon is not dependent on network traffic, as shown in Figs. 2 and 3 and our previous work.

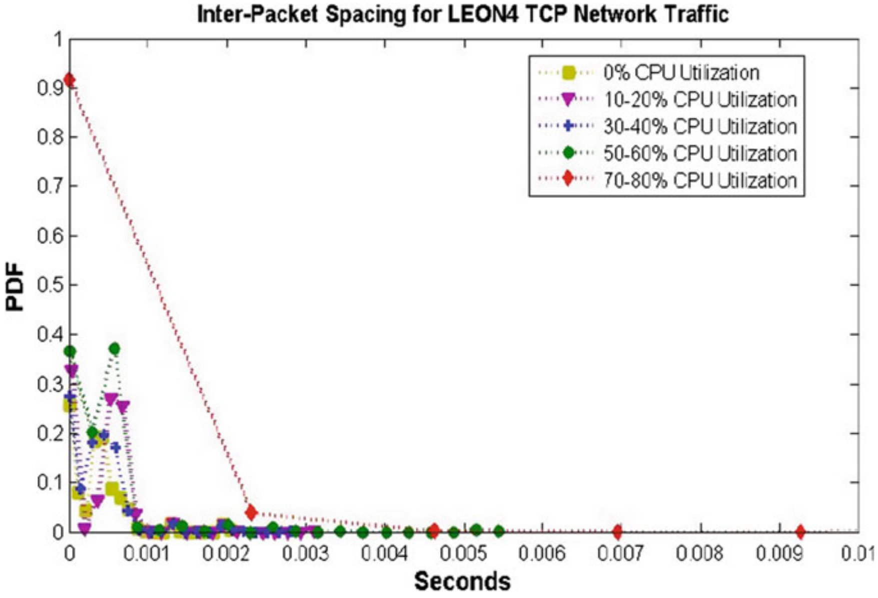


Fig. 2 PDF of TCP/IP inter-packet spacing from a general purpose node

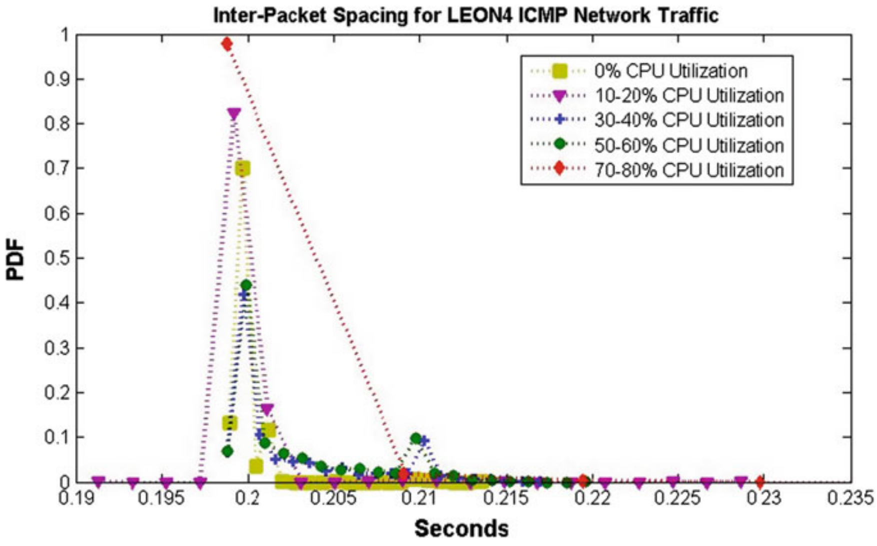


Fig. 3 PDF ICMP inter-packet spacing from a general purpose node

In Watkins et al. (2011), we take advantage of the ability to remotely ascertain the CPU busy state of a general purpose node. We demonstrate that for long running bimodal compute bound workflows in a cluster (See Fig. 4), a novel passive resource discovery algorithm can be developed with low protocol and software maintenance overhead. Because these workflows cause the compute nodes in the cluster to maintain long-running, high CPU loads, it is possible to use this novel resource discovery method to remotely and passively identify free nodes in a message passing interface (MPI) cluster. This concept was further researched in Watkins et al. (2015) and it was determined that the root cause of these detectable delays is the saturation of the cache system in general-purpose nodes due to heavy CPU utilization in the node. This saturation leads to the average cache memory access time increasing to the access time of lower levels of the memory hierarchy (See Figs. 5 and 6). Once this occurs, it takes longer to access memory to send network traffic just as it takes longer to access memory to run applications. We demonstrated that this passive resource discovery algorithm works well for TCP, UDP, and ICMP network traffic in compute bound and memory bound clusters. Note, Fig. 7 illustrates that network traffic emitted from a node with a heavy memory load is discernible from a node with a light memory load. Both of these approaches are limited in that they are only applicable to general-purpose nodes and only able to identify bimodal CPU or memory states, and thus we began to investigate other nodes and eventually other ways of detecting more states.

Watkins et al. (2013) demonstrated that the RUVi concept applies to Android-based mobile devices, showing this approach could be used to remotely determine the type of application executing on a mobile device. In this work, we determined that CPU throttling, which saves battery life by scaling the CPU speed

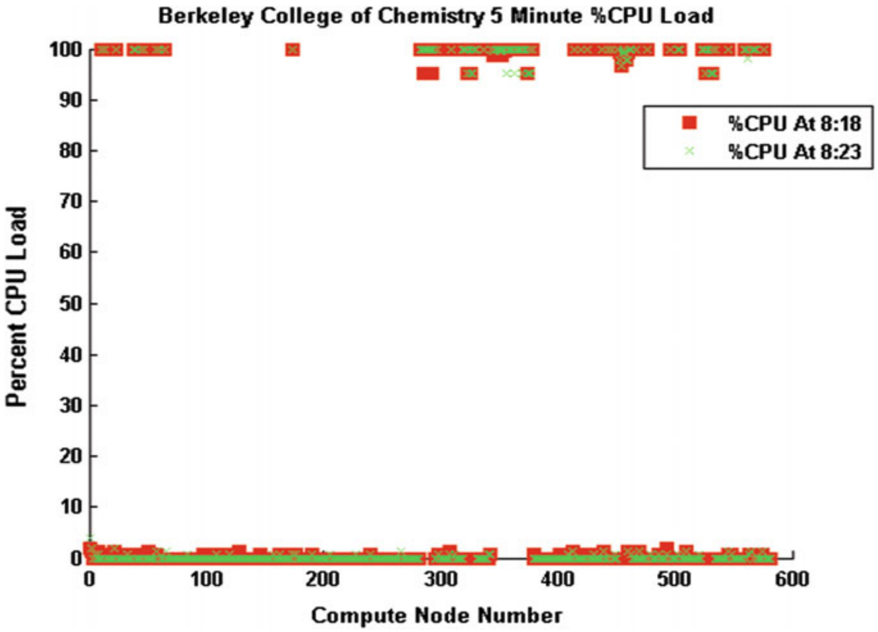


Fig. 4 Berkeley college of chemistry: example of long-running bimodal workload, 5 min duration (Berkeley college rocks cluster 2016)

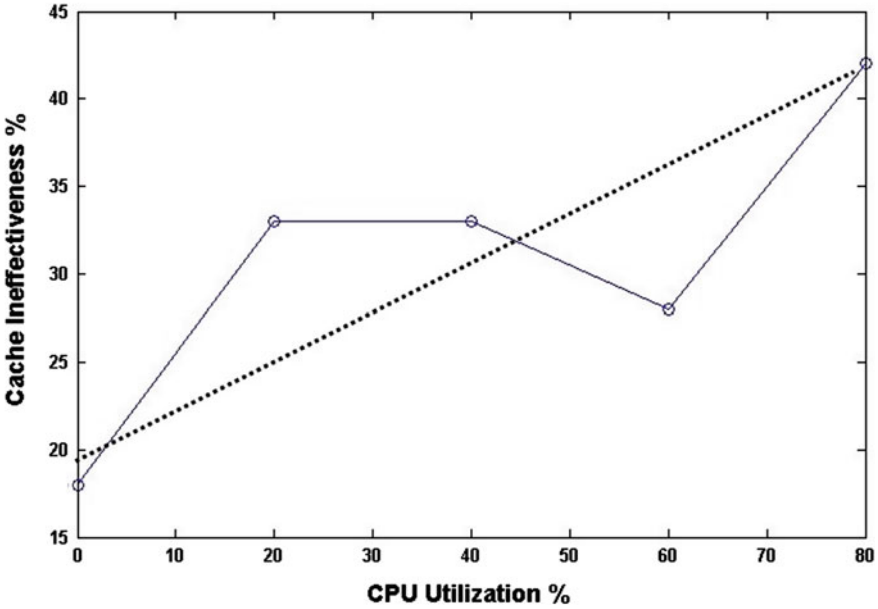


Fig. 5 Cache ineffectiveness as measured while sending ICMP network traffic

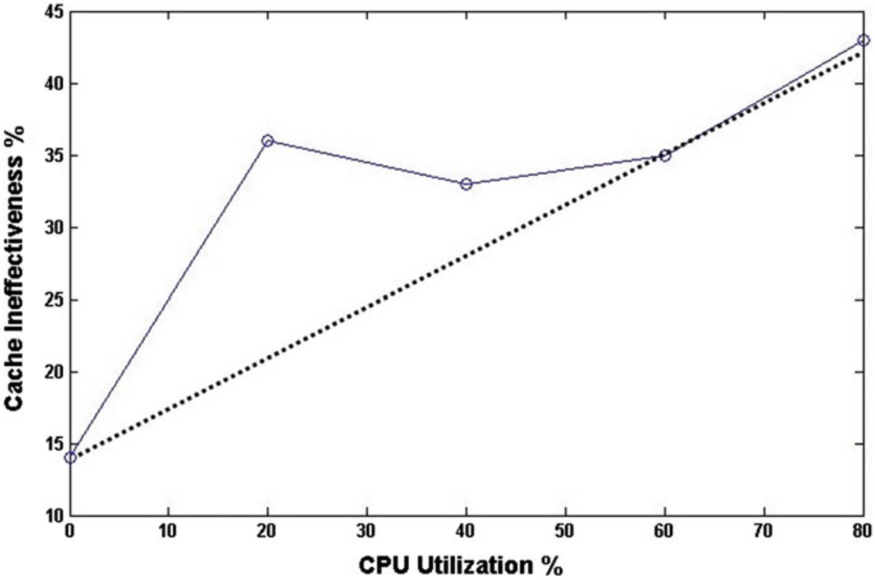


Fig. 6 Cache ineffectiveness as measured while sending TCP network traffic

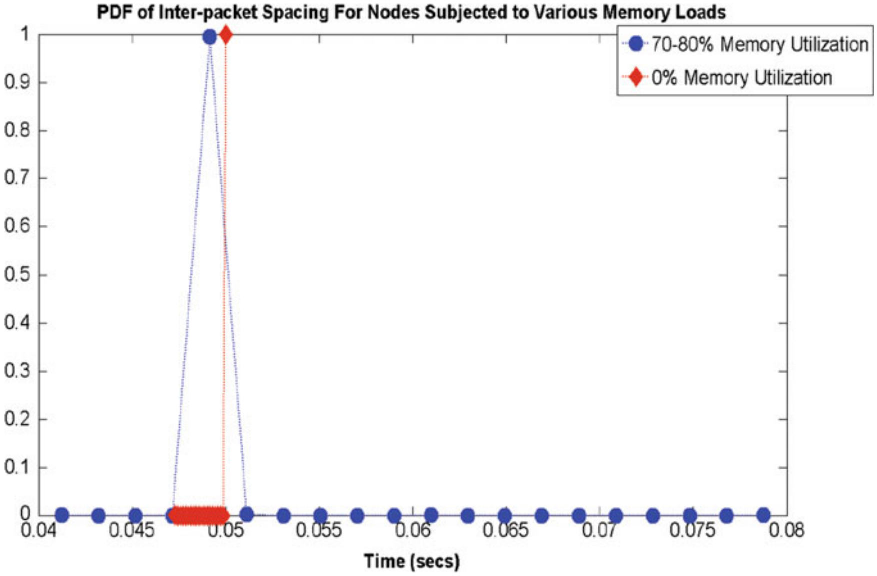


Fig. 7 PDF of TCP/IP network traffic from heavy memory loaded node

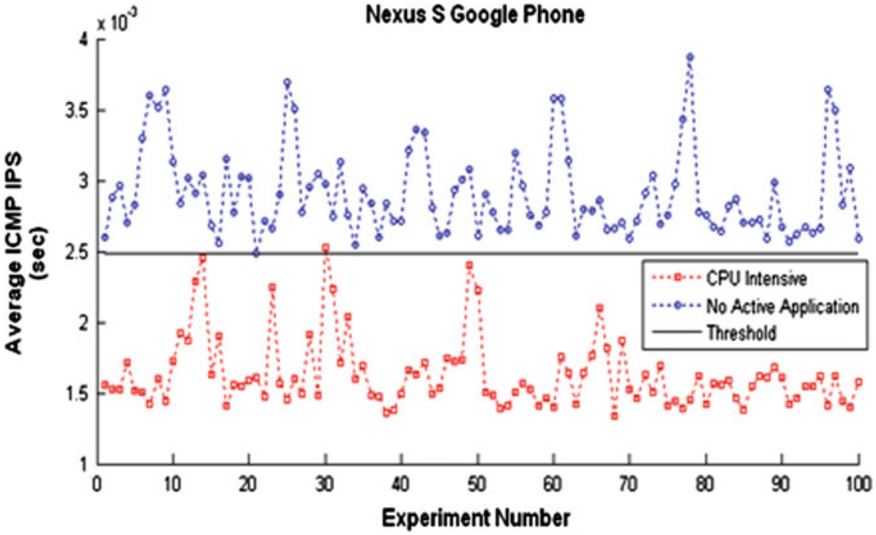


Fig. 8 Effect of mobile device application activity on network traffic

to fit the needs of the mobile application, caused the kernel instructions to be executed faster or slower depending on the speed of the CPU at the time of the interrupt used to preempt the foreground application's processes to send network traffic. This process induces detectable delays into network traffic incident from the mobile node. This point is illustrated in Fig. 8, where almost all of the mobile devices running CPU intensive applications can be distinguished from the mobile devices that are idle.

In Watkins et al. (2014), Matlab was used to emulate the functionality of an energy-aware wireless sensor network where nodes used RUVi theory to determine the energy level of their neighbors by only analyzing network traffic sent by that neighbor, as opposed to requiring each node to periodically send health and status packets. This approach lowers the overhead power expenditure of each node. This savings, coupled with the saving from only choosing the highest energy-level neighbors when forwarding data, increases the overall lifetime of the network. This work demonstrates the feasibility and benefit of using RUVi theory to correlate inter-packet spacing with battery power-level to increase wireless sensor node network lifetime. The correlation between network traffic and battery power levels is illustrated in Table 1.

In Lontorfos et al. (2015), we used RUVi theory to identify multiple CPU states in ICS devices. Our approach was to remotely extract information from a network traffic incident from an ICS device (i.e., ABB RTU560), statistically analyzing this information, and using machine learning to detect multiple CPU states. As illustrated in Fig. 9, there are four intertwined CPU load states for the target cyber-physical node. As described in Algorithm 1, by using a threshold of 51% on the Sensitivity (i.e., the ratio of true positives to the sum of the true positives and the

Table 1 Duty cycle modes and packet send rates

Duty cycle (%)	Energy range	Effective data send rate (Kbps)
100	if $E_{av}(n) \geq 0.84 * E_o(n)$	then $P_s = E_o(n) * 10$ k
35.5	$E_{av} < 0.84 * E_o(n)$ and $\geq 0.68{*}E_o(n)$	$P_s * 0.355$
11.5	$E_{av} < 0.68 * E_o(n)$ and $\geq 0.52{*}\ E_o(n)$	$P_s * 0.115$
7.53	$E_{av} < 0.52 * E_o(n)$ and $\geq 0.36{*}\ E_o(n)$	$P_s * 0.0753$
5.61	$E_{av} < 0.36 * E_o(n)$ and $\geq 0.20{*}\ E_o(n)$	$P_s * 0.0561$
2.22	$E_{av} < 0.20 * E_o(n)$ and $\geq 0.04{*}\ E_o(n)$	$P_s * 0.0222$

$E_{av}(n)$ = available energy, $E_o(n)$ = initial energy, P_s = packet send rate

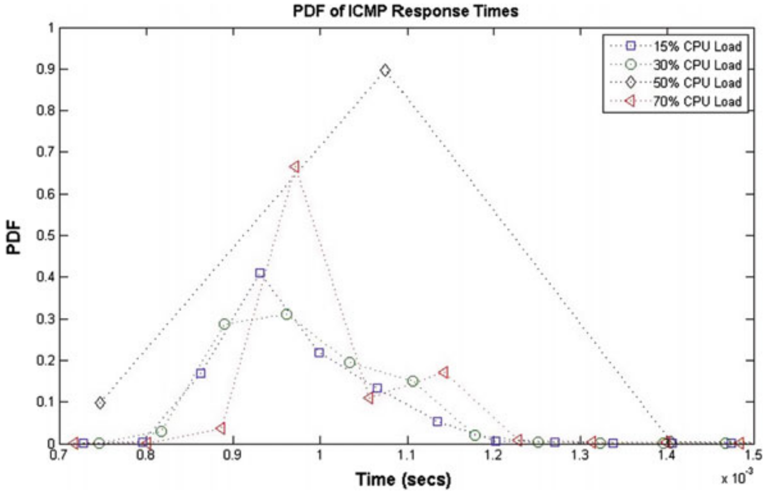


Fig. 9 PDF of ICMP response time

Table 2 Sensitivity Confusion Matrix

		Predicted CPU Load			
		~15%	**~30%**	**~50%**	**~70%**
Actual CPU Load	**~15%**	**65**	29	4	1
	~30%	31	**57**	3	8
	~50%	4	5	**72**	18
	~70%	6	10	21	**62**

false negatives) for each state in the confusion matrix (See Table 2), we demonstrate that we can successfully identify all four of these CPU load states for a cyber-physical node.

Algorithm 1
Input: cmatrix, A confusion matrix
Output: pc, Predicted Load Class. -1 means no conclusive decision

```
var iap_array[4]
//Inter-Arrival Pattern array

iap_array = count(cmatrix)
//count() returns number of patterns per class
//majority() returns class with majority patterns

for each Actual Class do
    if (majority(iap_array) == class_15%)
        pc = 15
    else if (majority(iap_array) == class_30%)
        pc = 30
    else if (majority(iap_array) == class_50%)
        pc = 50
    else if (majority(iap_array) == class_70%)
        pc = 70
    else pc = −1
end for
return pc
```

The previously mentioned works in this section serve as motivation for the usage of RUVi in ICS security. In the previous works, we had not considered using the information leaked into network traffic for the purposes of security; instead, we used this information for resource discovery, identifying mobile applications and the normal states of a cyber-physical device as well as battery power levels. Because there exists solid evidence from our previous work that various CPU load states of a compute node can be remotely extracted from network traffic accurately, we are motivated to apply the concepts of RUVi to the realm of network security in ICS. In doing so, we clearly illustrate the differences in the resource usage viewpoint (RUVi) of security and the traditional viewpoint of security. At the most basic level, the traditional viewpoint of security is based on signatures and rules and most recently on the behavior of application and operating system level events, whereas the RUVi of security focuses on the usage patterns of hardware resources and the use of machine learning to comprehend the complex intertwined states of the hardware resources. Our previous work has shown that other hardware resources, such as memory (Watkins et al. 2010), CPU speed and file input-output (Watkins et al. 2013), and battery power levels (Watkins et al. 2014) may be applicable as well, but in this chapter we focus solely on CPU load. The benefits of this approach are: (1) it does not require software or hardware to be installed on ICS devices, (2) it does not require constant signature updates, and (3) it has the potential to detect Zero Day attacks. The special characteristics of ICS networks lend themselves naturally to our approach, such as: (i) the devices are dedicated to one critical task,

(ii) the devices have a fixed location, (iii) ICS networks have fixed workloads due to fixed task cycle periods of the devices, (iv) the devices have little or no user interaction, (v) ICS networks are typically overprovisioned with excess bandwidth, and (vi) actively scanning ICS network devices can cause them to become overloaded and time critical traffic to be delayed.

In summary, the RUVi for ICS security was motivated by the success of previous work in correlating network traffic and compute node hardware usage behavior, the special characteristics of ICS networks, and the benefits that a novel algorithm based on remotely extracting CPU load information from network traffic provides. The RUVi of ICS Security is the belief that compromised ICS devices can be detected by monitoring the resource usage of ICS devices. This approach does not rely on traditional signatures or rules; instead, it relies on inferring the CPU load for ICS devices, learning the resource usage behavior of the ICS devices while under normal operation, and alerting when this normal resource usage behavior changes. Further, we propose this method as another layer of security in an overall defense-in-depth and not in lieu of defense-in-depth. The RUVi of ICS Security relies on the special properties of ICS networks, such as: (1) the devices are dedicated to one critical task, (2) they have fixed locations, (3) they have fixed workloads (due to fixed task cycle periods), (4) they have little or no user interaction, and (5) they are typically overprovisioned with bandwidth. These special characteristics of ICS networks ensure that there is no congestion on the LANs that contain ICS devices, and the ICS devices only have processes running on them aimed at the physical devices to which they are connected. These two points are critical, because they ensure that ICMP replies are not tainted with network delays and the resulting ICMP replies are indicative of contention inside the ICS device due to the critical functionality we want to protect.

4 Related Work

When considering previous and similar works, one must take into account not only the method used by an intrusion detection system (IDS), but also the location of the intrusion detection system. For most end users the concept of an intrusion detection system is manifested in the form of home or enterprise antivirus software. In general, this software operates in a combination of two methods. The first method, signature detection, works by finding known patterns of activity or known sequences in the executed binary or process memory space. The second method, anomaly detection, works by profiling user and/or system activity and alerting when that activity differs from expected behavior. There are various pros and cons to each general detection method such as the ability to generate signatures and detect activity despite various obfuscation techniques. Also, the ability to classify expected behavior and determine if a monitored behavior is malicious often involves statistical analysis and introduces the possibilities of false positives and false negatives. The rates of these misclassifications must be properly tuned.

If location is the key factor used in classifying an intrusion detection system, then the two major types of intrusion detection systems are host-based and network-based IDSs. The majority of end users are exposed to a form of host-based IDS (HIDS). These systems require a product to be installed directly on the user's system to allow monitoring and detection to occur. Conversely, network-based IDSs (NIDS) are often found in enterprise environments and are not installed on the end user system. NIDS normally operate by observing the network traffic generated and received by one or more hosts. Both of these types of systems may employ anomaly-based detection, signature-based detection, or a combination of the two. Furthermore, enterprises may choose to employ a combination of these systems to provide security in a layered fashion.

Industrial Control Systems have presented a unique challenge when compared to traditional host-based intrusion detection in that the market place is fairly heterogeneous. Unlike home and enterprise computing environments, which are currently dominated by Microsoft Windows and primarily use the x86 or x86_64 architecture, thereby presenting some level of consistency across systems, a SCADA system is highly dependent upon the vendor selected for a component and the operating system that vendor supports. For example, the Intel subsidiary Wind River Systems offers several operating system products, ranging from its proprietary VxWorks to a version of Linux, even extending to virtualization support. When this is coupled with the variety of hardware that an embedded device vendor may choose to use in developing their product, it is not surprising that HIDS options for SCADA systems are not as pervasive as traditional computing environments. However, certain components of a SCADA deployment, such as management systems, may employ traditional computer hardware and software, such as Microsoft Windows, and thus employ one or more of the previously described intrusion detection methods present in a variety of software.

From the standpoint of non-traditional HIDS, (Reed and Gonzalez 2012) proposed using a power fingerprinting (PFP) technique as a form of anomaly detection. In general, a current probe or other power monitoring hardware must be installed on the PLC in question to gather measurements. These measurements are then analyzed to determine if the device is behaving abnormally. Thus PFP can be effective against zero-day attacks. Like the research presented in this chapter, the PFP technique is inferring activity based up a measurement. However, our research differs in that it is not host-based, thus no augmentation must be done to the individual devices.

Mulder et al. (2013) present a different take on HIDS in that a monitoring agent is installed on the backplane of a PLC so that "changes to process control settings, sensor values, module configuration information, firmware updates, and process control program (logic) updates" can be detected through the collection of traffic between PLC modules. Rather than processing the collected data on the PLC, it is exported to a separate system. Since the captured communications are internal to PLC and data processing occurs offline, this system is more analogous to an Enterprise HIDS system that uses monitoring agents to collect and retrieve information from user systems rather than the antivirus protection normally found on consumer systems. This method is similar to the research of Carrier and Grand (2004) for memory acquisition. In that research, volatile memory is captured through the use of additional monitoring hardware inserted into the PCI bus slot of a computer.

Considering network intrusion detection systems, as noted in Zhu and Sastry (2010), several take approaches similar to traditional network intrusion detection systems. These approaches involve the capture and analysis of network traffic. From that point, different techniques can be used to determine if the NIDS should alert an administrator. A well-known traditional example is Snort, which can be setup to search for patterns in network traffic, which constitute a signature, that are typical of a specific or type of attack. These types of systems can also be setup to detect anomalous behavior in the way protocols are used on the monitored network; this includes using different learning techniques to classify the behavior.

Another method taken by NIDS is presented by Yoon and Ciocarlie (2014). Their approach can be classified as a deep packet inspection technique. They decode the ICS traffic to determine if the sequence of commands and data is normal or malicious. This anomaly detection type of NIDS is inherently tightly coupled with the system and the constituent components on which it is deployed. The research presented in this chapter, is similar to both the work of Zhu and Sastry (2010, 2014) in the sense that it uses anomaly detection and is network-based; it differs in that it does directly use the network traffic to determine if the system is under attack and should alert. One attribute that all the NIDS systems take advantage of is the limited behavior of ICS systems. While in traditional systems, especially personal computers, behavior varies widely based upon the actions of the end user(s) and network conditions; ICS and SCADA systems will generally have more predictable behavior based upon the logic being executed.

The most closely related works are those that infer the state of the system based upon the network behavior of different components. In Watkins et al. (2015), the ping tool was used to infer CPU load. It was shown that deviations in the response time could be attributed to latency in memory access times due to increased CPU utilization. While this work focused on a Linux-based system and therefore models a more traditional computing device, it was extended by Lontorfos et al. (2015) to demonstrate that the method could be used on ICS devices. Specifically, the work demonstrated that the load on an ABB RTU560 could be inferred through the application of machine learning algorithms on ICMP reply inter-arrival times. This could then be used to determine the task cycle period and detect unexpected changes to the logic the RTU was executing without the need for actually examining the RTU. While the work in Watkins et al. (2015) and Lontorfos et al. (2015) actively ping the systems being measured, (Formby et al. 2016) presents a method of passively developing fingerprints of ICS devices. The passive nature uses the inter-packet spacing of commands that retrieve data to develop a cyber fingerprint, while the inter-packet spacing of commands that have a physical effect are used to develop a physical fingerprint. This data is then processed using machine learning techniques to classify the measured device. This work differs from our work in that it is passive and based purely on the use of TCP/IP network traffic. Because their work is passive, there is no way for them to control the detection time of their method; instead, the detection time is intrinsically tied to the polling cycle of the network.

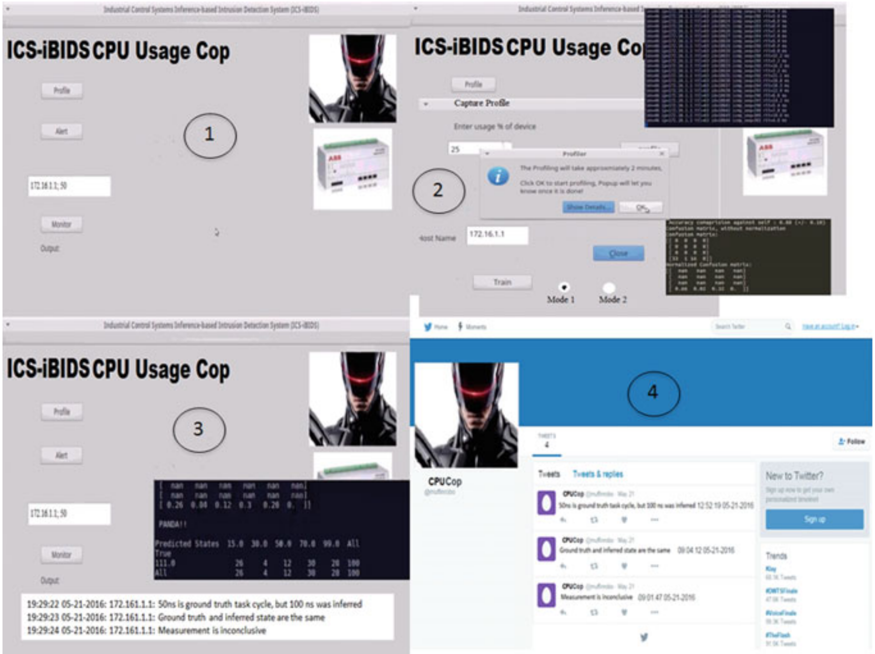
5 RTOS, CPU Load, ICMP Network Traffic, and Machine Learning

Our previous work has established a firm correlation between CPU load, wrapped by the operating system (OS), and network traffic as thoroughly explained early-on in Sect. 3. Further in Sect. 3, we discussed results from using machine learning to correlate the CPU load of an ABB RTU560, running the real-time operating system (RTOS) VxWorks, with ICMP network traffic emitted from it. In this section, we extend this work by developing a threat model and building a working prototype capable of: (1) generating ICS device profiles, (2) monitoring ICS devices, (3) customizing alert text and delivery, and (4) logging events from the tool.

Our tool, the ICS inference-based intrusion detection system (ICS iBIDS) CPU Usage Cop (See Fig. 10), is capable of automatically learning the normal states of the ABB RTU560. Once the normal states are learned, ICS iBIDS can be used to monitor the RTU. There are two modes associated with monitoring the RTU, Mode 1 and Mode 2. Each mode has a different functionality. Mode 1 is meant to detect the standard behavior of the RTU, which exhibits different CPU usages and also the behavior of our threat model. Mode 2 is meant to discern the standard behavior of the RTU from anomalous behavior (i.e., our threat model).

Specifically, Mode 1 uses a Random Forest classifier for identification of several states. The random-forest algorithm (Breiman 2001), (Python Scikit-Learn Random Forest Tree 2016), which was created by Leo Breiman and Adele Cutler, is considered one of the most versatile among classification algorithms for its ability to classify large amounts of data with considerable amounts of accuracy. This algorithm is basically an ensemble learning method wherein many decision trees are generated during training. Multiple “trees” are grown that are used for the classification of an object based on various attributes. Given input data, each tree gives a classification and casts a vote for each class. Since single decision trees are seen to have high variance, the concept of an ensemble of trees or a “forest” balances out such variances.

At the heart of Mode 2 is the support vector machine (SVM) developed by Vladimir Vapnik (Python Scikit-Learn SVM 2016), which is a one-class classifier. This classifier determines whether the currently submitted data fall in the known state or not, where the latter is considered as an aberrant or malicious state. If the



172.16.1.1; 50

25

The Profiling will take approximately 2 minutes,

Click OK to start profiling, Popup will let you know once it is done!

172.16.1.1

● Mode 1 ○ Mode 2

```
Accuracy comparision against self : 0.00 (+/- 0.10)
Confusion matrix, without normalization
Confusion matrix:
[[ 0  0  0  0]
 [ 0  0  0  0]
 [ 0  0  0  0]
 [33  1 34  0]]
Normalized Confusion matrix:
[[  nan   nan   nan   nan]
 [  nan   nan   nan   nan]
 [  nan   nan   nan   nan]
 [ 0.00  0.02  0.32  0.  ]]
```

```
[   nan   nan   nan   nan   nan   nan]
[   nan   nan   nan   nan   nan   nan]
[ 0.26  0.04  0.12  0.3   0.28  0.  ]]

PANDA!!

Predicted States  15.0  30.0  50.0  70.0  99.0  All
True
111.0               26     4    12    30    28  100
All                 26     4    12    30    28  100
```

```
19:29:22 05-21-2016: 172.161.1.1: 50ns is ground truth task cycle, but 100 ns was inferred
19:29:23 05-21-2016: 172.161.1.1: Ground truth and inferred state are the same
19:29:24 05-21-2016: 172.161.1.1: Measurement is inconclusive
```

CPUCop · May 21
50ns is ground truth task cycle, but 100 ns was inferred 12:52:19 05-21-2016

CPUCop · May 21
Ground truth and inferred state are the same 09:04:12 05-21-2016

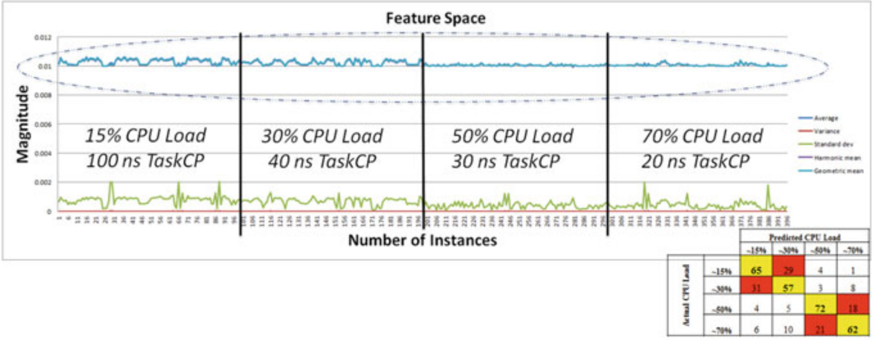
CPUCop · May 21
Measurement is inconclusive 09:01:47 05-21-2016

Fig. 10 (*1*) main screen, (*2*) ICS device profile capture screen with logging results, (*3*) monitor ICS device screen with logging results, (*4*) twitter alert example

output of the scoring function is negative, then the input is classified as belonging to class -1, but if the score is positive, then the input is classified as belonging to class 1. In both training (i.e., profile generation) and testing (i.e., monitoring), the inter-packet spacing (IPS) is calculated from the timestamps of the Layer 1 ICMP replies. Several features are extracted from this time series, such as: (i) mean, (ii) harmonic mean, (iii) geometric mean, (iv) standard deviation, and (v) variance. Then, these features are fed into the machine learning algorithms.

In Mode 1, alerts are generated whenever the RTU is inferred to be in a different state than documented in its profile, or if our threat model's behavior is detected. In Mode 2, alerts are generated whenever the RTU is inferred to be behaving outside of the normal. All of these alerts are delivered via Twitter. Also, all of the results from training during profile generation and testing during monitoring are logged into a time-stamped log file.

At the core of the ICS iBIDS CPU Usage Cop tool is the use of machine learning to correlate the CPU load of a device controlled by an RTOS (i.e., VxWorks) with ICMP network traffic. We now explain the relationship among these four entities by using results from Lontorfos et al. (2015). In the graph in Fig. 11, the feature space for the 396 instances from the accompanying confusion matrix is given. The graph is the number of instances versus the magnitude of the features that are extracted



		Predicted CPU Load			
		~15%	~30%	~50%	~70%
Actual CPU Load	~15%	65	29	4	1
	~30%	31	57	3	8
	~50%	4	5	72	18
	~70%	6	10	21	62

Fig. 11 Using machine learning to correlate CPU load wrapped in an RTOS with ICMP network traffic

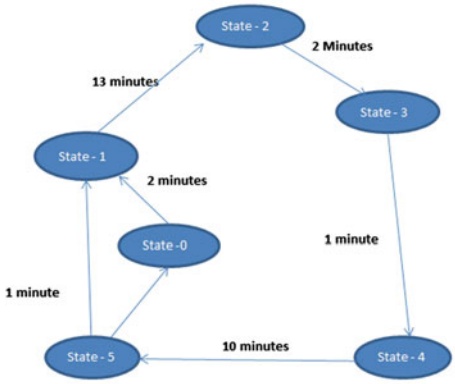
from the ICMP replies of the RTU at four CPU loads. We are only concerned about the top of the graph where the features for the average, harmonic mean, and the geometric mean are circled. Essentially, these features are on top of each other. These three features exhibited the highest information gain (i.e., were the most important in classify the CPU loads).

Note, each point on the graph represents the result of one of the five features for the same time series derived from the ICMP replies at specific CPU loads. Notice that the adjacent instances taken at 15% CPU load exhibit higher entropy than the adjacent instances taken at 70% CPU load. We have not done any experiments to conclusively determine the reasons for this behavior, but our theory is that when the PLC in the ABB RTU560 is active during its 20 ns task cycle period (TaskCP) for 70% CPU load, the RTOS is 5 times as likely to allow an interrupt to send ICMP network traffic through the scheduler than during the 100 ns TaskCP. In layman's terms, the 100 ns task cycle behaves like a long-running process blocking the interrupts from ICMP requests. Thus, some adjacent instances have higher values, which make all of the instances based on ICMP replies captured during 15% CPU load look like a square wave, while all of the instances based on ICMP replies captured during 70% CPU load look more like a straight line. Using this logic, it is easy to see that groups of instances captured at adjacent CPU loads are similar, while those captured at non-adjacent CPU loads are not (i.e., instances captured at 15 and 30% CPU loads are similar while instances captured at 30 and 70% are dissimilar). The confusion matrix in Fig. 11 supports this assessment, since the greatest confusion occurs at adjacent CPU loads. Note, this theory has only been used to visually correlate CPU load, the RTOS, and network traffic, but this approach is not used by the classifier to produce the classifier's results, since 10-fold cross validation was used in these experiments. This means that the order of the instances was necessarily shuffled in accordance to the 10-fold cross validation algorithm, and thus could not have been used to classify the instances.

6 Stuxnet-Type Threat Model

Because of the recent appearance of the Irongate malware, we felt that a Stuxnet-type threat model is representative of current threats in ICS. We developed an emulation of the Stuxnet malware for the ABB RTU560 by using the Asoftech automation tool to automate the five states Stuxnet assumed during its lifecycle at the Natanz nuclear facility in Iran. This approach was motivated by the W32 Stuxnet dossier (Falliere et al. 2011) and Ralph Langner's talk (Langner 2012), which helped with the construction of these events. The CPU load of the ABB RTU 560 was varied by chaining various task cycle frequencies as illustrated in Fig. 12. We used the same vendor-supplied configurations as (Lontorfos et al. 2015) to modify the CPU load of the ABB RTU 560. The state machine depicted in Fig. 12 came directly from Falliere et al. (2011); however, we modified the output such that it only reflects the assumed CPU loads induced by Stuxnet, but none of its malicious activities. To keep the emulation feasible for our experiments, we shrank the timeline on the activities of the original Stuxnet model, which required a period of 27 days. For our emulation, we assumed that one day in the real Stuxnet attack life cycle was equivalent to one minute for the emulation.

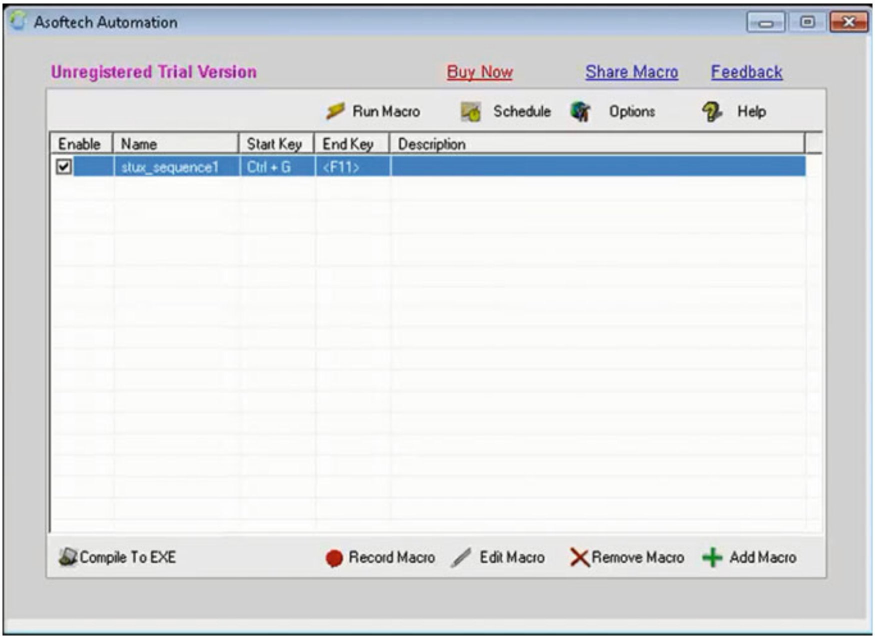
The Asoftech tool was used to replay captured point-and-click actions with pre-programmed timelines in-between them (Fig. 13). These actions were the steps required to impose various CPU loads on the RTU560 such that its behavior was comparable to our interpretation of Stuxnet. Once engaged, the emulation starts with State 1, which has the main objective of emulating the capturing of network traffic to and from the PLC. This is the longest state in the emulation. It takes around 13 min to complete. In the real Stuxnet attack, the first state was responsible for capturing enough data to replay to the PC controlling the PLC so as to make the



Usage	Approximate %
Low	15%
Low-Medium	30%
High-Medium	50%
High	70%

States	Objective	Resulting Device CPU Load/Speed*
State -1	Capture Network Traffic to and from the PLC	Hi-Med to Low
State -2	Wait State	Low
State -3	Manipulation of output values	High-Medium to Low
State -4	Increase/Decrease Frequency of drives	High to Low-Medium*
State -5	Reset of variables	Low-Medium to Low
State -0	Errors/ Catch All	Low

Fig. 12 Stuxnet-type emulation



Enable	Name	Start Key	End Key	Description
☑	stux_sequence1	Ctrl + G	<F11>	

Fig. 13 Asoftech automation application

operator believe that the device was functioning properly. We assumed this state to result in a CPU load that varies from High-medium to low, which is in the range of 50–15% CPU load. After this, the emulation switches to State 2, which is a wait state wherein the state timer starts. This wait state is around two minutes, and the lowest possible CPU level is maintained here. Next is State 3. This state corresponds to Stuxnet replaying captured values from State 1, and this state also suspends the execution of the compromised device's original PLC code in order to allow for the execution of State 4, which is the malicious PLC activity. The CPU usage induced here is between High to Low-Medium, which is approximately in the 70–30% range. State 4 is the most pivotal state for the execution of malicious activities, because the PLC is forced to increase the frequency of the centrifuge from safe operation at 1,064 Hz to extremely fast speeds at 1,410 Hz or extremely slow speeds at 2 Hz every 15 min, which introduced unsafe rotation speeds for the nuclear facility. This unauthorized activity damaged the nuclear centrifuges over a period of time. Stuxnet then switches to State 5, which is a reset state that sets global variables back to default states and transitions the flow back to State 1. We assume that State 5 has a low-medium to low CPU Usage. In case there are errors during State 5 or any other states, the flow transitions to State 0, which is a catch-all state where Stuxnet would wait for 5 h and move forward to State 1. We assume that State 0 would induce a low or negligible CPU load; however, we do not actually use this state in our emulation.

7 The PowerCyber Smartgrid Test-Bed

The PowerCyber test-bed at Iowa State University is a cyber-in-the-loop and hardware-in-the-loop smart grid security test-bed built with the explicit goal of providing an accurate representation of the cyber and physical environment of the bulk power system (Hahn et al. 2013). This goal is accomplished by including the relevant smart grid control, communication, and physical system components. These components are a combination of real, emulated, and simulated devices such that realistic cyber and physical environment results can be obtained (See Fig. 14).

The control aspects of the PowerCyber test-bed are separated into the: (1) Control Center and the (2) Substations. The control center is outfitted with SCADA functions, which includes measurement collection, field device statuses, operator forwarding commands, and historical data management. These functions are supported via Human Machine Interfaces (HMIs). These control operations focus on human-in-the-loop or protection (i.e., intelligent electronic devices (IEDs) can be configured to transmit their status and detect faults in their neighbors) approaches. The focus of the SCADA communications is between the SCADA servers and the software-based remote terminal units (RTU) in the substations. This communication provides the status of the substation's devices every second and displays this status via HMI. The substations interface with the power system simulations, which consist of both RTUs and IEDs. Substations are modeled as virtualized substations connected to virtual IEDs modeled by the power system simulators, or dedicated RTUs connected to physical IEDs (i.e., overcurrent protection relays).

The communications aspects include both physical network architecture and network protocols. A wide area network (WAN) is used to connect the control center and substations. The distributed network protocol (DNP3) protocol is used in conjunction with VPNs for added security for WAN network traffic. The PowerCyber test-bed is also connected to the Internet-Scale Event and Attack Generation Environment (ISE-AGE), which offers large cyber infrastructure modeling, network collection, and

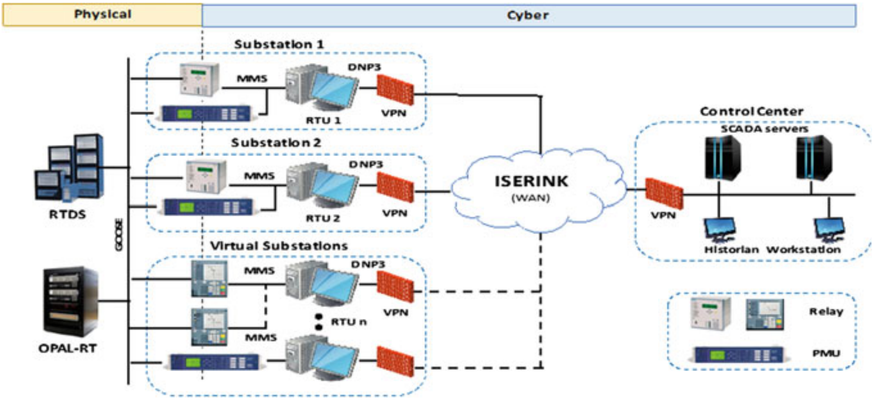


Fig. 14 The PowerCyber SmartGrid testbed at Iowa state university

coordinated attack simulation. The International Electrotechnical Commission's (IEC) 61850 protocol is used within the substations to communicate between IEDs and RTUs. The manufacturing message specification (MMS) protocols are used to communicate analog and binary values between the IEDs and RTUs.

Finally, three different and independent tools for power system simulation are used, the DIgSILENT PowerFactory, Opal-RT, and the real-time digital simulator (RTDS). The testbed supports wide-area protection (Remedial Action Scheme) and wide-area control algorithm (Automatic Generation Control) on WECC 9-bus and IEEE 30-bus model systems for cyber attack-defense experimentation. RTDS and Opal-RT perform real-time power system simulation with physical hardware integration. In contrast, DIgSILENT PowerFactory is a non-real-time power system simulation and does not provide physical hardware integration.

In future work, we plan to implement a host-based threat model for the intelligent devices in the PowerCyber smartgrid test-bed to further test the detection ability of our iBIDS tool. In Sect. 9, our case study, we discuss Mode 1 testing of iBIDS on an actual IED from the PowerCyber smartgrid test-bed.

8 Experimental Evaluation

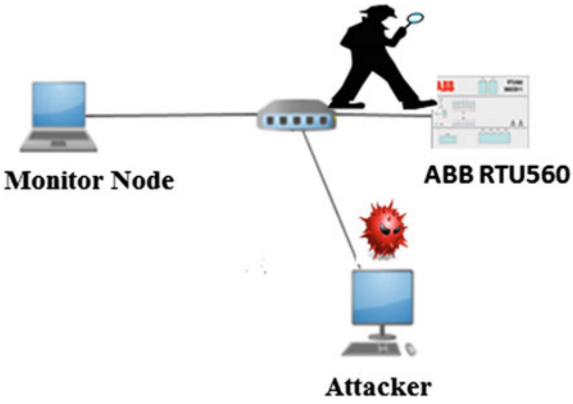
8.1 Experimental Setup

The experimental setup (Fig. 15) consists of: (1) an ABB RTU560 running on firmware version 11.2, on VxWorks 6.9.4.1., (2) two Intel Core i5-based laptops, one running a Linux virtual machine that hosts the ICS iBIDS tool and the other running the Asoftech automation tool that is used to manage the Stuxnet emulation, and (3) one switch. The ICS iBIDS tool was developed using Python and Python Scikit-Learn machine learning algorithms. The ABB RTU560 has a built-in software PLC. The Stuxnet emulation uses PLC code supplied by the vendor that simulates PLC activity by having it read its inputs at specific task cycle frequencies and perform CPU intensive calculations to induce the CPU loads 15, 40, 50, and 70%, then we chained together these CPU loads using the Asoftech tool to produce CPU loads we assumed to be indicative of Stuxnet. The experimental setup is essentially a local area network (LAN) that connects the monitor node (running the iBIDS tool) and the threat model emulation to the ABB RTU560 via Ethernet.

8.2 Experimental Procedure

The experimental procedure explains research done to test both modes of operation for the iBIDS tool. In Mode 1, the iBIDS tool monitors the ABB RTU560 looking for specific normal states, whereas in Mode 2, the iBIDS tool monitors the ABB RTU560 for anomalous behavior.

Fig. 15 Experimental setup



We investigate the detection ability of the ICS-iBIDS CPU Usage Cop tool by:

(1) creating profiles for 20, 30, 40, 100 ns task cycle periods (corresponding CPU loads are 70, 50, 40 and 15%), and the Stuxnet emulation, see Fig. 10, Screen #2. This entails training both a support vector machine (SVM) and a random forest trees machine learning algorithm using features extracted from the ICMP replies of the ABB RTU560 while subjected to the above mentioned CPU loads and the Stuxnet emulation. This allows the iBIDS tool to operate in both Mode 1 and Mode 2, which is the functionality to recognize the individual normal states of the ABB RTU560 and the Stuxnet emulation and to identify when the ABB RTU560 is behaving anomalously.

(2) testing the Mode 1 functionality of the iBIDS tool by monitoring the ABB RTU560 to determine if the iBIDS tool can accurately identify the normal states of the ABB RTU560 and the Stuxnet emulation. The ABB RTU560 was monitored by pinging it 10,000 times, calculating the inter-packet spacing from ICMP reply packet time stamps, extracting features from the inter-packet spacing, and testing the trained random forest trees algorithm on the features taken from 100 vector measurements (each vector containing 100 inter-packet spacing elements). As in Algorithm 1 taken from Lontorfos et al. (2015), the iBIDS tool bases its detection decision on the class where the majority of the test measurement instances get placed after the machine learning algorithm has concluded.

(3) testing the Mode 2 functionality of the iBIDS tool by monitoring the ABB RTU560 to determine if the iBIDS tool can accurately identify anomalous behavior in the ABB RTU560. The ABB RTU560 was monitored by pinging it 20,000 times, calculating the inter-packet spacing from reply packet time stamps, extracting features from the ICMP inter-packet spacing, and testing the trained SVM algorithm on the features taken from 100 vector measurements.

(4) observing Twitter to verify that when the ABB RTU560 is in a different normal state than expected or when anomalous behavior occurs, the proper alerts are tweeted.

9 Case Study: Discerning Between the Normal States of Intelligent Electronic Devices (IED) in Smartgrids

In this case study we describe how our RUVi of ICS security can be applied to a real-world application. This is done by using the equipment from the PowerCyber Smartgrid test bed located at Iowa State University and our iBIDS tool.

Before we describe our experimental approach, we discuss the high-level operation of a SCADA-based smartgrid. In smartgrids (i.e., power systems), SCADA systems are used to regularly send process data between the control center and devices in substations such as RTUs, PLCs, and IEDs. Normally, a control center oversees many power plants and substations within a region. Within substations are the RTUs, which are tasked with serving as an intermediary between the control center and the PLCs and IEDs or actuators. These PLCs and IEDs interact with devices in the physical world. When commands from the control center arrive at the RTU, these commands are relayed to the intended actuator. For example, when the operator in the control center wants to open a breaker controlled by Relay #1 in Substation #1, he will send the trip command to RTU #1 in Substation #1, and RTU #1 will forward this command to Relay #1 to open the breaker under its control.

The experiments described in Sect. 8 were performed using the ABB RTU560 on a LAN in our laboratory; however, in this section, we use the iBIDS tool with Wireshark captures (i.e., pcap files) of a Siemens IED (on the PowerCyber smartgrid at Iowa State University) pinged 10,000 times while it was at Level 1 (i.e., in overcurrent protection mode), and then another 10,000 times while it was at Level 2 (i.e., in both overcurrent and distance protection mode). Both of these modes correspond to normal states of the IED with different CPU loads. Since creating a profile for an ICS device using iBIDS is simply creating a directory and taking a Wireshark capture of the target ICS device being pinged, we copied the Wireshark captures from the IED from the PowerCyber smartgrid into a profile and a monitoring directory for a Siemens IED. Then, we placed the iBIDS tool in Mode 1 and slightly altered it to train a random forest trees machine learning algorithm on half of the data and to monitor the Siemens IED by testing on the other half of the Wireshark capture. Because 70% (i.e., 35/50) of the Level 1 and 82% (i.e., 41/50) of the Level 2 measurements were properly classified (See Fig. 19), the iBIDS tool, per Algorithm 1, correctly recognizes the individual normal states of the Siemens IED when only running in overcurrent protection mode or both overcurrent and distance protection mode. This functionality could be useful in detecting a malicious insider who wants to sabotage a smartgrid by changing the IED from an authorized normal state to an unauthorized normal state. In future work, we will develop a relevant threat model for the Siemens IED and evaluate the ability of iBIDS to detect anomalous behavior from this device while attached to the smartgrid.

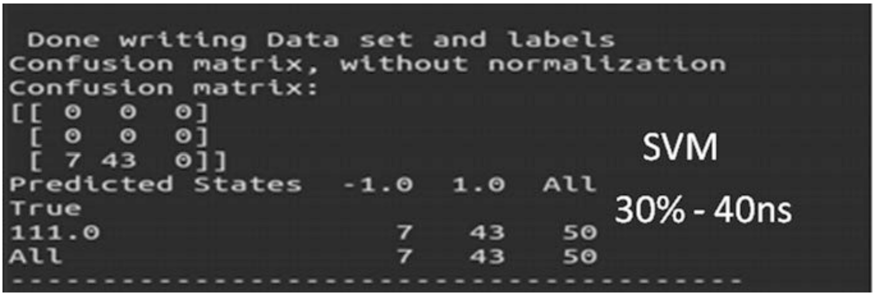
10 Results and Discussion

The ICS iBIDS prototype is an extension of the work done in Lontorfos et al. (2015). Our prototype automates all of the steps from Lontorfos et al. (2015) such that it is capable of profiling the normal states of the ABB RTU560 and monitoring with Mode 1 functionality. The work presented in this chapter introduces: (1) automated ICS device profiling and training, (2) a Stuxnet-type threat model, (3) Mode 2 monitoring, (4) customizable alert messages and alert delivery via twitter, and (5) logging of the ICS iBIDS prototype system events. We provide screen shots of the ICS iBIDS prototype to illustrate the functionality of device profiling and training, Mode 1 monitoring, alert customization and alert delivery, and system event logging. We include a clear explanation of our threat model in Sect. 6 and in this section we provide results and discuss detection of our threat model under Mode 2 functionality. Only results from Mode 2 (i.e., SVM results) are illustrated and discussed in this chapter, because the results for Mode 1 mirror the results presented in previous work done in Lontorfos et al. (2015). The results in Table 3 and Fig. 16 illustrate that the ICS iBIDS prototype running the SVM machine learning algorithm can be used to accurately detect normal and anomalous behavior in ICS devices. In Sect. 8, the experimental setup and procedures used are described. While trained on the normal states of the ABB RTU560 (i.e., task cycle periods of 100, 40, 30 and 20 ns), the SVM machine learning algorithm used by the ICS iBIDS prototype is capable of accurately inferring the anomalous behavior of the RTU when the Stuxnet-type threat model is executing and a sufficient amount of network traffic has been captured during monitoring. This point is illustrated in Figs. 17 and 18. We have also determined that the amount of measurement data is critical for achieving acceptable accuracy with the ICS iBIDS prototype. In future work, we will investigate the relationship between measurement network traffic and accuracy. Also, based on the initial results in our case study, it may be possible to use our current ICS iBIDS prototype in a working smartgrid to monitor ICS devices for transitions to unauthorized normal states, see Fig. 19. In future work, more experiments will be done on the PowerCyber test bed to ensure that these results are repeatable.

Table 3 Detecting anomalous behavior (SVM one class algorithm)

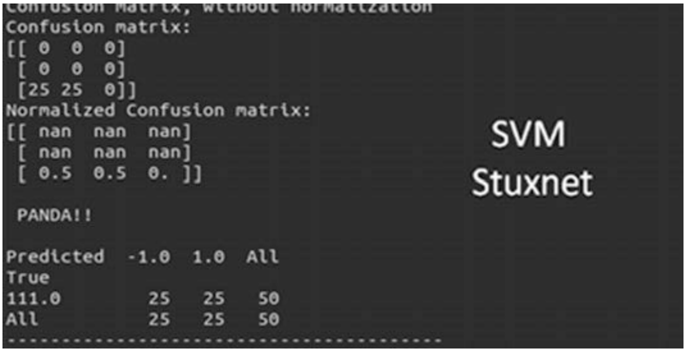
CPU load/TaskCP	Detection decision	False positive/negative
15%—100 ns	Normal	No
30%—40 ns	Normal	No
50%—30 ns	Normal	No
70%—20 ns	Normal	No
Stuxnet	Abnormal*	No

*The larger the data capture window (i.e., more instances) the better performance



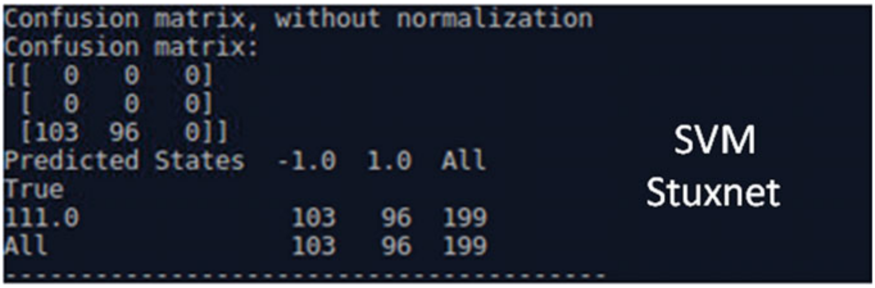
```
 Done writing Data set and labels
Confusion matrix, without normalization
Confusion matrix:
[[ 0  0  0]
 [ 0  0  0]
 [ 7 43  0]]
Predicted States   -1.0  1.0  All
True
111.0                 7   43   50
All                   7   43   50
-------------------------------------
```

Fig. 16 SVM results for one normal state (30% CPU load or 40 ns task cycle period)



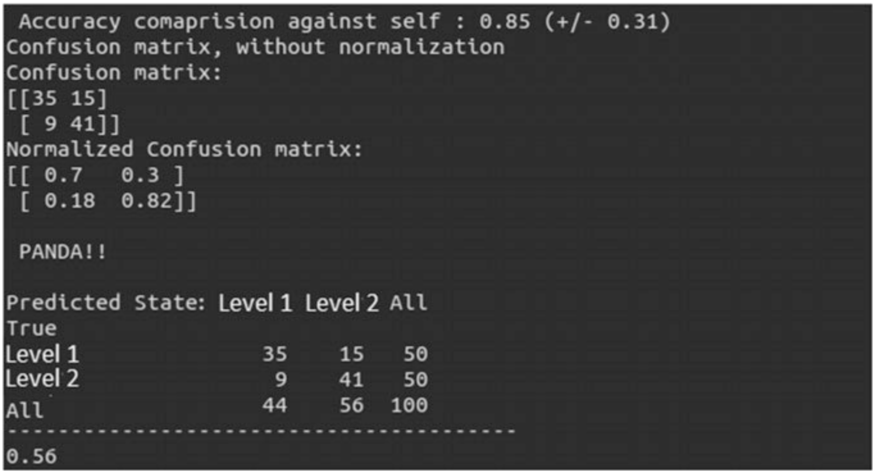
```
Confusion matrix, without normalization
Confusion matrix:
[[ 0  0  0]
 [ 0  0  0]
 [25 25  0]]
Normalized Confusion matrix:
[[ nan  nan  nan]
 [ nan  nan  nan]
 [ 0.5  0.5  0. ]]

 PANDA!!

Predicted  -1.0  1.0  All
True
111.0        25   25   50
All          25   25   50
-------------------------------------
```

Fig. 17 Failed SVM Stuxnet detection for 50 measurement instances



```
Confusion matrix, without normalization
Confusion matrix:
[[  0   0   0]
 [  0   0   0]
 [103  96   0]]
Predicted States  -1.0  1.0  All
True
111.0              103   96  199
All                103   96  199
----------------------------------------
```

Fig. 18 Successful SVM Stuxnet detection for ~200 measurement instances



```
 Accuracy comaprision against self : 0.85 (+/- 0.31)
Confusion matrix, without normalization
Confusion matrix:
[[35 15]
 [ 9 41]]
Normalized Confusion matrix:
[[ 0.7   0.3 ]
 [ 0.18  0.82]]

 PANDA!!

Predicted State: Level 1 Level 2 All
True
Level 1              35     15    50
Level 2               9     41    50
All                  44     56   100
------------------------------------
0.56
```

Fig. 19 Discerning between overcurrent protection and a combination of overcurrent protection and distance protection

11 Summary and Future Work

Our previous work in investigating information leakage in general-purpose, mobile, wireless sensor, and ICS nodes formed the basis of the RUVi of ICS security. This work demonstrated that useful CPU, memory, I/O, and battery power resource usage information can be extracted from the network traffic emitted by various compute node and used to develop applications. Interestingly enough, the processes that are currently running on the nodes drive the resource usages; thus, by using network traffic to infer resource usage, insight into currently running application activity can be gained. We decided to investigate the use of the RUVi of ICS security, because of the special properties of ICS networks, such as: (1) the devices are dedicated to one critical task, (2) they have fixed locations, (3) they have fixed workloads (due to fixed task cycle periods), (4) they have little or no user interaction, and (5) they are typically overprovisioned with bandwidth. Basically, since ICS networks are likely predictable for most tasks, a security framework can be developed by building a normal resource usage behavior profile, continuously monitoring ICS nodes, and using machine learning to identify deviations from normal resource usage.

This framework is the RUVi of ICS security and our ICS iBIDS prototype is the manifestation of this theoretical security framework. This prototype has four basic functions, which include: capturing ICS node profiles, monitoring ICS nodes, alerting on anomalous ICS node behavior, and logging prototype events for trouble shooting. The profile creation functionality of our prototype: captures network traffic, extracts features from the network traffic, and trains machine learning algorithms on normal resource usage patterns for a given ICS node. The monitoring functionality has two modes, Mode 1 and Mode 2. In Mode 1, the prototype monitors ICS nodes for unauthorized transitions to other normal operating states. In Mode 2, the prototype monitors ICS nodes for anomalous behavior. In both modes, we utilize the threat model to test the detection ability of the prototype. In Mode 1, we monitor ICS nodes to determine if they exhibit behavior indicative of the threat model; whereas in Mode 2, the prototype monitors ICS nodes to determine if the ICS nodes exhibit behavior other than that of the specific learned normal states. If the prototype infers the presence of the threat model, an unauthorized normal state, or an anomalous resource usage, then it alerts the user by tweeting a custom alert message to a specified twitter account. Lastly, the prototype writes the events that occur during its operation to a log file for trouble-shooting or later inspection.

In future work, we will investigate the accuracy of detecting the threat model as a function of node monitoring time as well as a function of profile capture time. Also, we plan to implement a host-based threat model for the other intelligent devices in the PowerCyber smartgrid test bed to further test the detection ability of our iBIDS prototype. Finally, we will enhance the prototype with the capability to make passive measurements using the existing TCP/IP network traffic emitted from the intelligent devices in ICS networks. This would give our prototype the ability to validate its measurements using both ICMP and TCP/IP network traffic, but also maintain its ability to manage its detection time, which is a property that related work done by Formby et al. (2016) does not have.

Acknowledgements I would like to thank and acknowledge Dr. Manimaran Govindarasu, Mehl Professor in the Department of Electrical and Computer Engineering at Iowa State University and his students for assisting and allowing my students at the Johns Hopkins University Information Security Institute access to the PowerCyber Smartgrid Testbed.

Lanier Watkins

Research Scientist, Johns Hopkins University Info. Security Institute, USA

References

Berkeley college of chemistry rocks cluster website August 2016. http://dino.cchem.berkeley.edu/ganglia/addons/rocks/top.php?c=College%20of%20Chemistry&sortby=HOST&sortorder=down

Breiman L (2001) Random Forests Mach Learn 45(1):5–32

Carrier BD, Grand J (2004) A hardware-based memory acquisition procedure for digital investigations. Digit Invest 1(1):50–60

Falliere N, Murchu LO, Chien E (2011) W32. stuxnet dossier. White paper, Symantec Corp., Security. Response 5:6

Formby D, Srinivasan P, Leonard A, Rogers J, Beyah R (2016) Who’s in control of your control system? Device fingerprinting for cyber-physical systems. In: Feb NDSS

Hahn A, Ashok A, Sridhar S, Govindarasu M (2013) Cyber-physical security testbeds: architecture, application, and evaluation for smart grid. IEEE Trans Smart Grid 4(2):847–855

ICS-CERT (2016-1) Alert (IR-ALERT-H-16-056-01) Cyber-attack against Ukrainian critical infrastructure. https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

ICS-CERT (2016-2). Alert (ICS-ALERT-14-281-01E) Ongoing sophisticated malware campaign compromising ICS (Update E). https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B

Kim SJ, Cho DE, Yeo SS (2014) Secure model against APT in m-connected SCADA network. Int J Distrib Sens Netw

Langner R (2011) Stuxnet: dissecting a cyberwarfare weapon. IEEE Secur Priv 9(3):49–51

Langner R (2012) Stuxnet deep dive. https://vimeopro.com/s42012/s4-2012/video/35806770

Lontorfos G, Fairbanks KD, Watkins L, Robinson WH (2015) Remotely inferring device manipulation of industrial control systems via network behavior. In: 2015 IEEE 40th local computer networks conference workshops (LCN workshops). IEEE, (pp 603–610).

Mandiant APT (2013) Exposing one of China's cyber espionage units. available from intelreport. mandiant. com/Mandiant_APT1_Report. pdf

Marble Security (2013) Protecting mobile device users from advanced persistent threats. Information week, August 19th, 2013

Mulder J, Schwartz M, Berg M, Van Houten JR, Urrea JM, King MA, Clements A, Jacob J (2013) WeaselBoard: zero-day exploit detection for programmable logic controllers. Sandia report SAND2013-8274, Sandia national laboratories

Python Scikit-learn SVM website August 2016. http://scikit-learn.org/stable/modules/svm.html

Python Scikit-learn random forest tree website August 2016. http://scikit-learn.org/stable/modules/generated/sklearn.ensemble.RandomForestRegressor.html

Reed JH, Gonzalez CRA (2012) Enhancing smart grid cyber security using power fingerprinting: integrity assessment and intrusion detection. In: Future of instrumentation international workshop (FIIW) 2012. IEEE, (pp 1–3)

Tankard C (2011) Advanced persistent threats and how to monitor and deter them. Netw Secur 2011(8):16–19

Virvilis N, Gritzalis D (2013) The big four-what we did wrong in advanced persistent threat detection? In: 2013 eighth international conference on availability, reliability and security (ARES). IEEE, (pp 248–254)

Watkins L, Robinson WH, Beyah R (2015) Using network traffic to infer hardware state: A kernel-level investigation. ACM Trans Embed Comput Syst (TECS) 14(3):55

Watkins L, Robinson WH, Beyah R (2011) A passive solution to the CPU resource discovery problem in cluster grid networks. IEEE Trans Parallel Distrib Syst 22(12):2000–2007

Watkins L, Robinson WH, Beyah R (2010) A passive solution to the memory resource discovery problem in computational clusters. IEEE Trans Netw Serv Manage 7(4):218–230

Watkins L, Corbett C, Salazar B, Fairbanks K, Robinson WH (2013) Using network traffic to remotely identify the type of applications executing on mobile devices. Mobile Secur Technol (MoST)

Watkins L, Crosby GV, Sharmin A (2014) Using network traffic to infer power levels in wireless sensor nodes. In: 2014 international conference on computing, networking and communications (ICNC). IEEE, (pp 864–870).

Yoon MK, Ciocarlie GF (2014) Communication pattern monitoring: improving the utility of anomaly detection for industrial control systems. InNDSS workshop on security of emerging networking technologies

Zander S, Armitage G, Branch P (2007) A survey of covert channels and countermeasures in computer network protocols. IEEE Commun Surveys Tutorials 9(3):44–57

Zhu B, Sastry S (2010) SCADA-specific intrusion detection/prevention systems: a survey and taxonomy. In: Proceedings of the 1st workshop on secure control systems (SCS)

Practical Security Aspects of the Internet of Things

Jörn Mehnen, Hongmei He, Stefano Tedeschi and Nikolaos Tapoglou

Abstract Industry 4.0 and with that the Internet of Things (IoT) are expected to revolutionize the industrial world. The vast amount of interconnected devices bear the great opportunity to collect valuable information for advancing decision making in management and technology to improve through-life management of a product. Cyber-physical systems and the Internet of Services will revolutionize our current world through fully interconnected communication where information and services are becoming ubiquitous. The availability of information across a system of systems can be very powerful when utilized properly and harnessed adequately. The vast network of small, power-sensitive and often deeply embedded devices that are streaming potentially commercially sensitive data over long periods of time poses an entirely different type of threat than known from the conventional PC world. Adequate and sensible measures need to be taken right at the design stage of IoT devices in order to take best advantage of Industry 4.0 technology. This chapter introduces a set of key security issues related to the implementation of IoT in an industrial mechanical engineering context. A real-world example concerning remote maintenance of CNC machine tools illustrates the different threat scenarios related to IoT in practice. The paper touches on Big Data and Cloud Manufacturing but will remain focused on improving security at the Edge of IoT, i.e. where data is collected, transmitted and eventually transferred back to the physical actuators. The aim of this chapter is to introduce a generic overview of real-world IoT security

J. Mehnen (✉)
University of Strathclyde, Glasgow G1 1XJ, UK
e-mail: jorn.mehnen@strath.ac.uk

H. He · S. Tedeschi
Cranfield University, Cranfield, Bedfordshire MK43 0AL, UK
e-mail: h.he@cranfield.ac.uk

S. Tedeschi
e-mail: s.tedeschi@cranfield.ac.uk

N. Tapoglou
AMRC with Boeing University of Sheffield, Advanced Manufacturing Park, Wallis Way, Catcliffe, Rotherham S60 5TZ, UK
e-mail: n.tapoglou@amrc.co.uk

L. Thames and D. Schaefer (eds.), *Cybersecurity for Industry 4.0*,
Springer Series in Advanced Manufacturing, DOI 10.1007/978-3-319-50660-9_9

issues as well as giving a deeper technical example-supported insight into practical considerations for designing IoT systems for practical use in business.

Keywords IoT security • Industry 4.0 • Remote maintenance of CNC machines

1 Introduction

The term "Industry 4.0", though not very well defined yet, is used to describe in broad terms the move from the third Industrial Revolution or Digital Revolution, which encompasses the change from mechanical, and electronic technology to digital technology, to the fourth Industrial Revolution which covers the world of Cyber-Physical Systems, the Internet of Things and the Internet of Services (Kang et al. 2016). All three aspects of Industry 4.0 are hinging on secure communication. Hence, it is of utmost importance that business can utilize the opportunities that the Internet offers in a secure, confident, agile and prosperous way. Business needs to be equipped with the knowledge about the capabilities and limitations and potential risks the Cyberspace poses to fully exploit the rich opportunities of the digital era. Cyberattacks continue to create a Tier 1 risk. This has been expressed clearly in the National Security Risk Assessment of 2015 (UK Government 2015).

Security helps improving trust, collaboration, individual industrial competitive advantage and even maintaining national security and individual safety. Industry 4.0 requires maintaining strict access to confidential data as well as to digital services and physical processes that are linked to complex cyber-physical systems that can control whole factories at a physical as well as at the decisions level. Fast and agile security measures that are able to adapt to the quickly changing attack strategies in Cyberspace need to be in place to make Industry 4.0 work efficiently now and in the long term future.

The intention of this chapter is to address the concerns of industry which is trying to adopt IoT to secure new business opportunities. Section 2 of this chapter introduces generic security threats related to industrial IoT. Section 3 of this chapter discusses a practical real-world example with the intention to demonstrate the generic security topics from Sect. 2 in a practical mechanical engineering environment. Section 4 summarizes the previous sections and draws further conclusions.

2 IoT Security Threats

In an Industry 4.0 context, communication cannot be treated as an isolated process anymore. Systems are getting increasingly interconnected and this trend will continue also in the future. Readily available information at every level will be expected by managers as well as by the people on the ground who are running and maintaining machines. Systems that may have been designed with the intention to be entirely isolated may, at a later stage, get connected to other systems to utilize their power more efficiently at a global level. For example, the connection of well-tested though isolated legacy systems with new and advancing services through the Internet can help retaining these useful legacy systems instead of making them obsolete. Systems—and particularly IoT systems—should be designed right from the start with the option to integrate them with other systems at any time in a well-controlled and comparatively easy and smooth way.

Industry 4.0 technology utilizes the Internet of Things to facilitate the concept of Cyber-Physical Systems (CPS) that offers new business opportunities through the Internet of Services. In the manufacturing domain, the Internet of Services is also known as Cloud Manufacturing (Li and Mehnen 2013). The concept of Servitization (Raddats et al. 2016; Huxtable and Schaefer 2016) introduces a new business approach where the conventional approach of selling a product is replaced by providing a service to a customer while the product itself often remains property of the manufacturer. This approach introduces new challenges to the manufacturer because the associated new availability contract schemes leave the manufacturer with the Through-Life service tasks which cover the whole life span of a product from its design and manufacture, over its repair, maintenance or overhaul to its final recycle or disposal. In this scenario, the Internet of Things can help in various aspects. Real-time data can be gathered for example for product and process monitoring purposes. Large amounts of data can be streamed together to form Big Data (Pääkkönen and Pakkala 2015) that can be exploited at a higher level, for example to support strategic condition based maintenance decisions based on thorough Big Data analytics or as feedback into design and manufacture. IoT can also help in converting the analytical decisions made in the Cloud into automated actions that influence processes and product utilization actively.

2.1 Top Security Issues in IoT Systems

The increasing use of the Internet and mobile devices means that the hard boundaries of enterprises are disappearing and, as a result, the risk landscape is increasing. IoT enabled Cyber-Physical Systems (CPS) are facing vulnerabilities and threats from the Internet (He et al. 2016). This has attracted the attention from researcher. For example, the European project E-CRIME (2016) provided a cyber-crime inventory and networks in non-ICT sectors. It has shown that the cause of system interference can range from viruses, worms, Trojan horses, software bombs, disrupting computer services, Denial of Computer Services to sabotage.

Advanced manufacturing systems are not secure like traditional systems. Cybersecurity has become a critical challenge in IoT enabled CPS, which could be threatened by a wide variety of cyber-attacks ranging from criminals and terrorists to hacktivists. As a consequence, Cybersecurity is critical for the success of Smart Manufacturing. Cyber-threats to the Industrial IoT are real, global and growing, including theft of trade secrets and intellectual property, hostile alterations to data, and disruptions or denial of process control (Albert 2015). The public is becoming increasingly aware of the potential security threats caused by the malicious exploitation of poorly secured systems.

A distinct feature of Smart Manufacturing is that the manufacturing processes are connected to the suppliers through the Internet. Suppliers will have increased visibility of material consumption on the plant floor and can replenish stock just-in-time. Pervasive visibility and proactive replenishment are the two major benefits of IoT to the Manufacturing Supply Chain (NN 2016). However, organisations or enterprises within a connected supply chain will have different levels of security. A determined aggressor, e.g. an Advanced Persistent Threat (APT), usually identifies the organisation with the weakest cybersecurity within the supply chain and uses these vulnerabilities to gain access to other members of the supply chain. The smaller organisations within a supply chain, due to more limited resources, often have the weakest cybersecurity arrangements (CERT-UK 2015) (Fig. 1).

It is estimated that the number of connected devices will increase to 40 billion by 2020 (Baxter 2016). A huge number of connected devices (including sensors) will produce a huge amount of data. The data flow across all levels of the information exchange throughout the whole IoT infrastructure can potentially be open to vulnerabilities. Therefore, data protection and privacy is one of IoT priority challenges (Chen 2012).

IoT is where the Internet meets the physical world. This has some serious implications on security as the attack threat moves from manipulating information to controlling actuation. Consequently, it drastically expands the attack surface from known threats and known devices to additional security threats of new devices, protocols and work-flows. Many manufacturing systems are moving from closed systems (e.g. SCADA, Modbus, CIP) into IP-based Cyber-Physical Systems. This further expands the attack surface. Figure 2 shows the evolution from a legitimate Industry Control System (ICS) to a modern ICS. Cybersecurity risks are

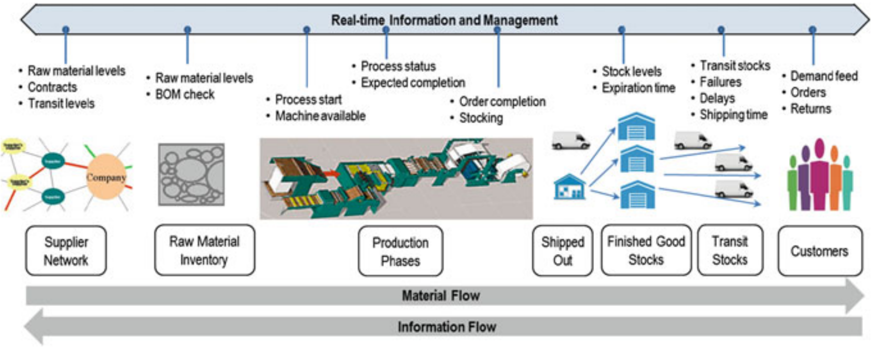


Fig. 1 IoT manufacturing supply chain (redrawn after NN 2016)

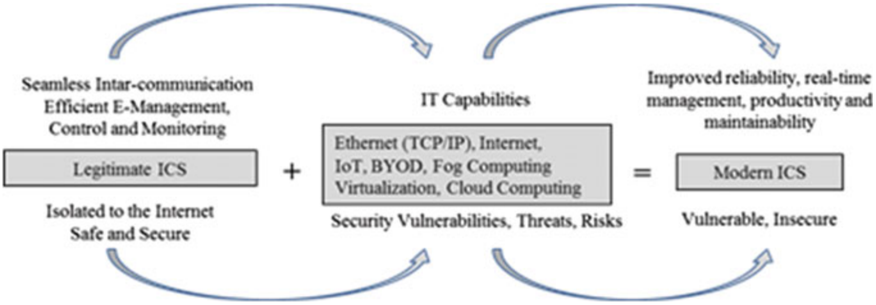

Seamless Intar-communication
Efficient E-Management,
Control and Monitoring
Legitimate ICS
Isolated to the Internet
Safe and Secure
+
IT Capabilities
Ethernet (TCP/IP), Internet,
IoT, BYOD, Fog Computing
Virtualization, Cloud Computing
Security Vulnerabilities, Threats, Risks
=
Improved reliability, real-time
management, productivity and
maintainability
Modern ICS
Vulnerable, Insecure

Fig. 2 Evolutions from legitimate ICS to modern ICS (redrawn after He et al. 2016)

brought to the modern ICS while a legitimate ICS is incorporated with IT capacity. The state of vulnerability is exacerbated by the fact that a legitimate ICS uses typically older equipment and is not yet well-secured against modern networked environments (Korolov 2016). This is because the components of a traditional ICS are communicating with specific protocols often without any security concern. Therefore, the big challenge is how to protect legitimate ICS from attacks when they are connected to the Internet.

2.2 *The Architecture of IoT Systems*

Considering the different areas of applications of IoT, one can, in general, divide IoT security issues into different areas which are either related to the fundamental IoT technical architecture and communication threats, the IoT application (threats from the environment, data flow and final use of data), or threats cause by IoT users (threats human interaction). It is also possible to divide IoT threats into logical (the use of data and meta-data and decision making), software threats and physical (hardware) threats. The categorization of IoT threats is closely related to the architectural structure of IoT and the use of IoT devices and its data.

Figure 3 shows the general IoT architecture as a multi-tiered hierarchical structure. The lowest level contains input and output devices—this level is often called the Edge. The second lowest level is the level where data is collected and processed but not sent into the Internet yet. Communication between devices at this level is generally referred to as Machine-to-Machine (M2M) communication. The third level concerns the transmission of data into the Internet and up into the related Cloud services. The highest level offers high level compute and/or memory intensive Cloud Services and Apps for either directly decision support or data storage and data exchange. Information can usually flow freely within this stack.

The Edge level itself can be further subdivided. The lowest tier of that level starts with the basic sensors or actuators which generally do not come with any particular intelligence per se. A simple data receiving and preprocessing device may

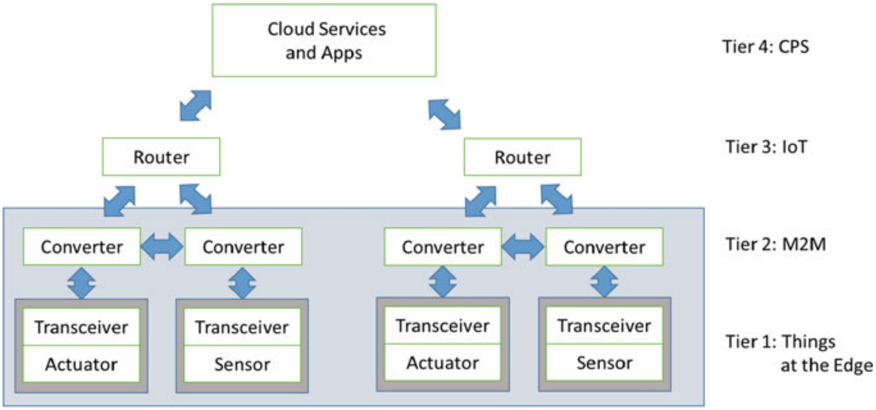


Fig. 3 IoT stack architecture

add additional basic intelligence to the sensor or actuator. An attached transceiver sends data from the intelligent sensor to an Internet connected element, for example a router. An additional transceiver may add an optional level for converting data protocols or switching between data communication technologies (e.g. Bluetooth to WiFi or NRF and LiFi and vice versa). This level is the typical domain of M2M communication which does not necessarily include any Internet connection. However, also this layer shall be considered in the following as an integral part of IoT. The approach of making IoT agnostic to the physical and transport layer protocols used by devices concept has been referred to as the Web of Things (WoT) (Guinard and Trifa 2016). Figure 3 shows the complete IoT stack including the detailed Edge.

2.3 *Security Issues in the IoT Stack*

Considering IoT security, one should consider the allover Internet protocol security down to the Edge. Concerning IoT security at Tier 3 and above only would imply ignoring any potential IoT security issues that are coming directly from the data generation and preprocessing levels. Security levels at Tier 3 and above are typically well-developed as these levels use conventional Internet technology. Security technology and threats at these levels are well understood and supported by agreed standards and controlled through strict regulations.

In the IoT world, however, several consortia such as AllJoyn, Thread, Open Interconnect Consortium (OCI) or the Industrial Internet Consortium (IIC) are developing (partially competing) IoT standards. At the communication/transport layer there are also various standards such as ISA100.11a, IEEE 802.15.4, NFC, ANT, Bluetooth, Eddystone, ZigBee, EnOcean, or WiMax. All these standards offer different levels and schemata for implementing security. Typical security standards in IoT—which are also used in the wider Internet—are the Open Trust Protocol (OTrP) and X.509 with the latter being the most popular standard for Public Key Infrastructure (PKI) management using digital certificates and public-key encryption.

Security issues at the top two tiers of the IoT stack are typically addressed through Internet security measures which apply to the conventional Internet world. As this is well-discussed in literature, in the following only the two lowest tiers of the IoT stack will be discussed in more detail to highlight especially potential security threats at the IoT Edge.

2.3.1 Threats at the IoT Edge

Threats to security at the Tier 1 and Tier 2 level, i.e. security issues at the sensor, transceiver and converter layer level can be divided into security threats (Shahri and Ismail 2012; Di and Smith 2007) caused by

(A) humans,
(B) technical insufficiencies, and
(C) physical attacks of the actual IoT hardware.

Examples for Class A threats at the IoT level, i.e. security issues caused deliberately or involuntarily by humans considering sensors, communication, and data exchange are:

- Data entry errors or omissions
- Improper use or disposal of sensitive data
- Improper use and electronic setup of equipment
- Inadvertent acts or carelessness
- Ignorance of warnings and errors
- Ignorance due to the low cost of the equipment (“throwaway mentality”)
- Underestimation of technological complexity
- Insufficient password management
- Procedural violation
- Espionage and eavesdropping
- Impersonation and identity theft
- Shoulder surfing, i.e. the deliberate attempt to gain access to protected information through observation
- High level data analytics can reveal hidden information

Examples for Class B threats due to internal technical issues, i.e. software and hardware issues, are:

- Compromising emanations, i.e. unintentional data-related or intelligence-bearing signals, which, if intercepted and analyzed, could disclose sensitive information that is transmitted and/or processed

- Corruption by system errors or system failures
- Data and system contamination, i.e. the intermixing of data of different sensitivity levels can lead to an accidental or intentional violation of data integrity
- Insertion of malicious code or software
- Poor programming styles and habits
- Insufficient authentication methods (weak cryptography due to limited power, memory and speed of the Edge devices; weak random number generators)
- Misrepresentation of identity or authorization
- Insufficient and irregular firmware updates
- Data overload and improper error handling (poor Quality of Service)
- Inadequately managed and operated equipment that is mostly dormant
- Exploitation of network flaws (connections and data protocols)
- Power failures
- Obsolescence and system inconsistencies over time
- Inconsistent or changing communication protocols

Class C deal with attacks on hardware and communication through physical means. Examples of Class C issues are:

- Physical tampering with the hardware, i.e. unauthorized physical modification or alteration of equipment in a manner that degrades the security functionality of the asset
- Electromagnetic attacks through electromagnetic interference (EMI) to impact the signal transmission or the device electronics directly causing interruptions in the electronic operation of the system
- Introduction of detrimental environmental conditions, i.e. inadequate humidity or temperature causing the circuits to malfunction or deliberatively degrade or age quickly
- Introduction of hazardous materials which are flammable, oxidizing or combustible, explosive, corrosive, an irritant or radioactive
- Mechanical attacks (cutting of cables, ripping, breaking, bending)
- Deliberate power fluctuation, low power or power spikes
- Side channel attacks (timing attack, power-analysis attack, electromagnetic attack) (Di-Battista et al. 2010; Kim et al. 2015)

Different to conventional Internet and PC technology, IoT devices are often embedded and hard to reach. Ideally, IoT devices are virtually invisible and working unnoticed over long periods of time while requiring minimal maintenance and external energy. IoT devices are susceptible to security issues due to their need for constant power supply, their limited memory size as well as potentially inadequate firmware updates and maintenance.

Regular integrity scans such as virus detections are much harder to achieve in IoT networks than in the PC world due to the limited electrical and computational power of the device. Secure authorization in IoT devices is of special importance as it guarantees legitimate access to the device for servicing and data access. For very power and memory limited IoT devices even authentication can become a serious issue as reliable cryptographic methods require power and memory. The use of poor pseudo number generators can compromise authentication and cryptographic exchange of data across the network.

The large number of IoT devices and their connectivity opens a potentially large attack surface. Re-organization of IoT networks, structures and data protocols and changing users with changing authorization rights require a strict and continuous maintenance of the IoT network already at the lowest levels. A single breach into one device can create a broad scale attack if many devices are following the same inadequate security setup.

A simple change of ownership of equipment containing embedded IoT devices can cause the leaking of potentially sensitive information to the new owner of the device. With the introduction of the EU General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679 enters application in May 2018), this risk will require serious consideration by the liable OEMs.

The physical attack of the IoT hardware itself with regards to tempering or destruction is hardly mentioned in the literature. However, the physical Edge of IoT is very vulnerable to physical attacks as it is exposed to either physical degradation over time or active physical attacks. This holds for many IoT devices, from wearables to sensors that are embedded in industrial tools or military applications. Relying on the correctness of the data from these devices can be crucial. Important decisions, jobs and even lives can depend on the reliability of the communication. Physical protection of the devices is a research topic that concerns design, manufacture, programming, installation as well as the maintenance of the devices. Adding security as an "afterthought" to an existing design has the potential to be inadequate or causing long term issues that can become expensive or even dangerous. Hence, designing IoT devices right from the start with security in mind becomes an imperative that cannot be overlooked. Lessons learned from the current Internet and PC world can certainly help building new IoT technology that is reliable, safe and secure.

2.4 IoT Communication Technology

The current typical data communication protocols and techniques available for the IoT stack between the Internet, local area networks, individual machines, transceivers, sensors and actuators are summarized in Table 1.

The choice of the best technology depends on the application and its requirements. This concerns communication speed, the distance any data can be sent reliably, memory requirements, data processing and transmission power and the required security level. Another practical issue to be considered is the physical environment (electrical noise) as well as the ease of installation, use and maintenance. The management of a large number of devices with their individual identification, authentication and management can become a challenge in IoT as well. Some protocols such as WiFi and ZigBee offer identification, authentication and

Table 1 Technical aspects of IoT device communication

Mode	Technology	Protocols
Internet	WiFi, ethernet, cloud	SHTML, MQTT, XMPP, TLS/SSL, CoAP, AMQP, Mihini/M3DA, DDS, REST, SOAP, websockets, OPC UA
M2M	Wifi, bluetooth, Xbee various NRF techniques, LiFi, laser, infrared, sound (e.g. ultrasound), direct wire connection	SHTML, HTML, MQTT, XMPP-IoT, TLS/SSL, CoAP, AMQP, MQTT-SN, Mihini/M3DA, DDS, LWM2M, REST, SOAP, websocket, reactive streams
Sensor/transceiver/actuator	Mainly direct wire. In case of a detached modular combinations (see also Fig. 5) any of the M2M options are applicable	Plain secure wire communication; otherwise see above

build-in data security, while other technologies such as Near Radio Frequency (NRF), point-to-point laser communication, LiFi (Light Fidelity, i.e. communication via light), basic infrared communication or sound often do not offer these features by default.

Data transport protocols such as SHTML and TLS (Dierks and Rescorla 2008) offer current best secure data communication modes based on authentication and keys. Bluetooth builds on authentication through pairing. However, Bluetooth is not immune to Denial of Service (DoS) attacks and hence an appropriate IoT software design is required to minimize any such risks. Bluetooth data is typically encrypted by default to minimize eavesdropping, however, issues have been reported around in low-energy variants of Bluetooth models (Zhang et al. 2011).

Popular protocols for Internet data exchange in IoT are REST (Representational State Transfer), SOAP (Simple Object Access Protocol), CoAP (Constrained Application Protocol) and MQTT and AMQP (both OASIS standards for light weight Internet/IoT), XMPP-IoT (Extensible Messaging and Presence Protocol) or LWM2M (Lightweight M2M). These protocols co-exist with several other protocols and also next to less flexible proprietary direct peer-to-peer data exchange protocols depending on the communication technique adopted. OPC UA is an international standard for connecting devices on the plant floor with well-developed interfaces to the Internet and Cloud services providing a unified standard for user authentication and authorization, auditability and availability. OPC UA is also the recommended standard of secure connectivity in the Reference Architecture Model Industry 4.0 (RAMI4.0) (VDI/VDE 2016).

REST is used in local networks or across the Internet. REST uses standardized HTTP verbs (GET, POST, PUT, DELETE, etc.) to send data or request data packages from web resources identified by Uniform Resource Identifiers (URI). RESTful implementations make use of standards such as HTTP, URL, JSON, and XML for a structured data exchange. REST like SOAP are not secure protocols per se. Security comes through other secure communication layers such as TLS, direct data encryption or Wi-Fi Protected Access (WPA) or through the implementation as in the case of Reactive Streams (Java/JavaScript).

MQTT (Message Queuing Telemetry Transport) was initially designed for oil pipeline maintenance through satellite communication. MQTT is an open data exchange protocol (OASIS standard since 2014, Banks and Gupta 2015) which is becoming increasingly popular in the IoT community due to its various light weight (i.e. small code size) implementations provided in many computer languages. It offers high data exchange speed and little overhead. MQTT supports scalability to manage very large numbers of IoT modules. MQTT requires a central data broker to which many clients can subscribe to receive messages related to topics that have been published on the broker by other clients. Clients can identify themselves at the broker through passwords. With respect to security, MQTT relies mainly on the security coming from underlying communication layers or the security offered by the application. Exchanged data is by default not encrypted but the MQTT payload can, of course, be encrypted. A major advantage of MQTT is the adjustable Quality of Service (QoS) that guarantee that messages reception can been acknowledged. This can be of particular interest for example in a TES manufacturing environment where e.g. information of machine downtime may need to be recorded reliably for contract reasons.

The enterprise-level Advanced Message Queuing Protocol AMQP (ISO/IEC 19464) provides a platform-agnostic method for ensuring information safe transport between applications and among organizations. Notable users of AMQP come from areas such as the financial sector, US Department of Homeland Security or operating systems. The framing and protocol definitions for security layers in AMQP are expected to be defined externally as in the case of TLS. An exception to this is the SASL (Melnikov and Zeilenga 2006) security layer which depends on its host protocol to provide framing.

The Cloud can provide a means to automate complex decision processes through secure Cloud computing services. When based on IoT technology, these services employ a variety of technologies that can process large amounts of data in a massively parallel way. Data may stream into these services at a continuous and rapid speed or at long time intervals when the device is dormant to save power. IoT means connecting systems with systems. Hence, one has to design IoT systems for a mix of different data speeds and data types. Devices and services with a variety of different properties and demands need to be managed in parallel using services that employ techniques such as asynchronous “lazy evaluation” (e.g. used in Node.js, Wilson 2013) in a non-halting manner to deal with different speeds of responses from the services to minimize waiting time for the service requesting clients. While this can be a challenge in itself, authentication and secure data exchange between the highest and the lowest IoT levels need to be maintained throughout the complex network of devices and services.

In contrast to the conventional PC world, where the communication is typically comparatively stable and error free; this might not be the case with IoT devices and their networks. IoT networks should to be designed with robustness against communication errors in mind. Due to the simple characteristics of the basic sensors in IoT systems communication errors are more likely. Noisy data should not be misinterpreted as attacks. Tunneling solutions that improve software security can potentially get confused or work less efficient if they are overloaded by erroneous data due to poor communication channels or deeply embedded or poorly designed IoT devices.

3 Technical Example: Remote Maintenance of Machine Tools

Remote maintenance of machine tools requires reliable and safe communication from machine to machine and from the machine to the services that offer decision making support through the Cloud. Remote maintenance also requires a secure route for the information back to the machine tool and the human where the decisions are automatically actuated or manually executed.

3.1 IoT Remote Maintenance Architecture

In the context of this section, remote maintenance of machine tools will be regarded as all tasks that cover machine tool monitoring, data analysis for through-life service support and the actuation of any maintenance of the machine tool. Through-life service support for machine maintenance deals with machine performance and failure prediction of individual machine tools and machine tool components and globally interconnected machine tool assemblies. Through-life service support also covers maintenance support through dashboards and rule based decisions support considering the whole-life performance of a machine tool.

IoT serves remote maintenance through sensor networks, advanced data analytics, visualization as well as, if requested, active automated or semi-automated maintenance services that help extending the life of a machine tool. A particularly attractive aspect of IoT is that this technology can be applied not only to existing new machine tools but also to upgrade older (in the following called "legacy") machine tools that are typically not well Internet enabled. Advancing legacy machines through IoT into the age of Industry 4.0 is not only attractive to industry as a technological means to maintain legacy machines but also to retain and upgrade existing and often very expensive equipment. IoT also offers the advantage that young machine tool operators can enjoy the quality of interaction with machines that a new generation of workers and technicians would be expecting after experiencing modern smart communication technology such as smart phones and tablets.

In this section an example of remote machine tool maintenance is presented that looks into security issues related to IoT sensors deployed in machine tools, the secure data transfer into the Cloud and secure data transfer back to the level of IoT actuators on the machine. Figure 4 illustrates the general setup of a possible IoT supported remote maintenance architecture for machine tools. In this setup, intelligent sensors and actuator units (see also Fig. 5) are embedded in the machine. The flexibility of small though powerful intelligent IoT Units and their application inside the machine tool makes the application of IoT technology a lot easier and more convenient than the use of large IoT devices. The setup in Fig. 4 can be applied to both, modern as well as legacy machines. Information from existing data interfaces directly from the machine tool such as MTconnect® or data from industrial ERP, PLM and Manufacturing Execution Systems (MES) can be augmented with Big Data from secure Cloud Services.

IoT security has to be considered especially in industrial networks where data security is associated with company integrity but also directly with safety on the plant floor. In a machine tool, IoT devices can get exposed to very harsh environments. Corrosive liquids, destructive heat and vibrations can be the source of device degradation and the sometimes intense electrical noise coming from the drives or the spindle can cause communication issues. Interception of data about machine performance and machine availability can be harmful to the reputation and competitiveness of a company. Unauthorized use or manipulation of IoT devices

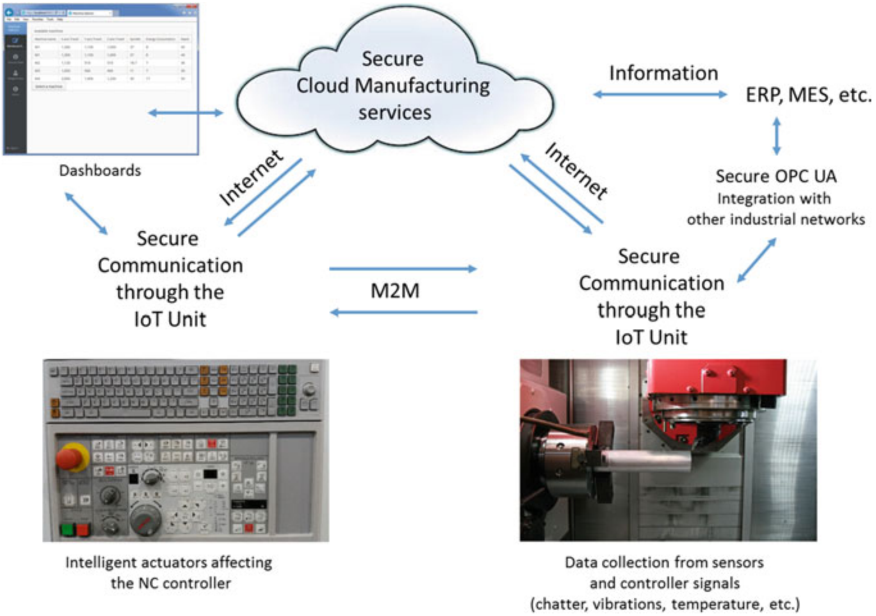

Dashboards
Secure Cloud Manufacturing services
Information
ERP, MES, etc.
Internet
Internet
Secure OPC UA
Integration with other industrial networks
Secure Communication through the IoT Unit
M2M
Secure Communication through the IoT Unit
Intelligent actuators affecting the NC controller
Data collection from sensors and controller signals (chatter, vibrations, temperature, etc.)

Fig. 4 An example of a Secure IoT supported remote maintenance architecture for modern as well as legacy machine tools

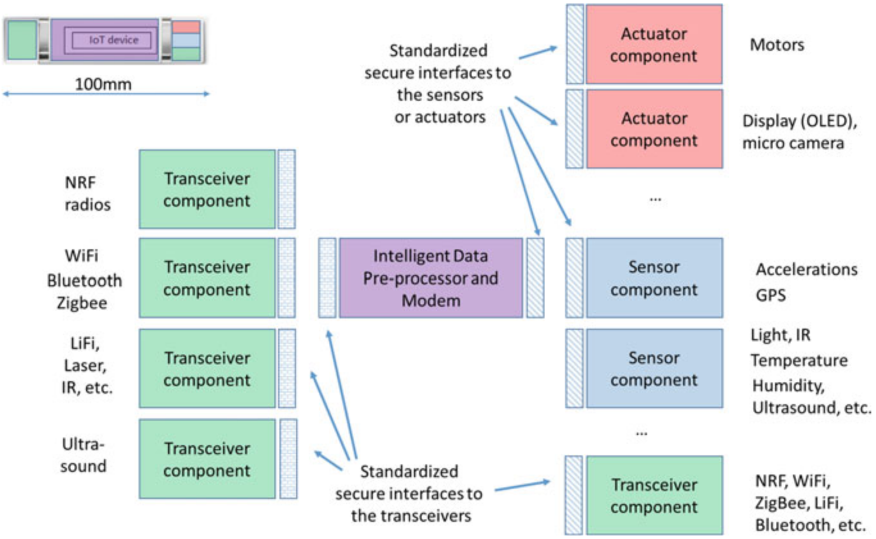


Fig. 5 Secure modular sensor/actuator/communication IoT Unit

can cause threats to the machine and potentially even to the operator. When embedded in the working space of a machine tool, IoT devices should be virtually unnoticeable, i.e. they should use as few wires and setups as possible. They should work robustly over long periods of time without any interruptions while needing none or only minimal maintenance (e.g. firmware updates or low power supply). This makes the selection of the right and reliable IoT technologies a non-trivial task.

Having a machine tool that can be controlled and operated remotely can safe cost and time, increase convenience and flexibility and even open new business opportunities. For example, remote maintenance can help saving cost on maintenance personnel that can otherwise be more efficiently deployed for complex tasks where human intelligence is really required. Employing secure IoT sensors and actuators should not be complex or expensive while requiring only a minimum amount of variation (i.e. non-invasive) to the machine tool. Augmenting machine tools should be gradually scalable, i.e. it should be possible to add, remove or replace as many IoT devices as deemed necessary while maintaining an entirely secure IoT environment. One approach to address these requirements is modularization of IoT devices.

3.2 A Novel Modular IoT Unit

In the following a new modularization concept for IoT devices is introduced. The advantage of modularization is the flexibility to easily replace specialized secure and temper-hardened components. Modularization also helps with flexible scaling of the device capabilities and adapting the device to the individual local requirements. Modular devices are lean and flexible and can adapt and scale to the actual engineering needs while minimizing the potential attack surface.

Figure 5 illustrates the concept of a modular and standardized IoT Unit for sensing, actuating and communicating at the M2M level as well as into the Cloud.

The standardized secure interfaces allows for quick replacement of individual sensors, actuators or transceivers. The IoT Unit can also act as a modem, i.e. it can convert one communication protocol and technology into another. This allows for building rapidly complex heterogeneous and robust IoT Unit networks. Although machine tool data will be collected in areas with potentially high electrical noise, all the data should be preferably transferred wirelessly to increase convenience of deployment. A modular approach allows to pick and choose the combination of the most robust communication means. Small and modular IoT devices also have the advantage to be comparatively cheap and easy to maintain and replace.

For the actual design of the IoT Unit a small and robust build size (estimated size between 50 and 100 mm excluding the power source embedded in epoxy) is preferred so that the actual unit fits easily into any machine tool. The power source uses ideally an energy harvesting unit or solar panel to allow longevity and independence. Although the current battery powered solutions are often feasible, a final choice of the power source will depend on the amount of power required for transferring data or for actuating e.g. motors.

The IoT Unit displayed in Fig. 5 shows an intended design of a sealed secure IoT Unit. Standardized communication interfaces between the components using an elaborate hardware and software authorization protocol allow access to the component data only for authorized users (Tedeschi et al. 2017). The whole approach is designed to be auditable so that any misuse can be spotted and prosecuted if necessary. The data preprocessing unit (in the middle of the IoT Unit) encrypts and decrypts data streams continuously to guarantee data security at all times. For that a miniature hardware AES cryptography low power IC solution has been developed and successfully tested.

To minimize the physical attack surface and also to accommodate for the small physical built size, the limited power supply and the typically limited memory to process data, the secure modular IoT sensor/transmitter/actuator device prefers a setup that uses only a single sensor or actuator and a single communication component at a time. In a machine tool environment the ZigBee protocol and hardware has shown to be a robust and secure communication solution (Tapoglou et al. 2015). Direct point-to-point communication through lasers is fast (e.g. for data streaming) and robust against electrical noise. However, this technique requires a clear line of sight and good geometric alignment of sender and receiver. Small IoT WiFi solutions (TCP/IP, UDP, etc.) offer the fidelity and convenience of classic Internet protocols with its associate security. Depending on the underlying protocols (e.g. MQTT is fast, reliable and scalable), WiFi protocols offer high speed (realistically between 20 Mbps and 100+ Mbps for 802.11 g/n and 802.11 ac, respectively) and reliability. The proposed IoT Unit offers the opportunity to flexibly configure hybrid solutions. NRF, WiFi, ZigBee and other technologies can be utilize and combined to make the best of all individual technologies.

The current cost for the hardware of the proposed and tested IoT Unit lies on the average around £10 (excl. the power source). The actual hardware cost of the IoT Unit depends, of course, on the cost of the individual components with GPS, micro cameras and ZigBee being the most expensive while light and temperature sensors and accelerometers being comparatively cheap. The small and extremely cost efficient ESP8266/NodeMCU® modules as well as the technically well-advanced Intel Edison® are very versatile and programmable IoT units (both low power 3.3 V technology). All sensor and actuator technologies shown in Fig. 5 have been implemented and successfully tested as prototypes. However, the proposed design is still in its early stage and under constant research and development.

Remote machine maintenance offers great opportunities for the end user on the machine through improved awareness of the current and predicted machine performance, information about potential optimization options of the use and setup of a machine tool as well as potential active remote repair and control of the machine tool. Remote maintenance is also a flexible platform for software and service developers that want to offer new machine tool related services. The interconnection of the IoT solutions offers opportunities to improve project planning through simulation and information of the supply chain well in advance before a tool breaks or a spare part is required. Secure remote maintenance can play an important role in providing new services and business opportunities for Through-life Engineering and Industry 4.0.

4 Summary and Conclusion

The Internet of Things is a phenomenon that is currently receiving immense attention due to the rapid move of industry to adopt Industry 4.0. The concept of Cyber-Physical Systems is an integral component of the Industry 4.0 idea. It requires that objects are connected through the Internet or amongst themselves to create a fully interconnected industrial networked environment that offers smart solutions that improve decision making or direct automated process control. However, the large number of interconnected things requires secure and safe communication so that any decisions and actions made are based on reliable and properly authorized information. The risks posed in the IoT world are different to those in the classic Internet world that runs on PCs. In IoT, devices may be very limited in size, computational power and physical power supply, difficult to access, and exposed to harsh environments and unreliable networks. IoT offers great opportunities for the manufacturing industry to utilize the power of communication —this applies both for new as well as legacy equipment. However, even under the extreme conditions some IoT devices have to operate, security of the data needs to be guaranteed at all times to provide the highest quality of service. This article describes various IoT threats. It also introduces an example of an IoT application in a real-world machine tool environment. A novel design—the IoT Unit—is proposed that thrives to lower the barriers to a more secure, easy and efficient application of IoT for a prosperous Industry 4.0 world.

Acknowledgements This work is partially supported by the EPSRC High Value Manufacturing Catapult Fellowship with the AMRC project "BAUTA: A non-invasive remote maintenance tool for legacy CNC machine tools". The project gratefully acknowledges the support of Kennametal and the EU project LegInt in collaboration with the University of Patras (LMS) and Formtec GmbH. The authors would also like to thank the reviewers for their helpful comments and suggestions.

References

Albert M (2015) 7 Things to know about the Internet of Things and Industry 4.0. Modern Mach Shop Mag 88(4):74

Banks A, Gupta R (2015) MQTT version 3.1.1 plus errata 01 OASIS standard incorporating approved errata 01, 10 December 2015, OASIS Open 2015. http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/errata01/os/mqtt-v3.1.1-errata01-os-complete.pdf. Accessed 10 Nov 2016

Baxter RJ (2016) Bluemix and the internet of things. https://developer.ibm.com/bluemix/2014/07/16/bluemix-internet-things/. Accessed 10 Nov 2016

CERT-UK (2015) Cyber-security risks in the supply chain. http://www.cert.gov.uk/wp-content/uploads/2015/02/Cyber-security-risksin-the-supply-chain.pdf. Accessed 2015

Chen Y-K (2012) Challenges and opportunities of internet of things. In: 17th Asia and South Pacific design automation conference (ASP-DAC), Sydney, Australia, 30 Jan–2 Feb 2012, pp 383–388

Di J, Smith S (2007) A hardware threat modeling concept for trustable integrated circuits. In: IEEE region 5 technical conference, 20–22 April 2007, pp 65–68. doi:10.1109/TPSD.2007.4380353

Di-Battista J, Courrege J-C, Rouzeyre R, Torres L, Perdu Ph (2010) When failure analysis meets side-channel attacks, cryptographic hardware and embedded systems. In: CHES 2010, Series lecture notes in computer science, vol 6225, pp 188–202. doi:10.1007/978-3-642-15031-9_13

Dierks T, Rescorla E (2008) The transport layer security (TLS) protocol version 1.2. IETF RFC 5246, RTFM Inc

EU FP7 E-Crime (2016) The economic impacts of cyber crime, D2.2 Executive summary and brief: cyber crime inventory and networks in non-ICT sectors. http://ecrime-project.eu/wp-content/uploads/2015/02/E-CRIME-Deliverable-2.2.pdf. Accessed 10 Nov 2016

Guinard D, Trifa V (2016) Building the web of things: with examples in node.js and raspberry pi. Manning Publications, ISBN-13: 978-1617292682

He H, Watson T, Maple C, Tiwari A, Mehnen J, Jin Y, Gabrys B (2016) The security challenges in the IoT enabled cyber-physical systems and opportunities for evolutionary computing & other computational intelligence. In: WCCI2016, Vancouver, Canada, 24–29 July 2016

Huxtable J, Schaefer D (2016) On servitization of the manufacturing industry in the UK. Proc CIRP 52:46–51

Kang HS, Lee JY, Choi S, Kim H, Park JH, Son JY, Kim BH, Noh SD (2016) Smart manufacturing: Past research, present findings, and future directions. Int J Precis Eng Manuf Green Technol 3(1):111–128. doi:10.1007/s40684-016-0015-5

Kim HH, Bruce N, Lee H-J, Choi Y, Choi D (2015) Side channel attacks on cryptographic module: EM and PA attacks accuracy analysis, information science and applications, pp 509–516. doi:10.1007/978-3-662-46578-3_60

Korolov M (2016) Dell report: attacks against industrial control systems double. http://www.techpageone.co.uk/technology-uk-en/dell-report-attacks-industrial-control-systems-double. Accessed 10 Nov 2016

Li W, Mehnen J (2013) Cloud manufacturing: distributed computing technologies for global and sustainable manufacturing. Springer, London, ISBN-10: 1447149343

Melnikov A, Zeilenga K (eds) (2006) Simple authentication and security layer (SASL). IETF RFC 4422, OpenLDAP Foundation

NN (2016) Smart manufacturing—IoT enables fourth industrial revolution. http://www.smarttechforyou.com/2015/03/smart-manufacturing-iot-fourth-industrial-revolution.html. Accessed 10 Nov 2016

Pääkkönen P, Pakkala D (2015) Reference architecture and classification of technologies, products and services for big data systems. 2(4):166–186. doi:10.1016/j.bdr.2015.01.001

Raddats C, Baines T, Burton J, Story VM, Zolkiewski J (2016) Motivations for servitization: the impact of product complexity. Int J Oper Prod Manage 36(5):572–591. doi:10.1108/IJOPM-09-2014-0447

Shahri AB, Ismail Z (2012) A tree model for identification of threats as the first stage of risk assessment in HIS. J Inf Secur 3:169–176. doi:10.4236/jis.2012.32020

Tapoglou N, Mehnen J, Vlachou A, Doukas M, Milas N, Mourtzis D (2015) Cloud-based platform for optimal machining parameter selection based on function blocks and real-time monitoring. J Manuf Sci Eng 137(4):040909, Paper no: MANU-14-1548. doi:10.1115/1.4029806

Tedeschi S, Mehnen J, Roy R (2017) IoT security hardware framework for remote maintenance of machine tools. In: Second international conference on internet of things, data and cloud computing (ICC’17), March 2017, Cambridge, Churchill College, UK (in print), pp 22–23

UK Government (2015) The controller of her majesty’s stationery office. National Security Strategy and Strategic Defence and Security Review 2015, OGL, ISBN 9781474125956

VDI/VDE (2016) Reference architecture model industries 4.0 (RAMI4.0), Status report, 2015. http://www.zvei.org/. Accessed 28 Sept 2016

Wilson J (2013) Node.js the right way, practical, server-side javascript that scales, Pragmatic Bookshelf

Zhang GH, Poon CCY, Zhang YT (2011) A review on body area networks security for healthcare, ISRN Commun Netw 2011:8, Article ID 692592. doi:10.5402/2011/692592

Cybersecurity for Industry 4.0 and Advanced Manufacturing Environments with Ensemble Intelligence

Lane Thames and Dirk Schaefer

Abstract Traditional cybersecurity architectures incorporate security mechanisms that provide services such as confidentiality, authenticity, integrity, access control, and non-repudiation. These mechanisms are used extensively to prevent computer and network intrusions and attacks. For instance, access control services prevent unauthorized access to cyber resources such as computers, networks, and data. However, the modern Internet security landscape is characterized by attacks that are voluminous, constantly evolving, extremely fast, persistent, and highly sophisticated Schnackenberg et al. (2000), Anuar et al. (2010). These characteristics impose significant challenges on preventive security services. Consequently, methodologies that enable autonomic detection and response to cyberattacks should be employed synergistically with prevention techniques in order to achieve effective defense-in-depth strategies and robust cybersecurity systems. This is especially true for the critical systems belonging to Industry 4.0 systems. In this chapter, we describe how we have integrated cyberattack detection and response mechanisms into our Software-Defined Cloud Manufacturing architecture. The cyberattack detection algorithm described in this chapter is based on ensemble intelligence with neural networks whose outputs are fed into a neuro-evolved neural network oracle. The oracle produces an optimized classification output that is used to provide feedback to active attack response mechanisms within our software-defined cloud manufacturing system. The underlying goal of this chapter is to show how computational intelligence approaches can be used to defend critical Industry 4.0 systems as well as other Internet-driven systems.

L. Thames (✉)
Tripwire Inc., Atlanta, GA, USA
e-mail: lthames@tripwire.com

D. Schaefer
University of Bath, Bath, UK
e-mail: d.schaefer@bath.ac.uk

L. Thames and D. Schaefer (eds.), *Cybersecurity for Industry 4.0*,
Springer Series in Advanced Manufacturing, DOI 10.1007/978-3-319-50660-9_10

1 Cyberattack Detection: Methodologies and Algorithms

Traditional cybersecurity architectures incorporate security mechanisms that provide services such as confidentiality, authenticity, integrity, access control, and non-repudiation. These services are used extensively to prevent computer and network intrusions and attacks. For instance, access control services prevent unauthorized access to cyber resources such as computers, networks, and data. However, the modern Internet security landscape is characterized by attacks that are voluminous, constantly evolving, extremely fast, persistent, and highly sophisticated Schnackenberg et al. (2000), Anuar et al. (2010). These characteristics impose significant challenges on preventive security services. Consequently, methodologies that enable autonomic detection and response to cyberattacks should be employed synergistically with prevention techniques in order to achieve effective defense-in-depth strategies and robust cybersecurity systems Iheagwara et al. (2006), Kabiri and Ghorbani (2005), Ruighaver (2008).

Cyberattack detection systems require algorithms that collect and analyze data generated by various events occurring within a cyber environment. The objective of a detection algorithm is to accurately discover suspicious activities based on the analysis of event data. This objective is fundamentally important as it forms the core of any attack detection system. However, the objective is hard to achieve, especially in terms of ***accuracy***. A detection algorithm that generates inaccurate results can negatively impact the performance of the entire system. Axelsson (2000) claims that the performance of an intrusion detection system, in terms of *effectiveness*, is limited by its false alarm rate. This performance limit is a consequence of the *base-rate fallacy*. For example, inaccurate detection algorithms generate large volumes of false alarms, which can lead to issues such as collateral damage, unnoticed detection of live attacks or intrusions, and unmanageable numbers of alarm notifications that overwhelm security administrators. Consequently, research has explored new algorithms and methodologies aiming to increase the performance and accuracy of detection systems Axelsson (2000), Ghorbani et al. (2010), Anderson (1980), Zhang et al. (2008), Khor et al. (2009).

The study of computational intelligence systems (CIS) is concerned with the theory and design of evolutionary and adaptive systems that possess emergent behavior and intelligent decision making capabilities and that operate within complex and dynamic environments Venayagamoorthy (2011). These systems are generally designed to cope with high dimensional and noisy data during their decision making processes. Since cyberattack detection systems are faced with large volumes of high dimensional data along with continuously evolving attack characteristics, computational intelligence systems have become logical choices to consider when designing new classification algorithms for detection systems.

A computational intelligence algorithm based on new hybridization and ensemble methodologies is presented in this chapter. The algorithms are constructed as generalized systems with no underlying domain-specific assumptions influencing the design. However, the systems are evaluated as classification frameworks for cyberattack and intrusion detection. Before introducing the core detection algorithm, we will first describe how we have integrated the detection system into our software-defined cloud manufacturing architecture. Then, we will provide the reader with a brief overview of neural networks and genetic algorithms. Next, we will describe our ensemble intelligence algorithm and provide details of how we evaluated its performance.

2 Cyberattack Detection and Response Within the Software-Defined Cloud Manufacturing Architecture

We introduced our software-defined cloud manufacturing (SDCM) architecture in Chap. 1. The goal of Chap. 1 was to introduce the reader to a broad array of technologies and paradigms based on the Industry 4.0 vision. The reader should refer back to Chap. 1 for specific details underlying SDCM. In this chapter, we show at a high level how we've incorporated real-time cyberattack detection and response to SDCM. We illustrate the system with Fig. 1. Recall from Chap. 1 that within the SDCM architecture all communications are managed by control elements (CE). SDCM control elements are highly distributed controllers deployed within the cloud. CEs are responsible for interconnecting SDCM entities, whether it is a cloud consumer using an application at the virtual layer that must interact with a hardware device or even if it

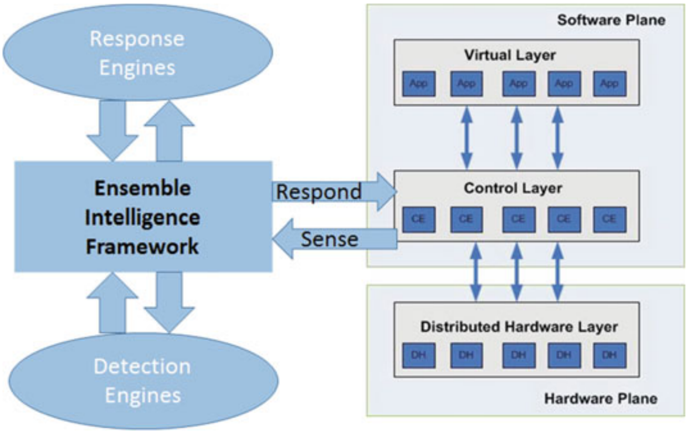


Fig. 1 Software-defined cloud manufacturing architecture with an ensemble intelligence framework for cyberattack detection and response

is multiple hardware devices needing to communicate with each other. Control elements can also communicate with each other to perform their tasks. Essentially, the intelligence of a SDCM system lies within the control layer. The elements of the virtual layer and distributed hardware layer are responsible for getting real design and manufacturing work accomplished. Since the control elements have deep insight into the activities and communications that are taking place, it is logical to use the control elements as data tap points. In our architecture, control elements act as sensors that feed streaming data into the Ensemble Intelligence Framework (EIF). The EIF is responsible for analyzing the sensed data and, when anomalies are detected, it is responsible for responding to the detected anomalies. We use the word anomaly here to reflect that the EIF can be used for other intelligence activities other than cyberattack detection. For example, this could be an intelligent system dedicated to predictive maintenance tasks. However, we are using it here for the purpose of cyberattack detection and response. As the figure illustrates, any number of detection engines can be employed as well as any number of response engines. Response mechanisms can include real-time communication connection termination, installation of new rules in perimeter firewalls, etc. Essentially, response in this context is anything the SDCM system employs for protecting its critical assets from an observed cyberattack.

We have described above at a high level how we have integrated real-time cyberattack detection and response to SDCM via the incorporation of an ensemble intelligence framework. The goal of this chapter is not to go into an in-depth discussion of the framework but instead to describe one possible algorithm that can be used as a detection engine in the framework. In particular, we will describe in the next few sections a neural network ensemble system that utilizes a neuro-evolved network oracle that can be used for analyzing streaming inputs collected by SDCM control elements for the purpose of detecting cyberattacks.

3 Neural Networks and Genetic Algorithms

In this section, we will provide an overview of neural networks and genetic algorithms and how we have used genetic algorithms to produced neuro-evolved neural networks that are capable of very good classification results.

3.1 Neural Networks

The underlying theory of Artificial Neural Networks (ANN or just network if no confusion arises) was originally inspired by biological processes. Specifically, ANNs are modeled after the human central nervous system, which consists of a very sophisticated interconnection of neurons and their associated axons, dendrites, and synapses.

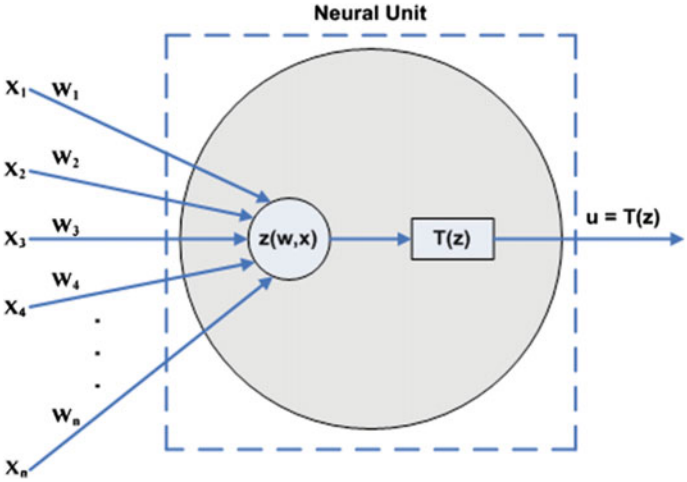


Fig. 2 A conceptual diagram of the neural unit

At the core of an ANN is the neural unit (NU) as shown in Fig. 2. The ANN is created by interconnecting many neural units across several layers to form a highly connected neural network. An NU takes as its input a vector $x = (x_1, x_2, \ldots, x_n)$. Associated with each input connection x_i is a synaptic weight w_i, and these weights form the weight vector w. The output of an NU represents its activation level for a particular set of inputs where the output is denoted by $u = T(z)$. $T(z)$ is the transfer function of the NU (sometimes T is referred to as the activation function). Several forms exist for the transfer function. In this chapter, will only consider three types, which are given by Eqs. 1, 2, and 3. Equation 1 is the logistic sigmoidal function or the logsig function, Eq. 2 is the hyperbolic tangent sigmoidal function or the tansig function, and Eq. 3 is the linear function or purelin function.

$$T(z) = \frac{1}{1 + e^{-z}} \tag{1}$$

$$T(z) = \frac{e^{2z} - 1}{e^{2z} + 1} \tag{2}$$

$$T(z) = z \tag{3}$$

The transfer function's input, z, is the dot product of the input vector with the weight vector as shown by Eq. 4.

$$z = \sum_{i=1}^{n} w_i x_i \tag{4}$$

Networks are created by interconnecting neural units to other neural units formed by one or more hidden layers, where each layer has some prescribed number of units. Networks learn how to map values in the input space to values in the output space via training, and training is provided by a learning algorithm, of which many different forms exist. Common types of ANN learning algorithms are based on the gradient decent algorithm. The basic idea is as follows. Training data is provided to the ANN in the form of $(x,f(x))$ tuples where x is the input data and $f(x)$ is the target function. The learning stage takes the training tuple and sends the input value(s) into the ANN. Then, the output $f_a(x)$ is compared to the target value and an error is calculated. This error is used to evolve the weights such that over time (training epochs) the error of the ANN is minimized to some preferably global but possibly local minimum error. For our work, we utilized networks based on the back-propagation algorithm, whose weight update rule is given by Eq. 5.

$$w_i(t+1) = w_i(t) + \alpha[f(x_i) - f_a(x_i)]x_i \tag{5}$$

During training, each weight vector component for each NU in the ANN is updated similar to Eq. 5. As seen in Eq. 5, as the approximation function approaches the actual function over increasing training epochs, the change in weight value w_i approaches zero such that at convergence $w_i(t+1) \approx w_i(t)$. The value α represents the learning rate, and this value determines how fast the weights evolve. Figure 3 will be used to further illustrate the weight training process. In this example, a single neuron is simulated that is initiated with a weight vector consisting of a randomly generated set of 1000 values. A single target vector with 1000 elements is used as the training data. The algorithm employs a constant learning rate of $\alpha = 0.5$. Figure 3 plots the target vector versus the weight vector as the training epoch is increased from $t = 0$ to $t = 80$. The emergence of a straight line indicates how the weight vector successfully converges towards the target vector with increasing training epochs.

The performance of an ANN is sensitive to the selection of parameters that define its overall configuration. These parameters include, just to name a few, the type of transfer function to use in each layer, the total number of layers, the total number of units per layer, the learning rate's value, the type of training algorithm to use, and the number of training epochs to use. Furthermore, these parameters are not generalized to any given network, and in many cases, they depend on the underlying data's input-output space. If an experienced network designer has a good understanding of the input-output space, then the designer's domain knowledge and expertise allows her to select respectable parameter values. However, this is normally a trial-and-error process even for experienced designers. Further, the problem is more challenging when working with high-dimensional input-output spaces where underlying patterns that drive the selection of parameters are not known. Hence, methods for automated selection of optimized parameters using other computational optimizations sounds promising. In particular, we will investigate the use of genetic algorithms for selecting optimal network parameters.

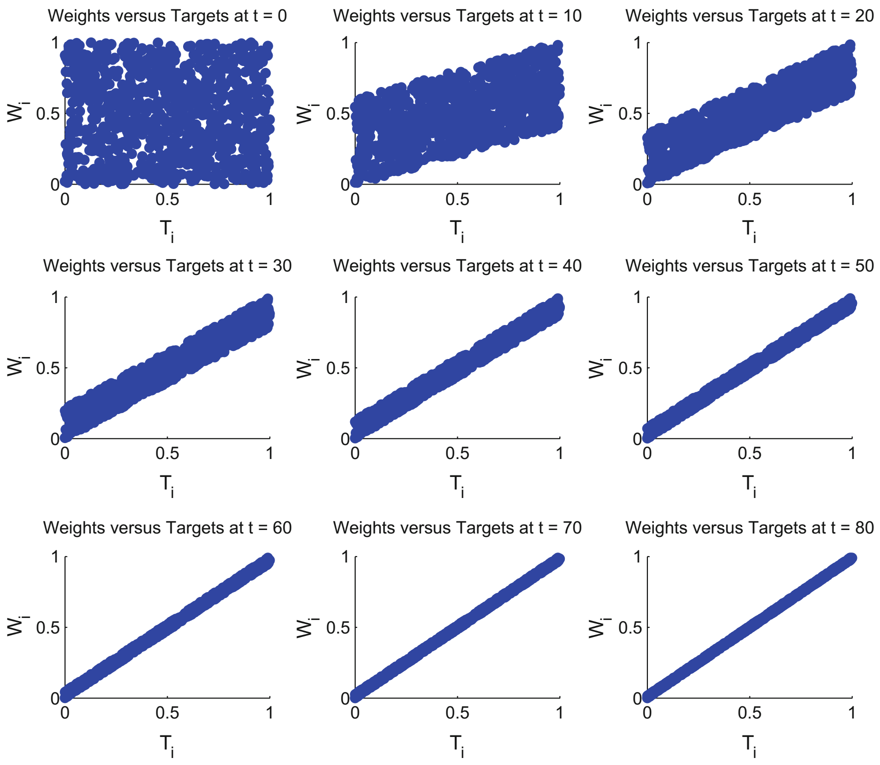


Fig. 3 Learning weights

3.2 Genetic Algorithms

The creation of genetic algorithms (GAs) was inspired by the biological evolutionary process. The primary inspiration is due to the fact that biological systems can adapt over time (evolve) within changing environments. Further, this adaptation can propagate through successor generations within the biological system. This adaptation-propagation scheme leads to the idea of survival of the fittest individuals that can adapt well to changing environments have a higher probability of survival.

The primary operations performed by GA include chromosome representation, genetic selection, genetic crossover, genetic mutation, and population fitness evaluation. In GAs, problem domains are encoded via chromosomes in a population $P(t)$. This chromosome encoding is usually in the form of a bit string or some numerical representation, i.e., one is required to map population members to a binary or numerical form. The population represents a particular state space of hypotheses at evolution time epoch t, where a hypothesis is a possible solution to a given problem. At each time epoch, the fitness of each individual of the population is evaluated. The fitness is evaluated with a fitness function $F(h_i)$ where h_i is the hypothesis represented by the ith member (chromosome) of the population and the fitness F represents how well a particular hypothesis represents the solution of the given problem.

In general, the GA's fitness function must be an increasing function with respect to a candidate hypothesis's response to the problem such that good solutions have higher fitness and poor solutions have low fitness. F is computed for each member, and the next population $P(t + 1)$ is created by probabilistically selecting the most fit members of the current population. Some of the members will be part of $P(t + 1)$ in their current form, and some are selected for genetic modifications such as crossover and mutation. Crossover produces offspring from two parents whereas mutation is the act of randomly modifying the encoding features of a selected set of individuals. There are two important design issues when using a GA. First, one must define a mapping from the input-output space of the problem into an encoding that can be used by the GA, i.e., a binary or numerical mapping. Second, one must design a fitness function for the problem domain. The power of the GA is in its ability to encode a very large set of possible solution spaces for a given problem. They are often used successfully for optimization problems, but they have also been used for function approximation, complex circuit layout, and scheduling. They are also used in neuroevolution to evolve neural networks. In this work, the GA will be used to optimize a certain set of ANN design parameters.

4 Cyberattack Detection with Ensembles of Computational Intelligence Systems

The performance of an artificial neural network is sensitive to the selection of parameters that define its overall configuration. Some of these parameters include the transfer function used within each layer, the total number of layers, the total number of units per layer, the learning rate, the training algorithm, and the number of training epochs to use. Furthermore, these parameters are not generalized to any given network and depend on characteristics of the classification data. Appropriate selection of neural network parameters is typically a trial-and-error process whereby the designer seeks the set of parameters that minimize classification error produced by the network. Optimization algorithms that autonomically tune the parameters of artificial neural networks can alleviate the trial-and-error parameter selection process and can lead to neural networks with better classification accuracy.

In this section, a classification algorithm for attack detection based on ensembles of neural networks is described. The novelty of the algorithm stems from the methodology employed for combining outputs of neural network ensembles. Particularly, a neural network oracle is utilized to combine the ensemble outputs. The neural network oracle is constructed with a genetic algorithm that finds a set of configuration parameters that produce high classification accuracy and low classification error.

4.1 The NNO Classification Algorithm

The proposed algorithm referred to as NNO employs a genetic algorithm to find an optimal selection of configuration parameters for a neural network oracle, which is responsible for combining the outputs of an ensemble of neural networks that classify features belonging to audit data for the cyberattack detection problem. The overall idea is illustrated by Fig. 4 and described as follows.

A set of artificial neural networks $\eta = \{\eta_i\}$ is assigned to features of the collection of labeled audit data that describe a classification domain. The collection of ANNs are trained with standard procedures. Once the collection has been trained, the training data is used to generate a secondary set of training data. The secondary set of training data contains the output of each ANN along with the actual output defined by the baseline training data. The secondary training data is then used to train the neural network oracle. However, the oracle uses a genetic algorithm to find the set of configuration parameters that minimizes its error.

The algorithm consists of two primary phases. During phase 1, a GA is constructed that contains a population of chromosomes that are numerical representations of ANN configuration parameters. At each evolution time epoch, t, the chromosome for each population member is submitted to the ANN. The ANN maps the chromosome's numerical values to their respective parameter types, implements a self-configuration based on these values, and then learns from a training set. Once the

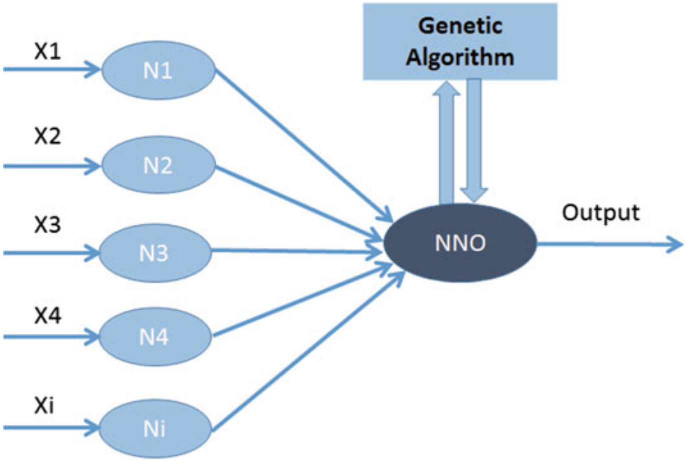


Fig. 4 Architectural illustration of the NNO algorithm

ANN has been trained, a set of labeled validation data from the input-output space is used to evaluate the ANN's post-training error response. This error response is then used to evaluate the fitness of the population member whose chromosome was submitted to the ANN for configuration and training. Since the goal is to find an ANN with minimal error, the error response, which is given by Eq. 6, is used as input to the fitness function of the genetic algorithm.

$$E_i = \sqrt{\sum_{j=1}^{N} \left(f(x_j) - f_a(x_j)\right)^2} \tag{6}$$

In Eq. 6, E_i is the error of the ANN configured and trained based on the chromosome h_i of the ith population member. $f(x)$ is the value of the target function for input x, whereas $f_a(x)$ is the approximation of $f(x)$ produced by the ANN. The error is calculated over a total of N evaluations from a validation dataset. The fitness function for the system is given by Eq. 7.

$$F(h_i; E_i) = \frac{1}{E_i} \tag{7}$$

The fitness function is inversely proportional to the error of the ANN configured by parameters represented by the ith chromosome (i.e., the ith hypothesis h_i) of the GA's population. With the fitness function of Eq. 7, a decrease in error produced by an ANN configured via h_i produces an increase in fitness, which is the underlying objective of the algorithm.

The steps described above are performed for each member of the GA's population. Once each member in the population has been evaluated for fitness, the GA performs selection, crossover, and mutation operations and then proceeds to the next evolution epoch, $t + 1$. This entire process proceeds until the evolution process terminates.

During phase 2, which proceeds after the simulated evolution process terminates, the GA submits the chromosome from the terminal population's best fit individual to the ANN. The ANN uses this chromosome to configure its parameters and then trains from a set of phase-2 training data. Once this training is complete, the system is ready to be deployed for its target application.

5 Datasets and Performance Metrics for Evaluating Cyberattack Detection Systems

Appropriate datasets for training and testing classification algorithms along with reliable metrics to evaluate classification performance are needed for the design of effective cyberattack detection systems. This section discusses the datasets and performance metrics used to evaluate the classification algorithms proposed in this chapter.

5.1 Datasets

Datasets containing relevant features that characterize cyberattacks are needed for the design, evaluation, and comparative analysis of new classification algorithms for attack detection systems. However, datasets and testing environments for evaluating attack detection systems are rare Athanasiades et al. (2003). Of the few datasets publicly available, the ones most frequently used by researchers were produced by the DARPA intrusion detection evaluation program Tavallaee et al. (2010). The objective of the DARPA intrusion detection evaluation program was to produce a collection of standardized datasets that could be used to formally evaluate and objectively compare the performance of intrusion detection systems Lippmann et al. (2000). The datasets have played a critical role in the advancement of intrusion detection systems along with the development of new attack detection and classification algorithms. The DARPA datasets were collected at MIT Lincoln Laboratories during the years 1998, 1999, and 2000. These datasets contain various types of *audit* data with features representing normal and attack traffic.

The KDD CUP99 dataset, which was used as a benchmark for the Third International Knowledge Discovery and Data (KDD) Mining Tools Competition, is frequently used to evaluate intrusion and attack detection algorithms. The CUP99 dataset is a derivative of the 1998 DARPA dataset (DARPA98). DARPA98 contains audit data generated by simulated background traffic representing *normal* packet flows between a military network and the Internet along with traffic representing *attack* packet flows.

The CUP99 data are viewed as sequences of connection records representing unique packet flows. A flow can be defined, similar to the packet filters of a firewall, by specifying a matching criteria over some set of header fields. The canonical flow is specified by a 5-tuple containing source IP address, destination IP address, source port, destination port, and protocol type. The records are classified by two types of flows: attack flows or normal flows. The attack flows are further categorized by 24 unique attack types.

Each record of the CUP99 dataset contains 42 fields. One field provides a label specifying the record's flow type, i.e., normal or attack type. The remaining 41 fields are comprised of features representing data extracted from the flow. The features are categorized as basic TCP features, content features, network-based traffic features, and host-based traffic features. The features are encoded numerically or symbolically. The goal of the KDD competition was to use the CUP99 dataset as a benchmark for evaluating attack classification algorithms produced by the various competitors of the KDD mining tools competition.

The DARPA and CUP99 datasets are out of date. Further, these datasets have been criticized by several whose investigations have discovered various limitations and deficiencies of the data McHugh (2000), Tavallaee et al. (2009). However, the datasets remain widely used for testing and evaluation of attack detection and classification algorithms because there are no suitable alternatives currently available Perdisci et al. (2009), Engen (2010).

In this chapter, classification algorithms for the cyberattack detection problem are introduced. Each algorithm was evaluated with the CUP99 dataset. Particularly, the well-known 10% CUP99 dataset was employed.

5.2 Performance Metrics

The ***accuracy*** of a classification algorithm is a key performance indicator that determines the algorithm's suitability for solving a particular problem. However, other performance indicators are commonly measured in conjunction with accuracy. For example, true positive rates and true negative rates measure a classifier's capability to correctly distinguish *positive* cases from *negative* cases. Classification problems based on two-class decision spaces can use positive and negative rates as performance measures. However, the positive and negative classes must be defined when designing the classifier. Many researchers who design algorithms for intrusion and attack detection problems define attack instances as the positive class and normal instances as the negative class. This is especially true for classifiers implementing anomaly detection. Anomaly detection is based on audit data that represents normal instances and instances deviating from the characteristics underlying the audit data are assumed to be anomalous and, by definition, indicative of an attack. Deviations indicate 'positively' that the instance is an anomaly. Hence, classification of an anomaly is defined to be positive whereas classification of a normal instance is defined to be negative, i.e., not anomaly.

The new classification algorithms proposed in this chapter for the attack detection problem were trained and tested with the CUP99 dataset. CUP99 contains records representing audit data that characterize both normal instances (normal traffic flows) and attack instances (attack traffic flows). Moreover, the dataset is comprised of a multiplicity of attack types. Consequently, CUP99 can be used to evaluate detection systems based on two-class or multi-class classification algorithms. The algorithms proposed in this chapter are designed as two-class classification systems.

Since CUP99 contains audit data characterizing normal and attack instances, several design scenarios can be considered. The data can be partitioned into normal classes for the design of anomaly detection, into attack classes for misuse detection, or the data can remain un-partitioned for mixed detection. The classification algorithms presented in this chapter were trained and tested as two-class mixed detection (non-partitioned) methodologies.

The mixed detection approach with two-class (binary) classification enables two perspectives for defining the positive and negative classes. These perspectives are illustrated by Table 1. The perspective defining the normal class to be positive and the attack class to be negative was chosen for the work described in this chapter.

Table 1 Perspectives of the positive and negative classes for mixed detection binary classification

Positive	Negative
Normal	Attack (NOT normal)
Attack	Normal (NOT attack)

Table 2 Basis parameters of the performance metrics defined in Table 3

Symbol	Description
TP	Total number of true positives
TN	Total number of true negatives
FP	Total number of false positives
FN	Total number of false negatives

Table 3 Definitions and nomenclature of the performance metrics used to evaluate the proposed classification algorithms

Name	Symbol	Calculation
Accuracy	ACC	$ACC = \frac{TP+TN}{TP+TN+FP+FN}$
Positive prediction rate	PPR	$PPR = \frac{TP}{TP+FP}$
Negative prediction rate	NPR	$NPR = \frac{TN}{TN+FN}$
False discovery rate	FDR	$FDR = \frac{FP}{TP+FP}$
False positive rate	FPR	$FPR = \frac{FP}{TN+FP}$
False negative rate	FNR	$FNR = \frac{FN}{TP+FN}$

Several metrics are commonly used when evaluating the performance of classification algorithms. Classification accuracy is a key performance indicator of classification systems. However, accuracy measurements alone do not provide complete information for comparative analysis and optimization purposes. Other key performance indicators include metrics such as error rates, true/false positive/negative rates, and predictive rates.

Evaluations of the new algorithms introduced in this chapter where made with the basis parameters shown in Table 2 and the performance metrics shown in Table 3.

5.3 NNO Ensemble Intelligence: Simulation Results

The NNO ensemble methodology investigated for the cyberattack detection problem used a neural network oracle parametrically optimized with genetic algorithms as described above. Although several parameters can be considered for the optimal response of the NNO, the evaluations described in this section were based on an

NNO configured with two hidden layers of nodes. The optimal parameters that were determined with the genetic algorithm included the number of neural units (nodes) to use for the first and second hidden layers, the type of transfer functions to use in the hidden layers, and the type of transfer function to use for the output layer.

The CUP99 dataset was used to evaluate the performance of the proposed system. An ensemble of 41 neural networks was created. Each feature of the CUP99 dataset was assigned to a single member of the ensemble. A subset of the CUP99 dataset was extracted for training. Each neural network was trained with respect to its corresponding feature. After the ensemble components were trained, a secondary training set was produced by collecting the output of each neural network in the ensemble over the phase-1 testing data and augmenting these outputs with the target class associated with each corresponding training vector. This secondary set of training data was then used to train the NNO. The NNO was parametrically optimized with a genetic algorithm as described above. Once the genetic algorithm converged to a best fit candidate representing the configuration parameters that minimized the NNO's error response with respect to the training data, the NNO was configured and trained via these parameters.

The simulation methodology is described as follows. The CUP99 dataset was partitioned into two disjoint sets comprising training data and testing data. The training procedure was described above. For evaluation, testing proceeded as follows. A total of 500 trials was performed. For each trial, a random selection of records were

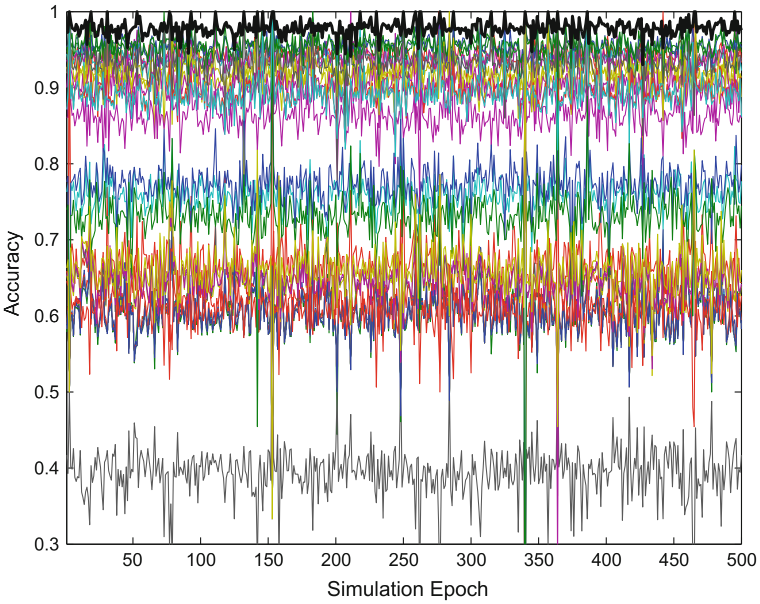


Fig. 5 Accuracies of the individual ensemble members and the neural network oracle over the 500 trials

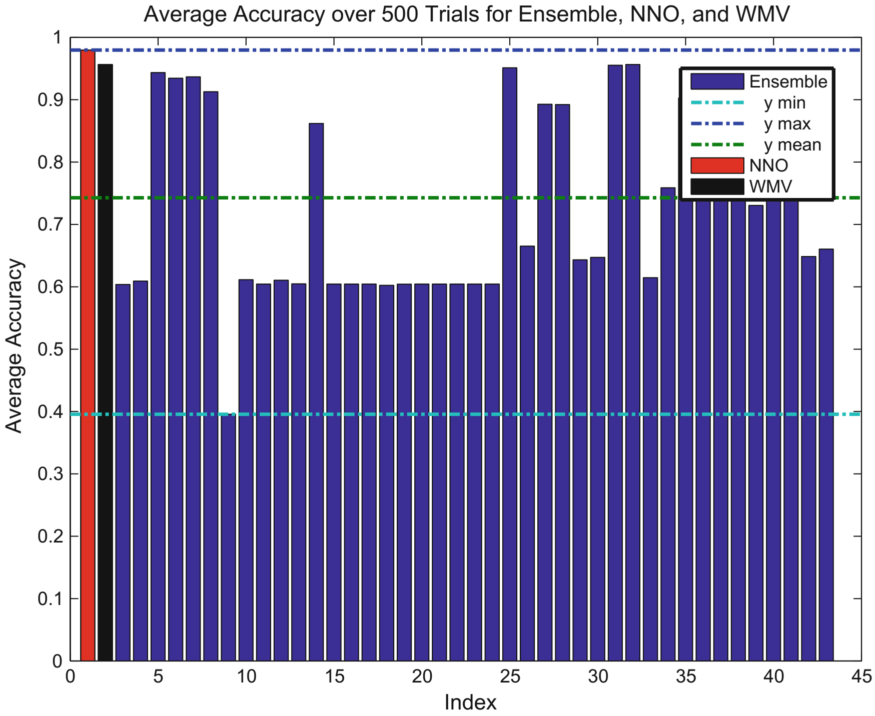


Fig. 6 Bar chart revealing the average accuracies produced over the 500 trials

selected from the test data, and performance metrics of the algorithm were computed and stored as average values. Moreover, the performance of the proposed algorithm was compared to that of the weighted majority vote (WMV) algorithm.

Figure 5 plots the average accuracy over 500 trials for each of the 41 neural networks of the ensemble along with the accuracy of the NNO. The accuracy of the NNO is highlighted by the thick black line towards the top of the figure. Two things should be noted from Fig. 5. First, the range of accuracies reveals that the system has diversity, which is a fundamental requirement for the design of ensemble systems. The accuracies indicate that some of the networks are poor classifiers, some are decent classifiers, and some are good classifiers. Second, the NNO performs consistently better than any given member of the ensemble.

Figure 6 provides a bar chart showing the average of the accuracies produced over the 500 trials for each neural network of the ensemble along with the NNO and WMV. As seen from the figure, the NNO outperforms each of the ensemble members as well as the WMV algorithm.

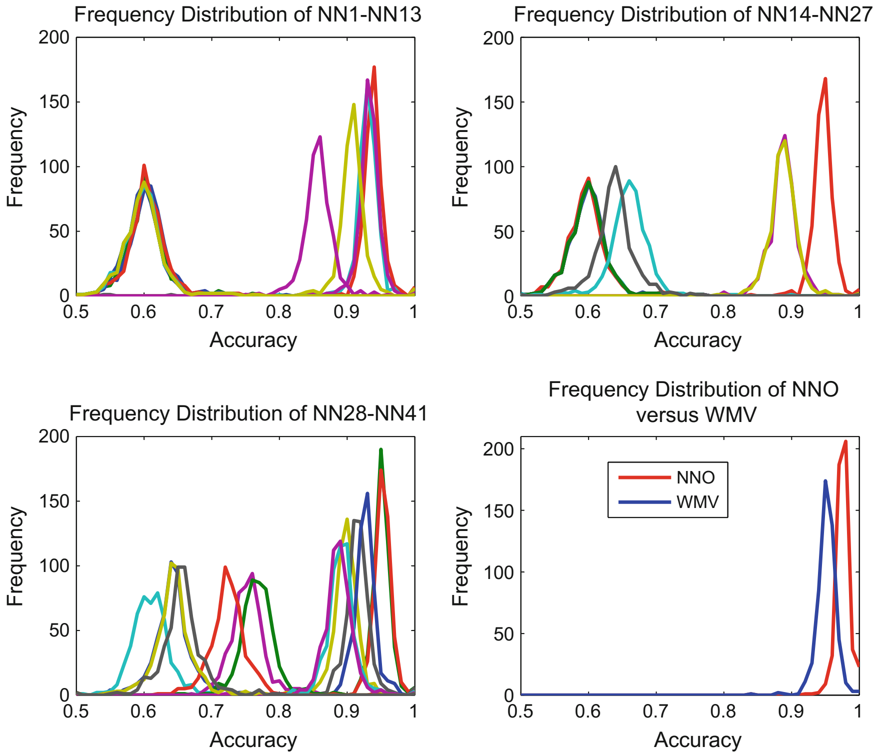


Fig. 7 Frequency distribution of the accuracies for each system over 500 simulation trials

The frequency distributions of the various metrics calculated over the 500 trials for the ensemble components, the NNO method, and the WMV method were generated in order to provide a finer-grained perspective of the performance of each system. A bin width of 0.01 was used to calculate the frequency distributions. Each of the following figures provide metrics for ensemble members, NNO, and WMV. The ensemble results are provided for completeness and for illustrating diversity of the system. However, comparing the performance of NNO versus WMV is the main objective.

Figure 7 plots the frequency distributions for classification accuracies. As seen by the lower right plot, NNO has better accuracy than WMV. Figure 8 plots the frequency distributions for positive prediction rates (PPR) for each classification algorithm. PPR measures how well a classification algorithm predicts the positive class correctly. As seen in the figure, NNO has a better PPR than WMV.

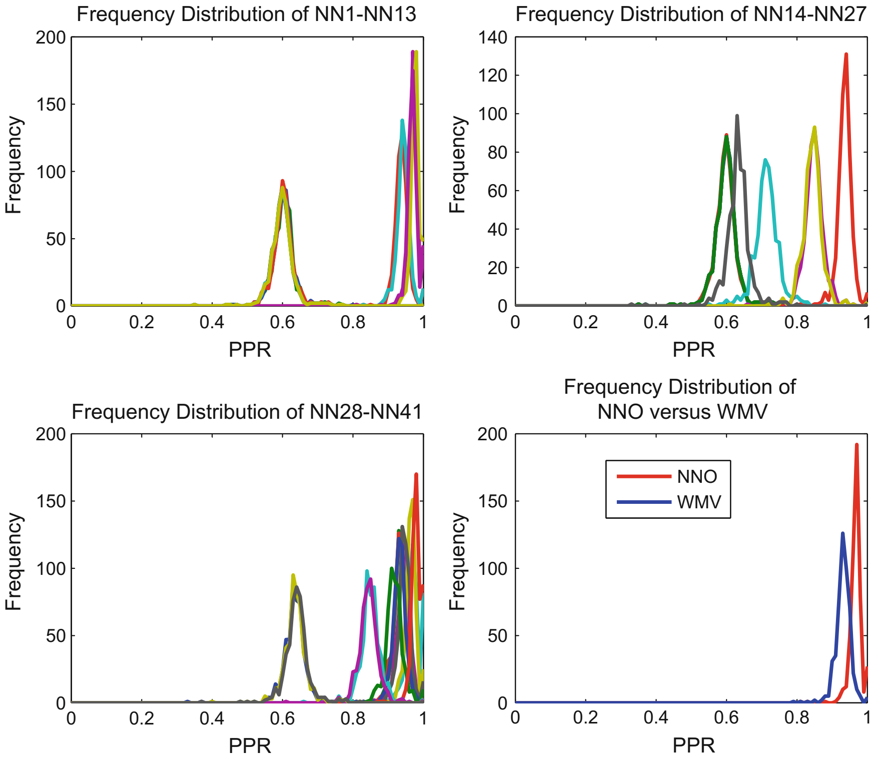


Fig. 8 Frequency distribution of the PPR for each system over 500 simulation trials

Figure 9 plots the negative prediction rate (NPR) of the algorithms. NPR measures how well a classification algorithm correctly classifies negative instances. For NPR, NNO and WMV both perform well and similarly. Figure 10 provides the false discovery rates (FDR) produced by the simulations for the classification algorithms. FDR should be small for good classification algorithms. As seen in the figure, NNO has better FDR performance than WMV.

Figures 11 and 12 plot the frequency distributions for the false positive rates (FPR) and false negative rates (FNR), respectively. Similar to FDR, a good classification algorithm should have small FPR and FNR. As seen in Fig. 11, NNO has better FPR performance than WMV. However, NNO and WMV perform comparably for FNR.

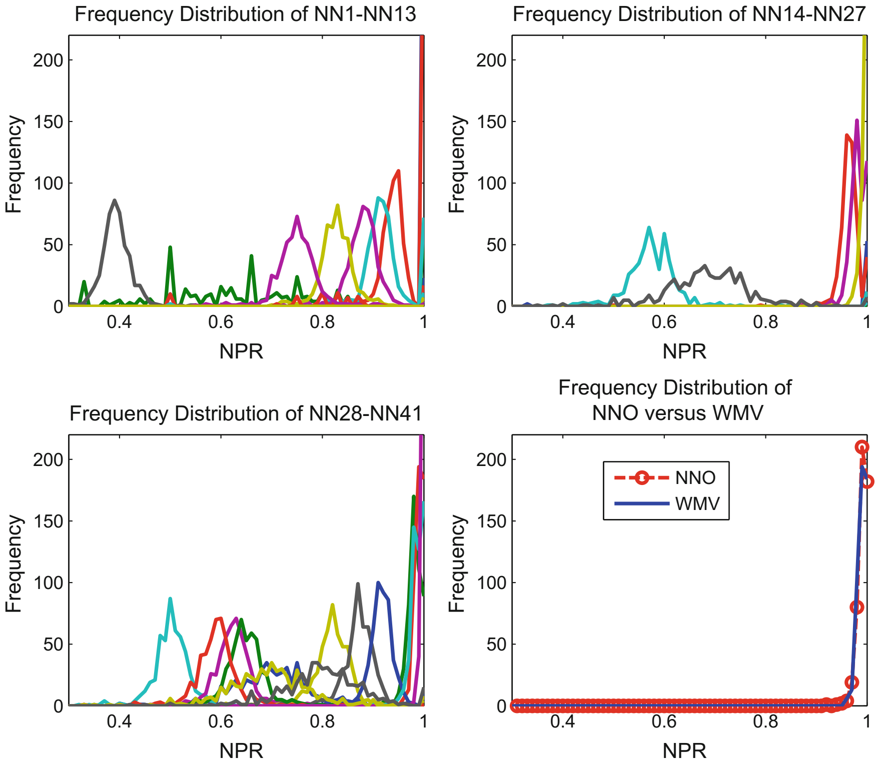


Fig. 9 Frequency distribution of the NPR for each system over 500 simulation trials

Based on the results obtained from simulations along with analysis of its performance metrics, the proposed ensemble methodology using a parametrically optimized neural network oracle provides good performance as a classification system for the cyberattack detection problem.

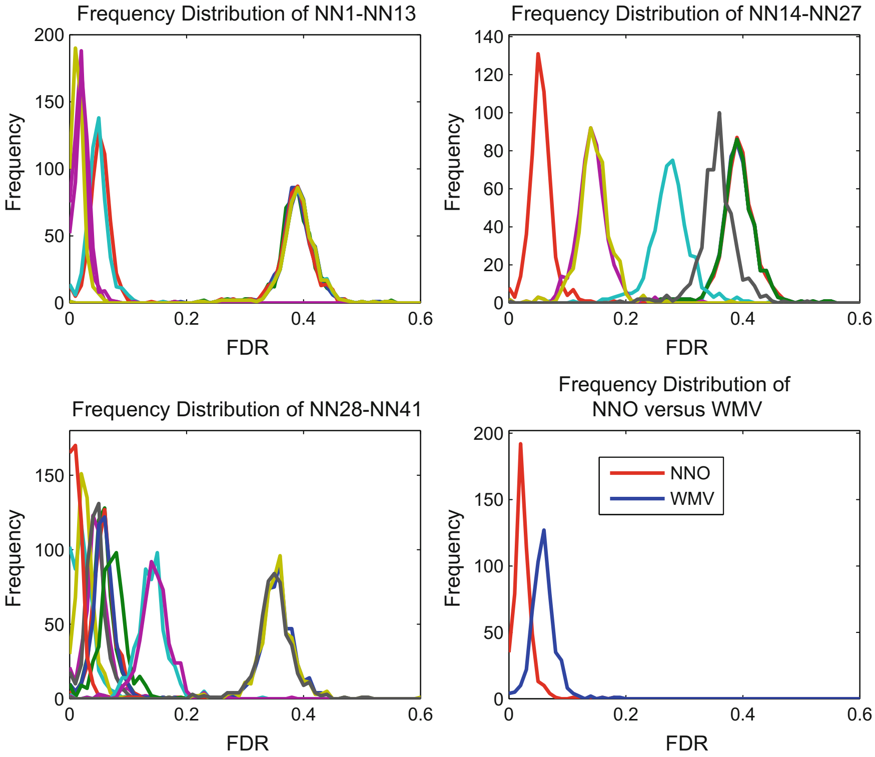


Fig. 10 Frequency distribution of the FDR for each system over 500 simulation trials

6 Summary

In this chapter, an algorithm for cyberattack detection for Internet-based systems such as Industry 4.0 systems was introduced. The algorithm, referred to as NNO, is based on an ensemble of neural networks along with a neural network oracle that has its configuration parameters optimized by genetic algorithms using a fitness function evaluated with neural network error responses. The performance evaluation of the

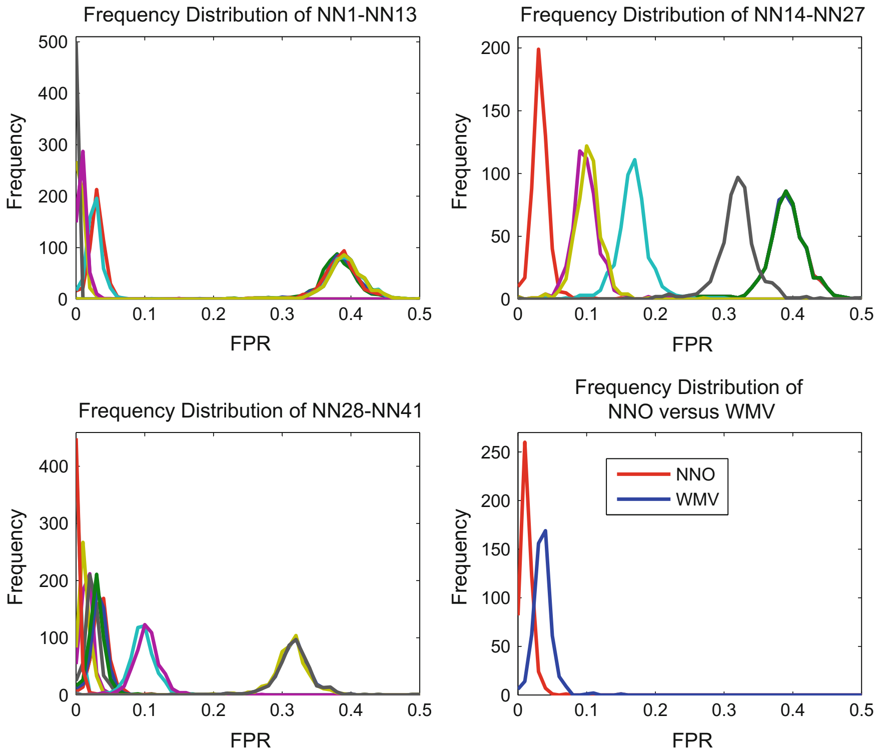


Fig. 11 Frequency distribution of the FPR for each system over 500 simulation trials

proposed algorithm was based on the CUP99 intrusion detection dataset. According to the simulation results obtained, the algorithm was shown to provide good classification performance when trained and tested with the CUP99 intrusion detection dataset. The algorithm can be used to successfully detect cyberattacks targeting Industry 4.0 systems and can be coupled with active response mechanisms in order to stop real cyberattacks.

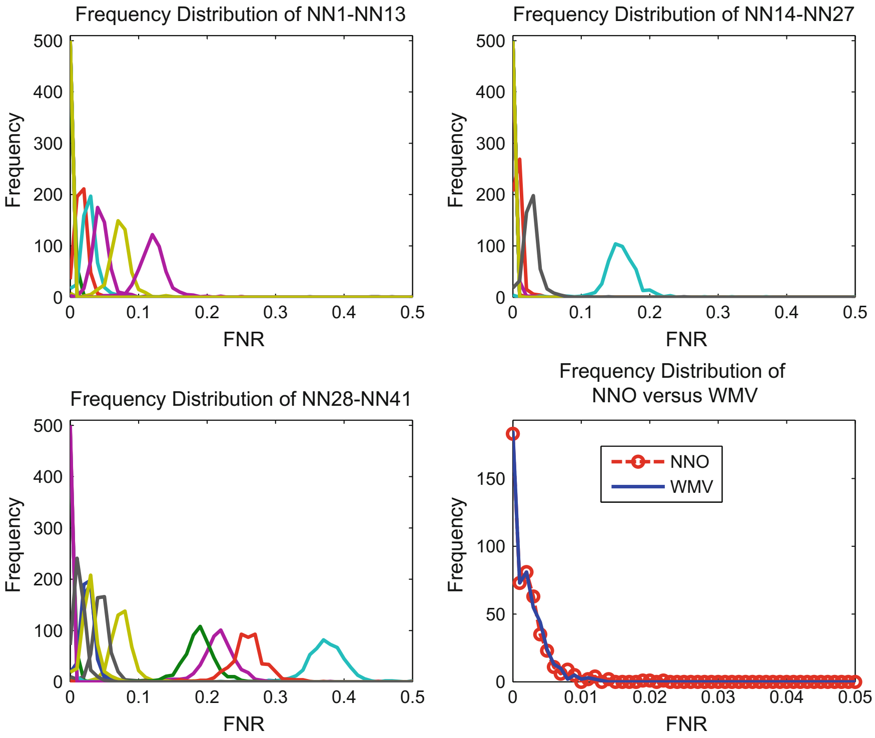


Fig. 12 Frequency distribution of the FNR for each system over 500 simulation trials

References

Anderson J (1980) Computer security threat monitoring and surveillance

Anuar NB, Papadaki M, Furnell S, Clarke N (2010) An investigation and survey of response options for intrusion response systems (IRSs). In: Information security for south africa (ISSA)

Athanasiades N, Abler R, Levine J, Owen H, Riley G (2003) Intrusion detection testing and benchmarking methodologies. In: Proceedings of the first IEEE international workshop on information assurance (IWIA'03)

Axelsson S (2000) Intrusion detection systems: a survey and taxonomy. Technical Report, Department of Computer Engineering, Chalmers University of Technology

Axelsson S (2000) The base-rate fallacy and the difficulty of intrusion detection. ACM Trans Inf Syst Secur 3(3):186–205

Engen V (2010) Machine learning for network based intrusion detection. PhD Thesis, Bournemouth University

Ghorbani AA, Lu W, Tavallaee M (2010) Detection approaches. Springer, J Network Intrusion Detection and Prevention

Hatch M (2014) The maker movement manifesto, McGraw-Hill Education. ISBN 10:0071821120

Iheagwara C, Awan F, Acar Y, Miller C (2006) Maximizing the benefits of intrusion prevention systems: effective deployment strategies. In: Proceedings of the 18th annual forum of incident response and security teams (FIRST) conference

Kabiri P, Ghorbani A (2005) Research on intrusion detection and response: a survey. Int J Netw Secur 1(2):84–102

Khor KC, Ting CY, Amnuaisuk SP (2009) From feature selection to building of bayesian classifiers: a network intrusion detection perspective. Am J Appl Sci 6(11):1949–1960

Knapp E, Langill J (2015) Industrial network security: securing critical infrastructure networks for smart grid, SCADA, and other industriaal control systems, 2nd edn. ISBN 978-0-12-420114-9

Li BH, Zhang L, Wang SL, Tao F, Cao JW, Jiang XD et al. (2010) Cloud manufacturing: a new service-oriented networked manufacturing model. Comput Integr Manuf Syst 16(1):1–7

Lippmann R, Haines J, Fried D, Korba J, Das K (2000) The 1999 DARPA off-line intrusion detection evaluation. Comput Netw 34(4):579–595

McHugh J (2000) Testing intrusion detection systems: a critique of the 1998 and 1999 DARPA intrusion detection system evaluations as performed by Lincoln laboratory. ACM Trans Inf Syst Secur 3(4):262–294

NIST Special Publication 800-82 (2011) Guide to industrial control systems (ICS) security. http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf

Open Networking Foundation (ONF) (2012) Software-defined networking: the new form for networks

Paul Brody (2013) Get ready for software-defined supply chain. Web: http://www.supplychainquarterly.com/topics/Manufacturing/20140110-get-ready-for-the-software-defined-supply-chain/

Perdisci R, Ariu D, Fogla P, Giacinto G, Lee W (2009) McPAD: A multiple classifier system for accurate payload-based anomaly detection. Int J Comput Telecommun Netw 53(6):864–881

Peterson A, Schaefer D (2016) Social product development: introduction, overview, and current status, In: Schaefer D (ed) Product development in the socio-sphere: game changing paradigms for 21st century breakthrough product development and innovation. Springer pp 63–98. ISBN 978-3-319-07403-0

Ruighaver A (2008) Organisational security requirements: an agile approach to ubiquitous information security. In: Proceedings of the sixth australian information security management conference

Schaefer D, Thames JL, Wellman R, Wu D, Yim S, Rosen D (2012) Distributed collaborative design and manufacture in the cloud motivation, infrastructure, and education. ASEE 2012 annual conference and exposition, San Antonio, Texas, June pp 10–13

Schnackenberg D, Djahandari K, Sterne D (2000) Infrastructure for intrusion detection and response. In: Proceedings of the 2000 DARPA information survivability conference and exposition

Tavallaee M, Stakhanova N, Ghorbani A (2010) Toward credible evaluation of anomaly-based intrusion-detection methods. IEEE Trans Syst Man Cybern Part C: Appl 40(5):516–524

Tavallaee M, Bagheri E, Lu W, Ghorbani A (2009) A detailed analysis of the KDD CUP 99 data set. In: Proceedings of the second IEEE international conference on Computational intelligence for security and defense applications, IEEE Press

Thames JL, Abler R, Hyder A, Wellman R, Schaefer D (2011) Architectures and design methodologies for scalable and sustainable remote laboratory infrastructures. In: Azad A, Judson (ed) Internet accessible remote laboratories: scalable e-learning tools for engineering and science disciplines. IGI Global Publishing, ISBN 978-1-61350-186-3, Chapter 13, pp 254–275

Thames JL (2014) Distributed, collaborative, and automated cyber security infrastructures for cloud-based design and manufacturing systems. In: Schaefer D (ed) Cloud-based design and manufacturing (CBDM): a service-oriented product development paradigm for the 21st century. Springer, pp 207–229. ISBN 978-3-319-07398-9. doi:10.1007/978-3-319-07398-9_8

Venayagamoorthy G (2011) Dynamic, stochastic, computational, and scalable technologies for smart grids. IEEE Comput Intell Mag 6(3):22–35

Wu D, Greer MJ, Rosen DW, Schaefer D (2013) Cloud manufacturing: strategic vision and state-of-the-art. J Manuf Syst

Wu D, Thames JL, Rosen D, Schaefer D (2012) Towards a cloud-based design and manufacturing paradigm: looking backward, looking forward. ASME 2012 international design engineering technical conference and computers and information in engineering conference (IDETC/CIE), Chicago, Illinois, August pp 12–15

Wu D, Thames JL, Rosen D, Schaefer D (2013) Enhancing the product realization process with cloud-based design and manufacturing systems. ASME J Comput Inf Sci Eng (JCISE) 13(4)

Xu X (2012) From cloud computing to cloud manufacturing. Rob Comput Integr Manuf 28(1):75–86

Zhang J, Porras P, Ullrich J (2008) Gaussian process learning for cyber-attack early warning. In: Proceedings of the SIAM international conference on data mining