

Integrated Trusted Protection Technologies for Industrial Control Systems

Jingpei Wang*, Jie Liu*, Shengming Yang*, Minghui Zhang**

*Information Security Research Center, China CEPREI Laboratory, Guangzhou, 510610, China

** School of Electronic and Information, Northwestern Polytechnical University, Xi'an 710129, China

wjpbupt@163.com, liujie@ceprei.com, yangsm@ceprei.com, nikkoch@163.com

Abstract—Security vulnerabilities in industrial control systems (ICS) and its open interconnected trends lead to security risks escalating. The existed security protection technologies, with poor applicability, are hard to meet the special requests of information security for ICS. In this paper, trusted protection theories and technologies for ICS were studied and an integrated trusted protection model was proposed. The proposed method protected data and system security of ICS from aspects of trusted computing platform, trusted data protection mechanism and trust management network. The trusted protection technologies were deployed on each of the three network layers of ICS according to differentiated resources and security requirements of each layer. Finally, analysis and simulation were performed and the results indicate the effectiveness and superiority of the proposed method. The established trusted protection model assists realizing the systematic information security protection for heterogeneous industrial control systems.

Keywords—industrial control systems; information security; trust; trusted protection; integrated model

I. INTRODUCTION

The inherent vulnerabilities of the industrial control system and the openness when networking lead the security threats continuing to expand. Worldwide security incidents had occurred continuously, typical events included the attack on water conservancy facilities control system in Canada in 2007, the event of city subway derailment in Polish in 2008, “Stuxnet” virus incidents in Iran in 2010, the attack on US cities water supply system in 2011, the “contaminated area” virus incidents in 2011, the “Flame” event in 2012, and the “dragonfly organization” attacks on European energy system in 2014, etc.[1]. As the ICS are often used in critical infrastructure, once destroyed, would seriously endanger public safety and social-economic lifeline, and even affect the national security [2]. Therefore, researching the theories and technologies of information security protection of ICS, is a great significance to ensure secure and stable operation of key industries and infrastructure.

However, the security protection for ICS is very difficult. As ICS and its equipment are proprietary, large number of industrial control system existed may not have available computing resources to improve their security capabilities of information systems. Since the real-time demand, many operator stations of ICS generally do not install anti-virus

software, even if the anti-virus function is deployed, the usage and upgrade are largely restricted. Therefore, the research of security protection technologies suitable for the feature of the industrial control systems is the focus of current researches.

Trusted mechanism is an information security protection technology widely used in different network system. This paper researched the trusted protection technology for ICS. It built trusted platform, trusted data protection mechanism and trust management network on each of the three layers network architecture of ICS. Combined with basic protection methods, the established protection mechanism ensured the security of the data life-cycle of industrial systems.

The rest of the paper is organized as follows. Section II presents the related works. Section III outlines the layered structure and security requirement of ICS. In Section IV, trusted protection technologies for ICS are explained in detail. Further, deploy framework of trusted protection model is given in Section V. Section VI presents some analysis and simulation, followed by the conclusions in Section VII.

II. RELATED WORKS

United States (U. S.) began to focus on information security issues for industrial control system since 1999. US Department of Homeland Security (DHS) organized relevant departments issuing the “protection Roadmap of the control system in energy industry” in 2006, and issuing the “protection Roadmap of the control system in chemical industry” in 2009. In 2011, “cross-industry information security Roadmap in industrial areas” was released, which summarized common objectives of the development of information security for industrial areas. In Europe, the protection guidance document of the industrial control systems developed by the European Network and Information Security Agency (ENSIA) was also released in December 2011. In addition, the United Kingdom, Netherlands, France, Germany, Norway, Sweden and other countries were gradually developing information security-related standards, guidelines and policy documents of industrial control system to guide and regulate the work of domestic information security for industrial control system [3-4].

In order to protect ICS, National SCADA Test Bed Program (NSTB) funded by the US Department of Energy (DOE) issued a protection roadmap of the control systems [5].

It was considered that the protective theory and technologies integrated closely with essential characteristics of the ICS were critical to realize each objective of the information security Roadmap.

Trusted computing is considered to be an important method to solve the intrinsically security of information system. Nagarajan proposed a dynamic trust enhanced security model for trusted platform based services [6], it combined ‘hard’ trust from properties measurements and ‘soft’ trust from past experiences and recommendations to improve trustworthiness of the attesting platforms. Daci implemented a Trusted Platform Module to improve data integrity and performance of the cryptographic structured log file systems [7]. Arun Fera designed a trusted monitoring framework providing a chain of trust that excludes the untrusted privileged domain, and utilized the trusted computing technology to ensure the integrity of the monitoring environment [8]. However, current researches of trusted theory and technology just focus on the general information systems or common communication network of ICS, they have not been applied to entire industrial control network.

Fadul advocated the use of a reputation based trust management system in the future communication-based “Smart” electric power grid [9]. Trust mechanism is one method to mitigate cyber-attacks and improve response time of the backup protection system with the increasing of communication capabilities. Okhravi proposed new network architecture based on trusted network for process control network, and discussed the basic components, protocols and operations of TPCN [10]. Adding trust to industrial control network reduces vulnerabilities to malware attacks. However, credible body would get the data leaked, it still need additional protection, e.g. access control and user authentication, to prevent data leakage resulting from internal threats.

III. LAYER STRUCTURE AND SECURITY REQUIREMENT

A. ICS Structure

ICS usually adopt proprietary software and hardware. Control device and system isolated from each other. But with the development of information technology and the increasing of functional request of industrial production, enterprise resource planning system (ERP), common communication protocols (e.g. TCP/IP protocol), general operating system and other intelligent components, are adopted in ICS increasingly. But more security threats are leaded to industrial control systems at the same time. The mainstream network architecture of industrial control systems and its security threats are shown in Figure 1.

As it can be seen from Figure 1, the security threats of ICS mainly come from external attacks and internal attacks. In external attacks, attacker use Internet attack techniques scanning the target network system, find its vulnerabilities, and then perform continuous attacks (such as APT attacks), until destroy system from normal operation, steal sensitive information and perform other threats. Internal attacks include malicious data leakage, viruses spreading by mobile devices,

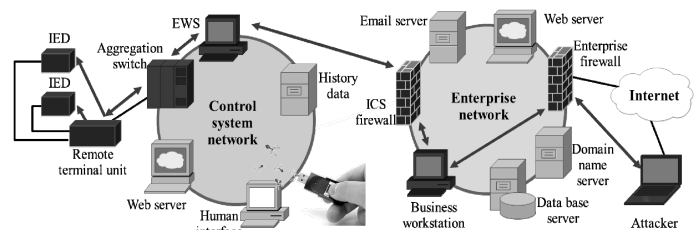


Figure 1. Structure of ICS and security threats

unintentionally attacks, e.g. inappropriate tests (vulnerability scanning, penetration testing), as well as unauthorized changes of system configuration, etc.

B. Security Requirement

In order to protect ICS, the basic protection technologies, i.e. firewall, isolation gateway, intrusion detection, malware detection, etc., are necessary. In addition, protection technologies suited for structural characteristics and features of ICS are also demanded. Study intrinsic security technology and propose an active, systematic, trusted protection method will be a viable solution. Firstly, three items will be addressed:

- **Item 1:** security protection and integrity protection should ensure availability of core control system.
- **Item 2:** external attacks and internal attacks should be considered simultaneously, systematic protection is populated.
- **Item 3:** proposed trusted protection scheme should be continuous in covering entire data security lifecycle.

IV. TRUSTED PROTECTION TECHNOLOGIES FOR ICS

Based on Figure 1 and security requirements, we proposed trusted protection technologies for the ICS. The proposed proposal mainly included three parts: trusted computing platform, trusted data protection mechanism, and trust network management, deploying in different layers of the ICS.

A. Definition of Trust

Definition 1: trusted $\approx$ reliable + security. In industrial control systems, reliability means that service is reliable and available, and real-time request is available; security refers to information security and behavior security, it satisfies the confidentiality and immune to malicious attacks.

Trusted computing platform is the basic method guarantying the credibility of the entire operating environment from hardware to software process, it ensure that the system works as expected behavior; trusted data protection mechanism is a set of data protection policies based on a trusted root, also it includes an active defense mechanism for sensitive data; trusted network is immune to malicious behavior of network nodes based on trust management. Trusted protection technologies ensure trusted operation of ICS from aspects of systems, data and network.

B. Trusted Computing Platform

Considering the availability and resource-constrained feature of field device system, deploy trusted computing

platform in production monitoring network layer. Trusted Platform Module (TPM) is embedded in trusted computing platform. TPM takes password and authentication technologies as a trusted chain, start from the physical hardware, induce the booting up and running of the system. The trusted chain transfers from the chip, motherboard, BIOS, operating system sequentially to ensure the integrity, credibility and security of the control computing platform, along with the trusted software protocol stack. The TPM checks all the operations between the field devices and the monitoring network, ensure the credibility of the operation platform by forbidding unauthorized operation and warning of system status. Trusted computing platform is resistance to various attacks, i.e. fabrication, falsification, illegal read, and also can prevent leakage of sensitive data in the platform. Trusted computing platform is mainly used in prior monitoring, legality certification of system to ensure computing platform controlled, and refusal of unintended control of device system after security incidents (e.g. the nuclear centrifugal rotating machine was controlled by the “Stuxnet” virus in 2010.).

C. Trusted Data Protection Mechanism

Deploy trusted data protection mechanism in the field device layer and production monitoring layer to protect core data of industrial control system. Core data include production data in field equipment, control data of transmission, stored sensitive data. Construct isolated communication environment similar to VPN dynamically in the field device layer, ensuring data used for device control being not leaked. Combining with trusted computing and virtualization technology, build a virtual machine system in production monitor layer, and establish a secure protection domain (SPD) for sensitive data, as shown in Figure 2.

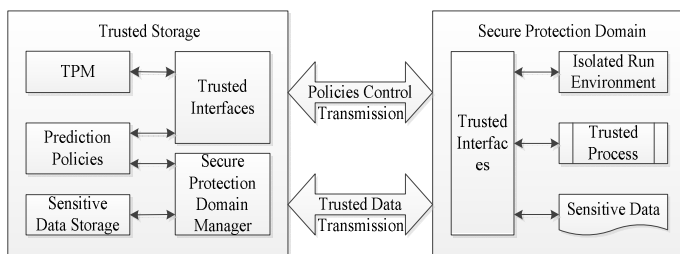


Figure 2. Trusted data protection mechanism

Sensitive data are bounded in SPD, the access of sensitive data is validated by security authentication and control policies according to the expectation of data protection, and thus the anti-leak of data is achieved. Security domain is a virtual isolated environment built dynamically, the processes of operating data only permitted in the security domain. File access, network access and communications are filtered by the security domain, and the operation of writing the data to an un-trusted storage area or sending to untrusted processes will be prohibited. SPD is encrypted and packaged by the TPM, and the expected policies of using data are set in advance. When certain process has access to sensitive data, the SPD test

the related environment of data usage initiatively, authenticate the user or process, and ensure that the access of data and its operation are in the trusted environment. Meanwhile it passes the untrusted process or clues to malicious code detection server, inspects malicious intrusions. Trusted virtual data protection mechanism is mainly used in the prior monitoring, security isolation, intrusion detection and post-audit.

D. Trust Network Management

Deploy trusted network in enterprise management network. Corporate management network connects to the Internet directly, and both the external attacks and internal malicious nodes will cause security threats. Thus it is necessary to introduce the trusted network to ensure the network controlled and service security. It adopts the generally accepted architecture of a trusted network: trusted terminal set, security gateway, trusted agent layer and application access layer. The security of trusted terminal is the core factor for a trusted network. In static evaluation, the security of trusted terminal is proved by trusted computing module. In dynamic evaluation, the trusted nodes have certain intelligence, the credibility are related to their actions and behaviors. Trust management is an effective solution to evaluate credibility of behavior. The trust values of nodes are determined by calculating their historical performance dynamically, and nodes whose trust values greater than a defined threshold are considered to be credible to participate services, thus malicious nodes will be isolated. A typical method of trust calculation is shown as (1).

$$T = \left[100 \left(\frac{S}{S+U} \right) \left(1 - \frac{1}{S+1} \right) \right] = \left[\frac{100S^2}{(S+U)(S+1)} \right] \quad (1)$$

Where S and U are the number of successful trading and failed trading in a certain-length time window T , T is defined as an integer, and $T \in [0, 100]$. Based on the trust values, a node is assigned one of the three possible states: 1) trusted, 2) un-trusted, or 3) uncertain to other member nodes. The half of the mean of all the trusted values and the 1/3 of the mean of all the un-trusted values are set to the medial boundaries of three states.

Trusted network is mainly used to detect behavioral attacks, protect the ICS coordinating with intrusion prevention, malicious code defense and post-audit.

V. SYSTEM DEPLOY FRAMEWORK

Based on above three information protection mechanisms, comprehensive trusted protection model of industrial control systems can be established. The model is deployed in the layers of field devices network, production monitoring, and enterprise management respectively, achieving integrated coordinated protection for industrial control systems. On the specific steps, trusted computing modules are embedded in the core control network of the industrial control system to perform access control of core component, trusted data protection mechanisms are embedded in operation monitoring module and field devices network of the industrial control system to achieve real and credible data management, trust

management model is embedded in enterprise management network module of the industrial control system to realize dynamic trust management of nodes. The deploy framework of comprehensive trusted protection model of industrial control systems is shown in Figure 3.

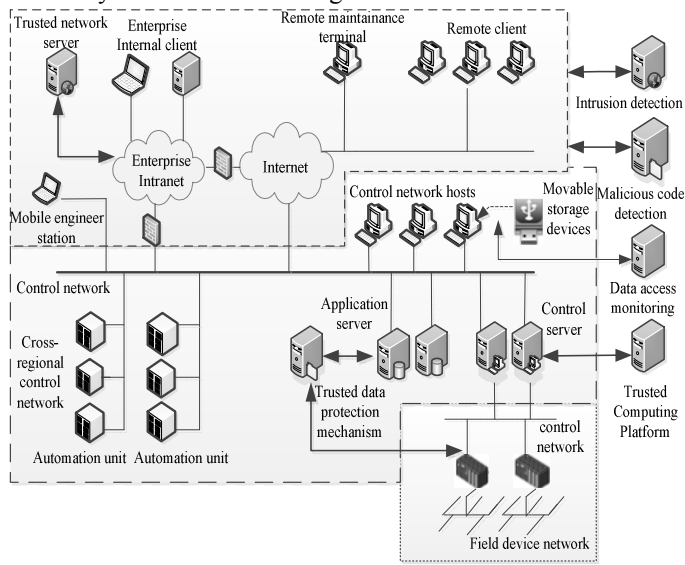


Figure 3. Trusted protection system architecture of ICS

Without loss of generality, the network architecture of ICS is mainly divided into the field device layer, production monitoring layer and enterprise management layer (including the Internet), the boundaries are indicated by a dotted line. Figure 3 shows that the security protection of industrial control network cover three areas including external security protection, internal protection of automation control network and field equipment network protection. Trusted computing platform, trusted data protection mechanism, trusted network are deployed at each layer coordinately.

The establishment of trusted protection technologies, combined with traditional data and system protection technologies, can realize data and system security of industrial control system. Meanwhile, trusted protection technologies analyze the data stream (i.e. network routing information, read and write information, data transmission information) of industrial control system from dimension of node and network, and determine its credibility, the results of which can be used for real-time or post auditing.

VI. ANALYSIS AND SIMULATION

A. Analysis of the Protection Proposal

Security: Malicious code attacks, unauthorized access, information disclosure, denial of service attacks are common attacks in ICS. In the comprehensive protection system, active trusted access monitoring in the trusted data protection mechanism can find the invasion through removable storage devices, trusted virtual domains can block malicious code attack based on integrity protection of access control. Therefore, malicious code attacks can be blocked by the proposed method. Unauthorized access is isolated by the

security enclosures preliminary, then rejected by trusted data protection mechanisms, and submitted to audit. Information disclosure mainly comes from internal network, the measurements of isolation environment of trusted data, security protection domain of sensitive data, read and write authentication of transmitted data, can be relied to protect information, and audit according to the operating logs when necessary. The goal of denial of service attacks is destroying the availability of the ICS, the control manager in production monitoring layer and field device layer should be protected priority. The proposed method prevents non-trusted access request mainly by the trusted computing platform, combined with the mechanism of protocol inspection and traffic monitoring, as well as redundancy mechanisms to ensure availability.

Availability: The proposed method takes advantage of different resource properties of three-tier architecture of ICS, deploy trusted protection technologies on one layer based on its heterogeneous nature. In field devices layer with the highest requirements of real-time, isolation mechanism of trusted virtual domain is used to prevent unauthorized access, and intrusion prevention mechanism is deployed in control interface between production monitoring layer and field layer, further protect the field devices effectively. In production monitoring layer, trusted computing platform and trusted data protection mechanism are deployed to ensure the reliability of the core control system. The trust network mechanism, malware detection mechanism, which consume large energy to calculate trust or system status, are deployed in enterprises management layer and control network of production monitoring layer which have better ability of computing and communication, to ensure the availability of the perimeter network.

Efficiency: Compared with previous protection method of ICS [5], the proposed method mainly increase trusted protection module (T), and the interface (I) with IPS and malicious code detection module, the time complexity degrees are $f(t(T))$, $f(t(I))$ respectively, where f is a function of time. In the intrusion monitoring stage, trusted protection module monitors system continuously, the time complexity of the proposed protection scheme (P) is $f(t(P))=f(t(T))=O(n)$, where n is the number of the deployed trusted modules. In the intrusion detecting phase, trusted protection detection, data and system protection testing will work. The complexity of trusted network computing is $O(n_1^2)$, where n_1 is the number of the transported nodes. The complexity of trusted data protection mechanisms is $O(n)+O(1)$, where $O(1)$ is the time of access monitoring for external attack from mobile devices occasionally. The complexity of the basic transaction of data and system detection is $O(n)$. Therefore, the time complexity in the intrusion monitoring stage is $f(t(P)) = f(t(T)) + f(t(I)) = O(n_1^2) + 2O(n) + O(1)$. The time complexity of post audit phase is $O(1)$. In aspect of space complexity, the proposed method increases some of the trusted management server and the corresponding data storage server, the space complexity is $mO(n)$, where m is the number of server, and n is the length of data vector of each server.

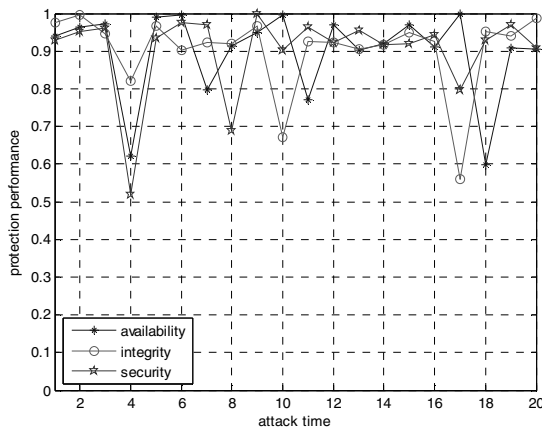
B. Simulation Analysis

In this section, simulation analysis is performed to further demonstrate the effectiveness and efficiency of the proposed protection method. Build the simulation environment, and deploy protection program according to the basic structure of Figure 2. Take the combination of Spirent Testcenter, Avalanche and ThreatEx as simulated attack method, and invade in the monitoring system 20 times. A successful attack is defined as reading and damaging control file of ICS.

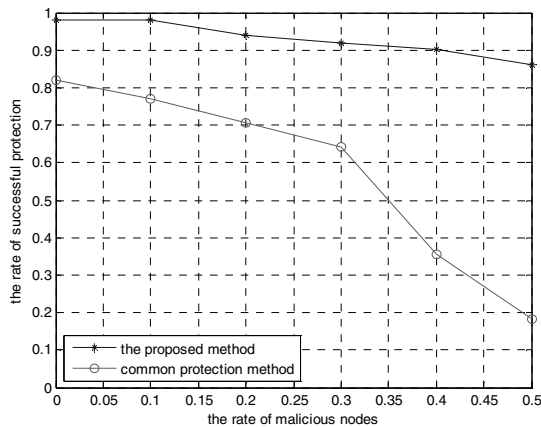
Function simulation: availability is described as the opposite of the weighted average probability between the proportions of which the part of the control server traffic flow exceed the basic flow RT relative to RT and the proportions of which the part of the delay exceed the basic control delay DT relative to DT . Integrity is described as probability of the control file not being destroyed. Security is described as probability of the control file not being obtaining or decrypting.

Effectiveness simulation: described as probability of successful attack. It is defined as the probability of successful protection (successful attack is described as a virus spreading to the field control node successfully.) The simulation results are shown in Figure 4.

Figure 4(a) describes the probability of the change of three functional features of the industrial control system along with the change of attacks number, it can be seen that the protection



(a) Function simulation



(b) Effectiveness simulation

Figure 4. Simulation results

program has certain reliability. Figure 4(b) describes the protective effect of the proposed method compared with common depth protection scheme [5], which indicates the effectiveness of the proposed protection scheme.

C. Comparison Analysis

Compared with the credible protection scheme for smart grid in [9] (shorted for Fadul scheme), the proposed method is more comprehensive. Fadul advocated the use of a reputation-based trust management system to mitigate network vulnerabilities (i.e. false trip breaker signal, malicious feedback) in future smart electric power grids. The trust system was deployed in smart grid devices based on a communication-based backup protection system. However, Fadul scheme is shortage in capability of anti-sudden attacks due to the poor sensitivity of reputation feedback. In terms of efficiency, reputation and trust management require an iterative calculation of multiple feedbacks from the overlapping network neighborhoods to calculate the trust values. The time complexity is close to $O(n^2)$, the space complexity is mn , where m is the length of history vector of entities, n is the number of entities. For the protective effect, Fadul' program has better security and availability as it adopted immune mechanism against malicious attacks based on reputation and reasonable distribution mechanism for communication bandwidth, whereas the integrity protection need improved.

Compared with the trusted network technology for control networks proposed by Okhravi [10], the proposed method has better architecture of trusted management. Okhravi improved the traditional process control network (PCN), introduced a trusted network architecture and implemented individual access control policies based on the trusted status of the hardware and software of devices when requested service. A group of authentication components and protocols constructed the trusted network (TN), and integrated into the PCN to form trusted process control network (TPCN). Some requirements were discussed, the availability was enhanced with redundant servers in the architecture. In terms of anti-attack, Okhravi method adopted authentication, authorization and access control (AAA) mechanisms and interaction protocol (e.g. HCAP) to avoid external intrusion, but for internal attack (e.g. information leakage intentionally) it is lack of flexible protection. In terms of efficiency, due to the implementation of several rounds of control strategies and agent communications, the time complexity surpasses $kO(n)$, where k is the complexity of access control policies and n is the number of entities inspected, the space complexity is $kO(n)$. In terms of protective effect, specific customization and architectural choices are introduced to increase the availability of the end devices and TPCN infrastructure, the integrity protection is missing, and trusted architecture and authentication reduces vulnerabilities to malware attacks, though internal attack need improved.

The compared analysis results are shown in TABLE 1. The proposed method is denoted as "new method". The performance of the protective effect is denoted as three levels: Good, medium, poor for the attributes. The performance of anti-attack is divided into two statuses: trusted and untrusted. Notice that, the results shown in TABLE 1 are relative

performance, taking the new method as the current evaluated criterion expect for the efficient column. It can be inferred from the table that the proposed method has better performance than others related programs.

TABLE 1. COMPARISON OF THREE PROTECTION METHODS

	external attacks	internal attacks	Efficient	availability	integrity
Fadul scheme	untrusted	untrusted	$O(n^2)$	good	poor
Okhravi method	trusted	untrusted	$kO(n)$	good	poor
New method	trusted	trusted	$\approx O(n)$	good	good

VII. CONCLUSIONS

This paper presented a trusted protection scheme of industrial control systems. Trusted computing platform, trusted data protection mechanism and trust network were deployed in the field device layer, production monitoring layer and enterprise management layer of ICS coordinately. Trusted protection technologies ensured trusted operation of ICS from aspects of systems, data lifecycle and network security, and immune to external attacks and internal leakage simultaneously. The availability of core control system is improved by lightweight layered deployment of protection architecture. The efficiency analysis, simulation analysis and comparison analysis show that the proposed scheme has better performance. As the trusted protection technologies integrated closely with essential characteristics of the control system, the proposed method can be deployed in heterogeneous industrial control systems.

REFERENCE

- [1] S. Mansfield-Devine, "Western energy firms come under concerted and successful cyber-attack," *Network Security*, vol. 2014, pp. 1-2, July 2014.
- [2] F. Kargl F, dHRW. Van, H Konig, A Valdes, MC Dacier, "Insights on the Security and Dependability of Industrial Control Systems," *IEEE Security & Privacy*, vol. 12, pp. 75-78, December 2014.
- [3] J. Eisenhower, P Donnelly, M. Ellis, "Roadmap to Secure Control Systems in the Energy Sector," Washington DC, USA: Energetics Incorporated, the US Department of Energy and the US Department of Homeland Security, 2006.
- [4] ICSJWG Roadmap Working Group, "Cross-Sector Roadmap for Cybersecurity of Control Systems," Washington DC, USA: U.S. Department of Homeland Security, 2011.
- [5] US-CERT, ICS-CERT[Z/OL], http://www.us-cert.gov/control_system/, June 2012.
- [6] A. Nagarajan, V. Varadharajan, "Dynamic trust enhanced security model for trusted platform based services," *Future Generation Computer Systems*, vol. 27, pp. 564-573, May 2011.
- [7] G. Daci, M. Shyle, "Improving data integrity and performance of cryptographic structured log file systems," *2011 3rd International Congress on Ultra-Modern Telecommunications and Control Systems and Workshops (ICUMT)*, vol. 5-7, pp. 1-5, 2011.
- [8] MA Fera, C. Manikandaprabhu, I. Natarajan, K. Brinda, R. Darathiprincy, "Enhancing Security in Cloud Using Trusted Monitoring Framework," *International Conference on Intelligent Computing, Communication & Convergence*, Procedia Computer Science, 2015, vol. 48, pp. 198-203.

- [9] J. Fadul, K. Hopkinson, C. Sheffield, J. Moore, T. Andel, "Trust Management and Security in the Future Communication-Based "Smart" Electric Power Grid," *Proceedings in 2011 44th Hawaii International Conference on System Sciences (HICSS)*, 2011, pp. 1-10.
- [10] H. Okhravi, DM. Nicol, "Application of trusted network technology to industrial control networks," *International Journal of Critical Infrastructure Protection*, vol.2, pp. 84-94, October 2009.



Jingpei Wang (E'14). He was born in Hubei Province of China in 1983, obtained a Bachelor degree in China Three Gorges University in Yichang, 2007. The major field of study is communication engineering. Then obtained the Master degree (Control Theory and Control Engineering) in the same University in 2010, and in 2014 earned the Doctor degree (information security) in Beijing University of Posts and Telecommunications.

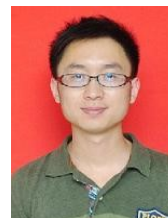
He joined the China CEPREI Laboratory in 2014, and became an Engineer (E) in 2014. He mainly engaged in the scientific and technical services of industrial control systems and information security. Current research interest is information security.



Jie Liu (E'89-SE'98-FE'11). He was born in Anhui Province of China in 1963. He obtained a Bachelor degree in Xi'an University of Electronic Science and Technology in Xi'an, China, 1983. The major field of study is computer technology.

He joined the China CEPREI Laboratory since 1983, and became an Engineer (E) in 1989, a Senior Engineer (SE) in 1998, and a Fellow of Engineers (FE) in 2011. Currently he is the director of information security research center, and engaged in the research and management of software reliability assessment and information security.

Professor Liu is an adjunct professor of South China University of Technology, the experts of China Software Industry Association, the member of SAC/TC24, the member of the Technical Committee of Chinese Institute of Electronics.



Shengming Yang (AE'13). He was born in Shanxi Province of China in 1985, obtained a Bachelor degree in Lanzhou University in Lanzhou, China, 2008. The major field of study is computer science and technology. Then he obtained the Master degree (information security) in Northwestern Polytechnical University in Xi'an, China, 2013.

He joined the China CEPREI Laboratory since 2013, and became an Assistant Engineer (AE) in 2013. He mainly engaged in the technical services related to information security, and the current research interests are information security and computer network.



M. Zhang received the B.S. degree in electronics and information engineering from Northwest Agriculture & Forestry University, Xi'an, China, in 2008, and M.S. degree in control engineering from Beijing Jiaotong University, Beijing, China, in 2012. She is currently working toward the Ph.D. degree in information and communication engineering at quantum information laboratory of Northwestern Polytechnical University, Xi'an, China. Her

current research is focused on the quantum information process and quantum communication, especially the quantum secure communication and quantum signature.