Review on Information Security of Industrial Control Systems

Wang Mingqian[1,2]，Gu Weijie[1,2]

1 School of Information Engineering, Changzhou Vocational Institute of Mechatronic Technology，Changzhou, Jiangsu Province，P.R.China

2Jiangsu Internet of Things and Manufacturing Information Engineering Technology Research and Development Center，Changzhou, Jiangsu Province，P.R.China

[1]wmq1989219@126.com, [2] 51956630@qq.com

***Abstract*—**Industrial control systems (ICS) are widely used in critical infrastructure such as national water resources, power, transportation, energy and so on. These important industrial systems have a profound impact on national security and economic development. In recent years, the occurrence of various security incidents and their serious consequences further reflect the seriousness of the information security situation of industrial control systems. In this paper, the current situation of information security in industrial control systems is summarized and analyzed. The existing problems in ICS information security and the corresponding measures taken are focused on. Further more, the problems to be solved and the development direction are pointed out.

***Key words*—**"Industrial Control System (ICS); Data Acquisition and Monitoring System (SCADA); Information Security".

I.INTRODUCTION

Key industrial infrastructure constitutes an important foundation of our national economy, modern society and national security, such as water conservancy, electricity, transportation, energy and important industrial systems. Their security directly affects the production, life and people's life and property security. The early industrial control system was isolated from the outside world and was not easily threatened by security because of its special system and communication mechanism. With the deep integration of informationization and industrialization and the rapid development of the Internet of Things, the industrial control system entered the stage of network control with SCADA, DCS and PLC as the main parts. Fieldbus Technology and industrial Ethernet became its core communication mechanism.

The fierce market competition promotes the openness of industrial control network to furtherly expand in order to obtain the latest information and make fast and efficient decisions. However, the integration of industrial control network and enterprise information network, the connection of information network and Internet, and the general systems, software, hardware and protocols bring openness and compatibility. At the same time, bring many industrial control network systems. Information security risks and threats. Viruses, Trojans, worms, hackers and other serious threats to the security of industrial control networks, the situation is becoming increasingly grim. In October 2010, the Stuxnet virus, which ravaged Iran, delayed power generation at the Bushehr nuclear power plant and had a large impact on

Iran's domestic industry, arousing the attention of governments and security agencies [1]. Information battlefield has been transferred from traditional network to industrial network with stronger influence and destruction. Information security of industrial control network has been upgraded to a new strategic level. On October 27th, 2011, the Ministry of Industry and Information Technology issued the Notice on Strengthening the Information Security Management of Industrial Control Systems, emphasizing the importance and urgency of strengthening the information security management of industrial control systems. Therefore, it is of great significance to study the information security of industrial control network system.

This paper summarizes the information security status of industrial control network system, summarizes and introduces the information security loopholes, security threats, current status and problems of industrial control system information security, and discusses the measures and methods to ensure the information security of industrial control network, and puts forward the problems to be solved and future research directions.

II.Information Security Vulnerabilities in Industrial Control Networks

Like the Internet, the rapid development of industrial control network has gradually exposed some information security vulnerabilities, mainly in the following areas [51] as shown in Figure 1.

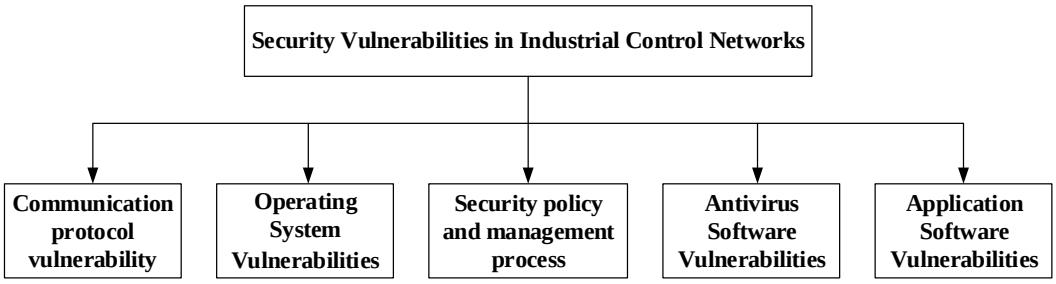

Figure 1. Type of Security Vulnerabilities in Industrial Control Networks

A. Communication protocol vulnerability

TCP/IP protocol and general protocol such as OPC (OLE for Process Control) are more and more used in industrial control network, and their communication protocol vulnerabilities are becoming increasingly prominent. For example, the use of an unstable dynamic port number (any of 1024-65535 ports) in OPC communications leads to the failure of traditional IT firewalls based on ports or IP addresses to ensure their security [12].

B. Operating System Vulnerabilities

At present, most Engineer stations/operating stations of industrial control systems are based on Windows platform. In order to ensure the stability of the control system, this kind of system usually does not install any patches on Windows platform, thus burying potential safety hazards.

C. Security policy and management process vulnerabilities

Many industrial control systems do not adopt complete and effective security strategies and management processes for ease of use, which also poses a threat to the information security of industrial control systems. For example, without setting access control policies for mobile storage media, viruses and Trojans may spread through this way.

D. Antivirus Software Vulnerabilities

In order not to affect the availability of the system, many industrial control system operating stations usually do not install anti-virus software. Even if antivirus software is installed, its virus library is not updated frequently. These vulnerabilities are vulnerable to virus attacks.

E. Application Software Vulnerabilities

Due to the diversity of application software, it is difficult to form a unified protection specification to deal with security problems. Usually network-oriented application software needs open application ports. If these designs are vulnerable and controlled by intruders, it may bring disaster.

III.Security Threats to Industrial Control Networks

Industrial control network is a kind of communication network that organizes all production processes and automation control systems in the whole factory into a whole through various communication devices. The definition of information security in IEC 62443 [3] for industrial control systems is as follows: (a) measures taken to protect the system; (b) system state obtained by measures taken to establish and maintain the protection system; (c) freedom from unauthorized access to system resources and unauthorized or accidental changes, damage or losses; (d) ability of computer systems to ensure unauthorized personnel and systems. It can neither modify software and its data nor access system functions, but ensure that authorized personnel and systems are not blocked; (e) prevent illegal or harmful intrusion into industrial control systems, or interfere with their correct and planned operation.

However, there are many security vulnerabilities in industrial control networks, which are often attacked by internal (unsatisfactory employees) or external (industrial spies, competitors, hackers, etc.), mainly in the following aspects [3]:

A. Denial of service attack

Denial-of-service attack is one of the most common attacks by attackers, which is shown in Figure 2. It is an attack that tries to stop the target machine from providing services. Once the control network suffers serious denial-of-service attacks, it will lead to the paralysis of the operation station services and the interruption of communication with the control system, with extremely serious consequences.

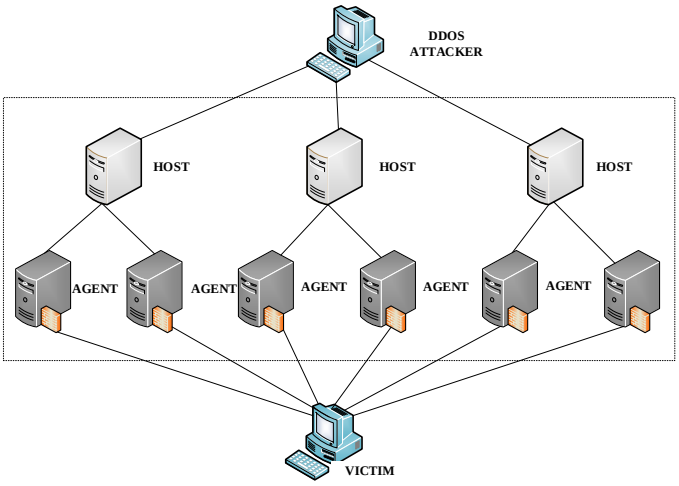

Figure 2 Denial-of-service attack

B. Man-in-the-middle attack

As presented in Figure 3, Man-in-the-middle attack is an active way of eavesdropping information. In this way, the attacker establishes a connection with the victim computer and transmits information between the victim computers. On the premise of understanding the communication protocol of the control system, attackers often use ARP spoofing or DNS spoofing to implement man-in-the-middle attack. Such attacks can lead to the leakage of internal information.

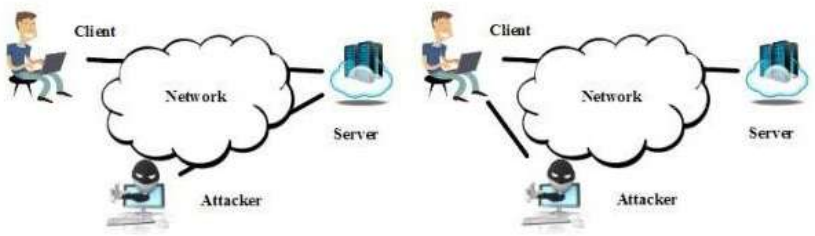

Figure 3. Man-in-the-middle attack

C. Viruses, worms, Trojans

These are the most vulnerable security threats at present. Viruses are self-replicating computer programs that use vulnerabilities in systems or software to implant victim hosts and spread across the network. Worms differ from viruses in that they do not need to be attached to other programs and can exist independently. The ultimate goal of Trojan Horse is to enable unauthorized users to access the system. This kind of malicious code will make the control system unable to work properly, causing serious security incidents, highly destructive.

D. SQL Injection Attack

Database application has become the core component of control system and related accounting tools. SQL (Structured Quevy Language) injection attack is an attack that an attacker exploits a vulnerability in an application to obtain data. Due to the high dependence of industrial control system on the accuracy of data storage and control data, and the wide application of SQL database, this attack has become the number one threat to the safety of industrial control network. The procedure of SQL Injection Attack is given in Figure 4.

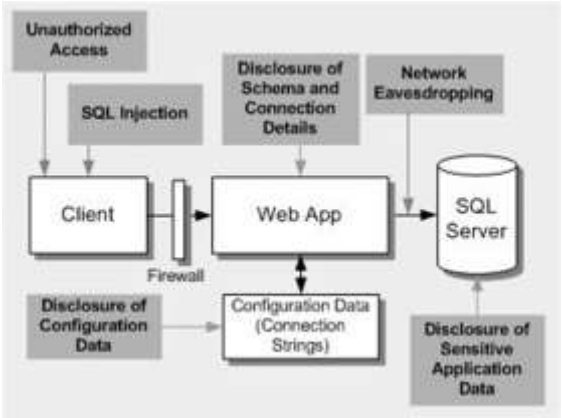

Figure 4. SQL Injection Attack

E. Illegal visits

Industrial espionage (unauthorized remote users access enterprise intranet resources, such as confidential information in competitors' equipment), hacker attacks or sabotage

activities (mainly based on the availability of known connections to achieve the interception, tampering, forgery, redistribution of data information and production instructions transmitted in the control network).

Thus, industrial control network system is threatened by various attacks, and information security is facing great challenges.

IV.Current Situation and Problems of Information Security in Industrial Control Network System

A. Ideas and management

Safety is not a technical problem at first, but is more influenced by managers' concepts and management level. Many enterprise managers are weak in information security awareness of industrial control network, the corresponding security management mechanism and security strategy are not perfect, and staff lack specialized security training.

B. Institutions and standards

At present, China has not yet formulated laws and regulations on industrial control network security, lacking institutional guarantee. However, developed countries such as the United States and the international community attach great importance to the information security of industrial control networks, especially the data acquisition and monitoring system (SCADA), and have formulated a series of security standards as the basis for the formation of security strategies and frameworks of industrial control network systems.

NERC CIP (North American Electricity Security Organization, Key Infrastructure Protection) Regulation is the first sanctioning network security standard, which has a far-reaching impact on large power system organizations [4]. The U.S. government attaches great importance to information security in the energy sector, such as electricity, and elevates it to a high level of national security. Therefore, in January 2006, the U.S. Department of Energy and the Department of Homeland Security jointly released Roadmap to Secure Control Systems in the Energy Sector [5]. Meanwhile, the United States Department of Homeland Security (DHS) launched the Control System Security Program (CSSP) [6-7]. The International Standards Administration of the United States (ISA) formulates the ISA 99 standard, which provides detailed instructions for the establishment and implementation of security plans for control systems [8]. The National Institute of Standards and Technology (NIST) of the United States has developed safety guidelines for SCADA systems and industrial control systems [9-10].

IEC/TC65/WG10 (Working Group on Industrial Process Measurement, Control and Automation/Network and System Information Security) and ISA 99 of IA set up a joint working group to jointly formulate IEC 62443 International Standards for Industrial Process Measurement, Control and Automation Network and System Information Security [11,12].

However, the international information security assessment and certification for industrial control systems is still in its infancy, there is no unified evaluation criterion, and there is a lack of criteria that can really be used for information security assessment of industrial control systems.

C. Technology and Finance

Unlike the information security technology of general IT network, the security design of

industrial control network system should first ensure the availability, real-time and reliability of the system. Most security measures, such as system vulnerability scanning, patch updating, IDS intrusion detection and anti-virus software operation, data encryption and key management, will occupy system resources, resulting in additional overhead, which may reduce the performance of the control system [13]. Therefore, the design of reasonable, feasible and effective industrial control network security protection technology has posed a huge challenge.

In addition, the implementation of the security mechanism of industrial control network system also requires a large amount of funds for risk assessment, configuration of corresponding security equipment, maintenance and updating of system components and so on. With the frequent occurrence of industrial control system security incidents and serious consequences in recent years, the government, society and enterprises began to attach importance to the information security of industrial control network, and increased financial investment.

V.Measures and Methods to Guarantee the Information Security of Industrial Control Network

Protecting the hardware and software and their data in the network system from being destroyed, altered or leaked by accident or malicious reasons, ensuring the continuous and reliable operation of the system and uninterrupted network services have become the main content of industrial control network security [14]. Therefore, in view of the information security problems in the above industrial control network system, it is necessary to formulate corresponding security protection strategies and methods on the basis of considering the particularity of industrial control network, especially the real-time and reliability requirements.

A. Security framework

Safety protection measures generally accepted in the field of industrial control refer to the relevant requirements of the international industry standard ANSI/ISA-99. It divides the control equipment with the same function and safety requirements into the same area, and carries out pipeline communication between regions. Also, it achieves three major objectives of industrial network security protection by controlling the communication content in the pipeline between regions: regional isolation, communication control and real-time. Alarm, so that failure problems can be quickly found and solved in the original area, to ensure the stable operation of the control system [1]. According to the requirements of this standard，The strategy of "defense in depth" for industrial control network system is put forward by Kuipers [15]. The network is divided into different security zones and industrial firewalls are installed in the border areas. Wang Hao et al. established a DMZ (Demilitarized Zone) model based on regional security between the enterprise information network and the control network to protect the security of the control network as an agent area [16]. Li Jianjun et al.[17] constructed a security interface model between the information network and the control network. The interface area uses UTM integrated gateway, and the data to be exchanged is synchronized to the pre-server in the area in real time, waiting to be accessed.

B. Risk assessment

Risk assessment of industrial control network system is the basis of formulating security strategy and configuring security technology [13]. Therefore, it is of great significance to accurately analyze the security risks in the control network. Risk assessment is a multi-stage process, including risk identification, analysis, evaluation and rating, management and response [18]. Article [19] provides a commercial system, Risk Watch, for qualitative or quantitative analysis of security vulnerabilities of systems. In paper [20], a threat model is established by FTA, and a framework OCTAVE for identifying and managing information security risks is given. In paper [21], fault tree graph analysis (FTA) and failure mode effect and consequence analysis (FMECA) are used to propose a model-based risk analysis method for important safety systems, CORAS.

Lopez [22] points out that the most difficult part of risk assessment is risk characterization analysis. As the most comprehensive risk identification methodology, HHM (hierarchical holographic modeling) can identify all risk sources in SCADA system [23-25]. Haimes et al [26] described a priority-based risk filtering, rating and management method, RFRM, on the basis of HHM risk identification. In paper [27] and [28], IIM (inoperability input-output model) is used to quantify the effectiveness of risk management. Probabilistic Risk Assessment (PRA) is a systematic and comprehensive quantitative risk analysis method, which includes many kinds of analysis methods, such as FTA, attack tree analysis, ETA, vulnerability tree analysis, failure mode and impact analysis (FMEA), failure mode impact and critical analysis (FMECA), causality analysis (CCA). Quantitative risk assessment can quantitatively explain the possibility and degree of risk of the evaluation object, and accurately describe the risk of the system. It is the focus and direction of the current industrial risk assessment of control system.

C. Security Policy and Management

At present, the security strategies of typical industrial control network systems include [29]: attaching importance to the security of the whole life cycle of industrial control systems from structure to purchase, installation, maintenance to outage. Adopting multi-layer network topology structure to make the most critical communication in the most secure and reliable layer and isolating network according to function and security level, using virtual local area network (VLAN) And Virtual Private Network (VPN). Ensure that key devices are redundant and set up redundant network; Stop unused ports and services after testing without affecting the operation of industrial control network system. Restrict external access to industrial control network and equipment, such as notebook computers and mobile storage media. Defining the authority of different users of industrial control system. Confidential letter Information and instructions are encrypted and authenticated; data storage and backup in network system.

The key management problem caused by encryption and authentication is related to the system overhead of industrial control network and affects its control performance. On the basis of SKE [30], SKMA [31] and ASKMA [32] key management methods, Choi et al. proposed ASKMA+, which reduced the number of key storage in remote terminals and the computational overhead in communication. Kang et al. [34] adopted the decentralized key

distribution mechanism, and used the QoS benefit function to solve the optimal number of keys and the distribution cycle, so as to reduce the system overhead of key management.

D. Security Defense Technology

Typical information security protection technologies include the following contents: Firewall, IDS, Access Control, Enryption, Antivirus and so on. In the industrial control network system, it is necessary to design a special security defense technology based on the traditional IT information security technology according to its characteristics, characteristics and requirements.

Intrusion detection system monitors the behavior of host and network in real time, and sends an alarm signal as soon as abnormal behavior is found. But the embedded intrusion detection and anti-virus software needs frequent updates, and system monitoring and scanning will also occupy system resources, affecting the real-time performance of the control network. In order to solve this problem, Zhang Shuai et al. [35] proposed an ICS threat recognition model based on private cloud technology, which put the process of intrusion detection and virus detection into the cloud with security mechanism for processing, without occupying the system resources of the control network. Jeffrey et al. [36] designed an intrusion detection tool, PFP (Power Fingerprinting), which can produce negligible overhead independent of the software and hardware of the operating system and system. Naedele takes security devices including intrusion detection, firewall, access control and anti-virus software as the access terminal of the controller to protect the peripheral without affecting the system operation, but this method can not resist physical access attacks on the controller [37]. A similar method is to build the same image system as the control system and scan the vulnerability of the image system.

Effective intrusion detection method for industrial control network system is also one of the research hotspots. Zhang Yungui et al. [38] proposed a non-parametric CUSUM intrusion detection method based on industrial control model. Using the input and output characteristics of ICS, a mathematical model was established to predict the output of the system, and the difference between the model and the actual measured signal was calculated. Tsang et al. established a multi-agent IDS [39] based on bio-inspired learning model [40]. Based on the regularity and stability of industrial Ethernet Modbus TCP network, the system behavior is characterized and the IDS based on anomaly detection is adopted. Berman et al. [41] used Gumstix technology to simulate the field equipment of industrial control network, to characterize the possible attack behavior, as the basis of IDS based on feature detection.

In addition, scholars at home and abroad have also conducted in-depth research on other protective measures. Li Aiguo et al. [42] proposed to overcome the problem of information security in traditional industrial Ethernet by using the characteristics of multi-hosting and multi-streaming SCTP protocol. Paper [43] Aiming at the characteristics of smart grid, an improved method based on PKI technology is adopted to access control [37]. It is pointed out that the control system should have the switching mechanism of emergency mode and security mode, and can enter the control system without hindrance through the host authentication step in an emergency. Sun et al. [44] adopted EPON as the communication mode of distributed automation system, and used equipment mutual authentication algorithm

based on symmetric key. In paper [45], the standard cryptographic protocol IEEE P1711 based on the network security of substation serial links is used to flexibly select cryptographic components and configure cryptographic overhead according to system requirements. The American Gas Association (AGA12) proposes a fast encryption method for SCADA system, which reduces the execution time of the encryption system [46,47,48]. Fang et al. proposed a malicious code analysis framework based on ICS attack graph model [49]. Paper [50] uses Co-evolutionary Genetic Algorithm to balance the security and real-time performance of networked control systems.

VI.Problems and Development Directions Still to be Solved

Although there are many standards and strategies to guarantee the information security of industrial control network system, some problems that are difficult to resolve still exist. Such as the contradiction between the frequent updating of system software and the requirement of continuous and efficient operation of control system. The contradiction between security and real-time caused by the system overhead of embedded security software. In addition, there is still a lack of uniform and effective safety assessment and verification standards in industrial control network system.

In the future, how to use complex system theory to model industrial control systems will be studied. The interdependence between industrial control systems and the impact of industrial control systems on interdependent key infrastructure will also be furtherly researched. At the same time, it must be considered that the impact and consequences of information security incidents in industrial control systems on key infrastructure, as well as on macroeconomic, national security and social production and life. Macro-management and decision-making of information security in industrial control systems are major challenges and research directions in the field of information security in industrial control systems.

VII.Conclusion

This paper summarizes the information security status of industrial control network system, and points out the difficulties and development trend of the research. Firstly, the information security loopholes in the industrial control system are analyzed, and the various security threats faced by the industrial control system are expounded from the perspective of external attacks. Secondly, the status quo and existing problems of the information security in the industrial control system are summarized and analyzed. Finally, the information protection of the industrial control network is discussed from the aspects of security framework, risk assessment and security defense technology. It is hoped that this study can provide a bridge for researchers engaged in industrial control information security to understand current situation, key technologies and research directions of industrial control systems.

CKNOWLEDGMENT

The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

This work is supported by the Changzhou Key Laboratory of Industrial Internet and Data Intelligence (No.CM20183002), Innovation and Entrepreneurship Training Program for

College Students of Jiangsu Province (Grant No.: 201913114004Y), the Project of Changzhou Vocational Institute of Mechatronic Technology.

REFERENCE

1. Falliere, N., Murchu, L. O., Chien, E., W32. Stuxnet Dossier[Z]. http://www.symantec.com/content/en/ us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf, November 2010.
2. Li Yumin. Protection Measures and Application of Information Security in Industrial Control Network[J].China Instruments and Instruments, 2012, 11: 59-64.
3. IEC. IEC 62443-2-1Edition 1.0, Industrial communication networks–Network and system security–Part 2-1: Establishing an industrial automation and control system security program[S]. Geneva: IEC, 2010.
4. NIST SP800-82. Guide to Industrial Control System (ICS) Security[S]. Gaithersburg, USA: National Institute of Standards and Technology (NIST), 2011.
5. Ray A, Åkerberg J, Björkman M, et al. Future research challenges of secure heterogeneous industrial communication networks[C]. IEEE International Conference on Emerging Technologies & Factory Automation, 2016.
6. DHS CSSP. Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-DepthStrategies[S]. http://www.us-cert.gov/control_systems/practices/documents/Defense_in_De pth_Oct09.pdf, October 2009.
7. DHS CSSP. Common CyberSecurity Vulnerabilities in Industrial Control Systems[S]. http://www.us-cert.gov/ control_systems/practices/documents/DHS_Common_Cybersecurity_Vulnerabilities_IC S_2010.pdf, May 2011.
8. ANSI/ISA-99.01.01-2007. Security for Industrial Automation and Control Systems: Terminology, Concepts and Models[S]. Los Angeles, USA: The International Society of Automation (ISA), 2007.
9. Stouffer, K., Falco, J., Kent, K. Guide to supervisory control and data acquisition (scada) and industrial control systems security[S]. Sp800-82,NIST, September 2006.
10. Stouffer, K., Falco, J., Scarfone, K. Guide to Industrial Control Systems (ICS) Security[S], http://csrc. nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf, 2011.
11. Wollschlaeger M, Sauter T, Jasperneite J. The Future of Industrial Communication: Automation Networks in the Era of the Internet of Things and Industry 4.0[J]. IEEE Industrial Electronics Magazine, 2017, 11(1):17-27.
12. Sheela S J, Suresh K V, Tandur D. Security of Industrial Wireless Sensor Networks: A review[C]. International Conference on Trends in Automation, 2016.
13. Coffey K, Smith R, Maglaras L, et al. Vulnerability Analysis of Network Scanning on SCADA Systems[J]. Security & Communication Networks, 2018, 2018(4):1-21.
14. Vizarreta P, Bemten A V, Sakic E, et al. Incentives for a Softwarization of Wind Park Communication Networks[J]. IEEE Communications Magazine, 2018, PP(99):1-7.
15. Genge B, Haller P, Kiss I. Cyber-Security-Aware Network Design of Industrial Control Systems[J]. IEEE Systems Journal, 2017, 11(3):1373-1384.
16. Wang Hao, Wu Zhongfu, Wang Ping, Research on Industrial Control Network Security Model[J].Computer Science, 2016, 34(5): 96-98.
17. Li Jianjun, Yu Wenjin, Ji Qi, Analysis of the Security Data Interface Model between Enterprise Management and Control Network[J].Computer Age, 2009, 9: 74-76.
18. Ralston, P. A. S., Graham, J. H., Hieb, J. L., Cyber security risk assessment for SCADA

and DCS networks[J]. ISA Transactions, 2017, 46: 583-594.
19. Genge B, Haller P, Kiss I. Cyber-Security-Aware Network Design of Industrial Control Systems[J]. IEEE Systems Journal, 2017, 11(3):1373-1384.
20. Alberts, C., Dorofee, A., Stevens, J., Introduction to the OCTAVE Approach. CERT Coordination Center[Z], http://www.cert.org/octave/approach intro.pdf; 2013.
21. Aagedal, J., BraberB, F. D., Dimitrakos, T., Model-based risk assessment to improve enterprise security[C]. In Proceedings of the sixth international distributed object computing conference, 2002: 51-62.
22. Genge B, Haller P, Kiss I. Cyber-Security-Aware Network Design of Industrial Control Systems[J]. IEEE Systems Journal, 2017, 11(3):1373-1384.
23. Cheminod M, Durante L, Seno L. Performance evaluation and modeling of an industrial application-layer firewall[J]. IEEE Transactions on Industrial Informatics, 2018, (99): 1-1.
24. Do V L, Fillatre L, Nikiforov I, et al. Feature article: security of SCADA systems against cyber–physical attacks[J]. IEEE Aerospace & Electronic Systems Magazine, 2017, 32(5):28-45.
25. Chittester, C. G., Haimes, Y. Y., Risks of terrorism to information technology and to critical interdependent infrastructures[J]. Journal of Homeland Security and Emergency Management, 2014, 1(4): 1-6.
26. Haimes, Y. Y., Kaplan, S., Lamber, J. H., Risk filtering, ranking, and management framework using hierarchical holographic modeling[J]. Risk Analysis, 2012, 22(2): 381–95.
27. Haimes, Y. Y., Chittester, C. G., A roadmap for quantifying the efficacy of risk management of information security and interdependent scada systems[J]. Journal of Homeland Security and Emergency Management, 2015, 2(2): Article 12.
28. Crowther, K. G., Haimes, Y. Y., Application of the inoperability input–output model (IIM) for systemic risk assessment and management of interdependent infrastructures[J]. Systems Engineering, 2015, 8(4): 323-341.
29. Fang Laihua, Information Security of Industrial Control System[J].Electrical Era, 2018, 10: 88-121.
30. Beaver, C., Gallup, D., Neumann, W., Key Management for SCADA[Z]. http://sandia.org/scada/docum ents/013252.pdf, 2012.
31. Colin, R. D., Boyd, C., Manuel, J., KMA-A key management architecture for SCADA systems[C]. In Proceedings of 4th Australasian Information Security Workshop, 2016:138-192.
32. Choi, D., Kim, H., Won, D., Advanced key management architecture for secure SCADA communications[J]. IEEE Transaction on Power Delivery, 2009, 24(3): 1154-1163.
33. Choi, D., Lee, S., Won, D., Efficient Secure Group Communications for SCADA[J]. IEEE Transaction on Power Delivery, 2010, 25(2): 714-722.
34. Kang, D. J., Lee, J. J., Kim, B. H., Proposal strategies of key management for data encryption in SCADA nework of electric power systems[J]. Electrical Power and Energy Systems, 2011, 33: 1521-1526.
35. Zhang Shuai, Safety Risk Analysis of ICS Industrial Control System[J].Computer Safety, 2012, 1: 15-19.
36. Jeffrey, D., Reed, H., Carlos, D., Aguayo, G. R., Enhancing Smart Grid Cyber Security using Power Fingerprinting: Integrity assessment and intrusion detection[C]. In Proceedings of Future of Instrumentation International Workshop, 2012: 1-3.
37. Naedele, M., Addressing IT Security for Critical Control Systems[C]. In Proceedings of 40th Annual Hawaii International Conference on Systems Science, 2017: 115-122.
38. Zhang Yungui, Zhao Hua, Wang Lina, Nonparametric CUSUM Intrusion Detection

Method Based on Industrial Control Model[J]. Journal of Southeast University: Natural Science Edition, 2012, 42(S1): 55-59.
39. Tsang, C. H., Kwong, S., Multi-agent intrusion detection system in industrial network using ant colony clustering approach and unsupervised feature extraction[C]. In the proceedings of IEEE international conference of Industrial Technology, 2015: 51-56.
40. Cheung, S., Dutertre, B., Fong, M., Lindqvist, U., Skinner, K., Using Model-based Intrusion Detection for SCADA Networks[Z]. http://www.csrdc.us/papers/scadaTDS07/SCADA-IDS-S4-2007. pdf, 2017.
41. Berman, D., Butts, J., Towards Characterization of Cyber Attacks on Industrial Control Systems: Emulating Field Devices Using Gumstix Technology[C]. In Proceedings of 5th International Symposium on Resilient Control Systems (ISRCS), 2012: 63-68.
42. Li Aiguo, Application of SCTP in Industrial Ethernet Communication Technology[J].Modern Electronic Technology, 2011, 34(3): 160-162.
43. Lee S, Lee S, Yoo H, et al. Design and implementation of cybersecurity testbed for industrial IoT systems[J]. Journal of Supercomputing, 2017(20):1-15.
44. Gungor V C, Hancke G P. Industrial Wireless Sensor Networks: Applications, Protocols, and Standards[J]. Crc Press, 2017, 81:1-2.
45. Hurd, S., Tutorial: Security in Electric Utility Control Systems[C]. In proceedings of 61st Annual Conference of Protective Relay Engineers, 2018: 304-309.
46. Ding D, Han Q L, Wang Z, et al. A Survey on Model-Based Distributed Control and Filtering for Industrial Cyber-Physical Systems[J]. IEEE Transactions on Industrial Informatics, 2019, 99(99):1-16.
47. American Gas Association, Cryptographic protection of SCADA communications: Background, policies and test plan[R]. AGA Report No.12, part 1, http://www.gtiservices.org/security/aga12 wkgdoc homepg.shtml, March 2016.
48. Pan F, Pang Z, Luvisotto M, et al. Physical-Layer Security for Industrial Wireless Control Systems: Basics and Future Directions[J]. IEEE Industrial Electronics Magazine, 2018, 12(4):18-27.
49. Fang, L., Miao, Q., Wang, C. L., Toward an Analysis Framework for Industrial Control System Malicious Code[J]. IEEE Transaction on Industrial Electronics, 2011: 164-169.
50. Addo-Tenkorang R, Helo P T. Analysis of enterprise supply chain communication networks in engineering product development[J]. International Journal of Logistics Management, 2017, 28(1):47-74.
51. Qingdao Dofino Information Security Technology Co., Ltd. Analysis and Solution of Hidden Danger of Industrial Network Information Security[Z], http://www.gongkong.com/company/solution/201212270951590 0001.htm, 2012.12