DOI 10.15302/J-SSCAE-2021.02.009

Development of industrial Internet Security Technology in China

Dong Yue[1], Wang Zhiqin[2], Tian Huirong[1] , Li Shan[1], Qin Guoying[1], Wushour Silamu[3]

1. Institute of Security Research, China Academy of Information and Communications Technology, Beijing 100191, China
2. China Academy of Information and Communications Technology, Beijing 100191, China
3. College of Information Science and Engineering, Xinjiang University, Urumqi 830046, China

Abstract: With new-generation information technologies, such as cloud computing and big data, deeply integrating with traditional industrial operation technologies, the industrial Internet has become a new driving force for the digital transformation of industrial enterprises. However, industrial Internet security problems have increased; therefore, improving the technological capabilities for guaranteeing industrial Internet security becomes a prerequisite for the high-quality development of the industrial Internet. In this study, we first analyze the demand for industrial Internet development and summarize the development status of industrial Internet security protection, evaluation, and monitoring technologies. Subsequently, we investigate the development trends, technological difficulties, and challenges for the industrial Internet security technology and propose key technologies and their development approaches. To promote the safe and healthy development of industrial Internet in China, the industrial Internet security technologies need to be customized in accordance with industrial characteristics and scenarios. They should also closely integrate with new technologies such as big data and AI to achieve active defense and create endogenous security capabilities.

Keywords: industrial Internet security; security protection technology; security evaluation technology; security monitoring technology

1 Introduction

As computer and network technologies continue to develop, new-generation technologies such as Internet, big data, and artificial intelligence (AI) are being increasingly integrated into the real economy. Under such a development background, the industrial Internet has become a key support for many developed and emerging developing countries to seize development opportunities and accelerate strategic deployment [1,2]. China attaches great importance to the safe and efficient development of the industrial Internet. 2021 Chinese Government Work Report proposes the development of industrial Internet and the building of more generic technology research and development (R&D) platforms. In traditional industrial production, the work environment is relatively closed and trusted. With the development of industrial Internet, the industrial manufacturing industry is witnessing an opening up of work environment. Meanwhile, conventional Internet security threats have gradually penetrated into the industrial sectors, resulting in intertwined security issues, complex security situations, and increasing security risks [3,4].

Industrially developed countries, represented by the United States and Germany, and certain internationally renowned companies are putting vigorous efforts to promote the transformation of industrial Internet security technologies from strategic planning to deployment and implementation. The efforts have focused on the practical

Received date: January 22, 2021; **Revised date:** March 17, 2021

Corresponding author: Tian Huirong, senior engineer from the Institute of Security Research, China Academy of Information and Communications Technology. Major research fields is industrial Internet security. E-mail: tianhuirong@caict.ac.cn

Funding program: CAE Advisory Project “Strategic Research on the Development of the New-Generation Industrial Internet Security Technologies” (2020-XZ-02)

Chinese version: Strategic Study of CAE 2021, 23 (2): 065–073

Cited item: Dong Yue et al. Development of Industrial Internet Security Technology in China. *Strategic Study of CAE*, https://doi.org/10.15302/J-SSCAE-2021.02.009

application of industrial Internet security technologies [5,6]. To stimulate the application of the industrial Internet security framework in the industry, the United States has issued a series of white papers and user guides to guide relevant enterprises in deploying industrial Internet security protection measures.Germany and Japan launched the Reference Architecture Model Industrie 4.0 and the Industrial Value Chain Reference Architecture, respectively. In both architectures, industrial Internet security is considered an important component for the overall design. CyberX, an industrial cybersecurity company in Israel, has launched a security service that predicts the attack vector of industrial control systems (ICSs). Kaspersky Lab released threat predictions for industrial security in 2019, focusing on the cyber-security challenges faced by the industrial sectors [7].

Although research on industrial Internet security technologies started late in China, it has quickly caught up, focused on improving the top-layer design of industrial Internet security to guide the development of security technologies and the industrial Internet security industry. In 2019, the Ministry of Industry and Information Technology of the People's Republic of China jointly issued the *Guiding Opinions on Strengthening the Work on industrial Internet Security* with other nine government bodies. According to the Guiding Opinions, efforts should focus on industrial Internet security to strengthen the R&D of security operations such as attack prevention, vulnerability mining, and situation awareness, and to explore the use of new technologies such as AI, big data, and blockchain to improve the security protection level. In addition to relying on traditional network security technologies to expand the functions of security technology products, China also focuses on the R&D and innovation of new-generation network security technology products based on emerging Internet technologies. Related research mainly investigates the industrial Internet edge endpoint protection technology [8], industrial firewall technology [9], industrial Internet vulnerability mining technology [10], penetration testing technology [11], and security situation awareness technology [12]. Most of the research focuses on the analysis and application of a single technology. Considering there is a lack of research that systematically summarizes and classifies industrial Internet security technologies, this study analyzes the development needs of industrial Internet security technologies in depth, systematically reviews the development status of such technologies, and summarizes the development trends, existing problems, and approaches to tackling the problems in key technologies. Finally, on the basis of this, countermeasures and suggestions are proposed.

2 Demand analysis for industrial Internet security technologies

Traditional ICSs work in closed and trusted environments. They adopt a double-layer and three-level defense system and a hierarchical and domain-based isolation idea; thus, they generally lack the ability to defend against network attacks. With the development of industrial Internet, industrial equipment has become intelligent, and relevant services such as business migration to cloud and enterprise collaboration have emerged. The deep integration of the Internet into production components and services in industrial enterprises has resulted in conventional Internet security threats such as viruses, Trojan horses, and advanced persistent threats (APTs) spreading to industrial enterprises (Fig. 1). In contrast to the traditional Internet, which focuses on information security protection, the industrial Internet needs to integrate information security closely with functional security and interweave traditional industrial control security and Internet security. Therefore, industrial Internet security is a more complicated affair.

2.1 The confrontation between network attack and defense continues to escalate, and the industrial Internet has become a major target of attacks

The probability of industrial Internet-related systems being successfully attacked is 12%, which is much higher compared with e-government systems (1%) and the communications industry (5%) [13]. With the continuous escalation of confrontation between network attack and defense, network attacks have also shown some new characteristics: (1) Attack technologies are becoming more sophisticated, transforming from a single attack to a combination of multiple complicated attack technologies. (2) Attacks have become more targeted. In the past, attacks were launched mostly for gaining benefits, without any fixed targets. However, APTs have now become the main attack method. In particular, attacks are mostly targeted and remain latent for a long time; thus, they are difficult to detect. (3) Attack actors have changed from non-state actors to state actors. In particular, the security risks of state-level network attacks have been intensified. Attacks are frequently conducted against important sectors such as energy and electricity, which has a direct impact on industrial production, residents' lives, stable economy and society, and even national security [14].

To effectively defend against external cyber attacks, the industrial Internet needs to continuously improve technological capabilities. Driven by the security protection needs of industrial enterprises, industrial Internet security protection technologies are on a path of continuous development and innovation. For example, border protection adopts border control technologies such as industrial firewalls and white-list mechanisms; industrial mainframe protection needs to adopt the mainframe reinforcement technology that integrates identity authentication and access control. In view of the leakage risks of industrial Internet data, industrial Internet data security protection technologies such as data confidentiality and data loss prevention (DLP) should be adopted.

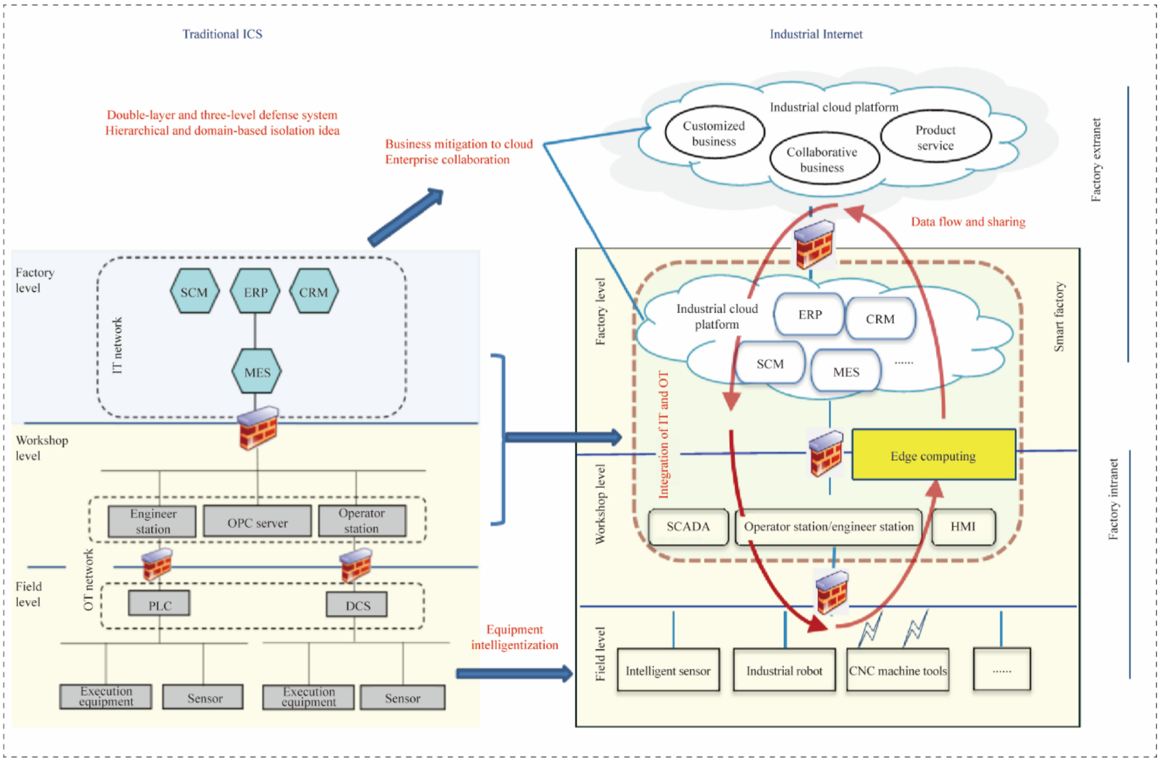


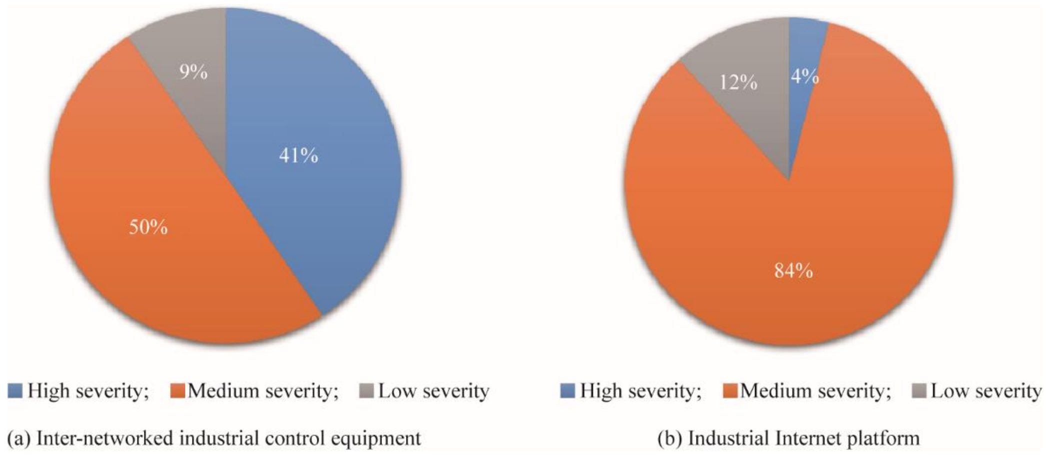
Fig. 1. Transformation from traditional ICS to industrial Internet.

Note: SCM stands for software configuration management; ERP stands for enterprise resource planning; CRM stands for customer relationship management; MES stands for manufacturing execution system, i.e., the execution management system in the production process of manufacturing enterprises; OPC stands for object linking and embedding (OLE) for process control; PLC stands for programmable logic controller; DCS stands for distributed control system; SCADA stands for supervisory control and data acquisition system; IT stands for information technology; HMI stands for human-machine interface; OT stands for operation technology.

2.2 The number and severity of vulnerabilities in inter-networked industrial equipment and platforms are high, and potential threats cannot be ignored

Due to inter-connectivity of networks, most of the originally closed ICSs have experienced various problems. For example, security is vulnerable, security vulnerabilities are difficult to patch, and security issues can hardly be solved in the short term. As of June 30, 2020, the National industrial Internet Security Situation Awareness and Risk Warning Platform had cumulatively monitored and discovered a total of 946 hidden vulnerabilities in inter-networked industrial control equipment, including 385 high-severity vulnerabilities and 472 medium-severity vulnerabilities. Medium- and high-severity vulnerabilities combined accounted for 90.6% of the total number of vulnerabilities [13]. In addition, severe vulnerabilities also exist in the direct connection between industrial Internet platforms and numerous critical equipment in the enterprise, and most of them are medium- to high-severity vulnerabilities. As of June 2020, a total of 3381 vulnerabilities had been discovered through scanning 136 key industrial Internet platforms, including 133 high-severity vulnerabilities and 2852 medium-severity vulnerabilities, together accounting for 88% of the total number of vulnerabilities [12] (Fig. 2).

There are many vulnerabilities in industrial equipment and industrial Internet platforms, and the severity of the vulnerabilities is high. To discover potential threats in a timely manner, vulnerability scanning and vulnerability mining technologies should be used. Furthermore, a security evaluation is required before industrial Internet platforms or related systems are officially put into use. However, the industrial Internet assets are now numerous and unclear, and security risks are unknowable; only after the development of an industrial Internet security situation awareness platform can the industrial Internet security risks be visible and knowable. Therefore, driven by the need for corporate security compliance and government regulation, there is an urgent need to vigorously develop industrial Internet security evaluation and monitoring technologies.



(a) Inter-networked industrial control equipment

(b) Industrial Internet platform

Fig. 2. Distribution of hazard severity of network vulnerabilities in industrial enterprises.

2.3 industrial Internet security architecture alteration and new technology applications continue to introduce new security risks

Measures such as the access of critical industrial equipment to the network and the cloudification of enterprise platforms have further accelerated the transmission and extension of security risks. The original network security borders have collapsed, and traditional security protection measures have failed. The range of network attacks has continued to expand from the border to the core. Identification and resolution systems are confronted with risks such as distributed denial of service (DDoS) attacks and domain name hijacking. Different identification systems such as Handle, object identifier (OID), Ecode, and GS1 systems have also introduced new security risks in the compatibility process. The popularization and application of new technologies such as the fifth generation of mobile communications (5G) and Internet Protocol Version 6 (IPv6) in the industrial Internet has also brought with them more network security challenges.

Advances in the information and communication technology (ICT), AI, and blockchain have introduced disruptive changes in the IT architecture, providing the underlying technical support for industrial Internet security technologies. For example, cryptography has developed from classical cryptography to modern cryptography and then to contemporary cryptography. In the future, the development of new technologies and new businesses such as big data and blockchain will pose great challenges to cryptography. Security technologies will face new application environments and demands when they develop up to a certain stage. At that time, breakthroughs in technological bottlenecks will be pursued so that security technologies can be further integrated with new technologies for development.

Security technologies vary depending on industrial Internet protection objects such as equipment, control, network, application, and data. Such technologies are mainly classified into four categories (Fig. 3): underlying technology, security protection technology, security evaluation technology, and security monitoring technology. (1) Underlying technologies include cryptographic algorithms, AI, and blockchain. By providing basic technical means, they offer technical support for industrial Internet security protection, evaluation, and monitoring. (2) Security protection technologies refer to the technologies and measures for border control, identity authentication, and access control and are deployed at all levels of the industrial Internet. Such technologies involve five major security protection objects, namely, equipment, control, network, application, and data in the four levels of the industrial Internet security system architecture. This category of technologies is the core of industrial Internet security technologies. (3) Security evaluation technologies are mainly used for vulnerability scanning, vulnerability mining, penetration testing, and go-online testing on industrial equipment and systems. (4) Security monitoring technologies mainly consist of technologies and measures for asset safety management, security monitoring and audit, and situation awareness for industrial Internet protection objects.

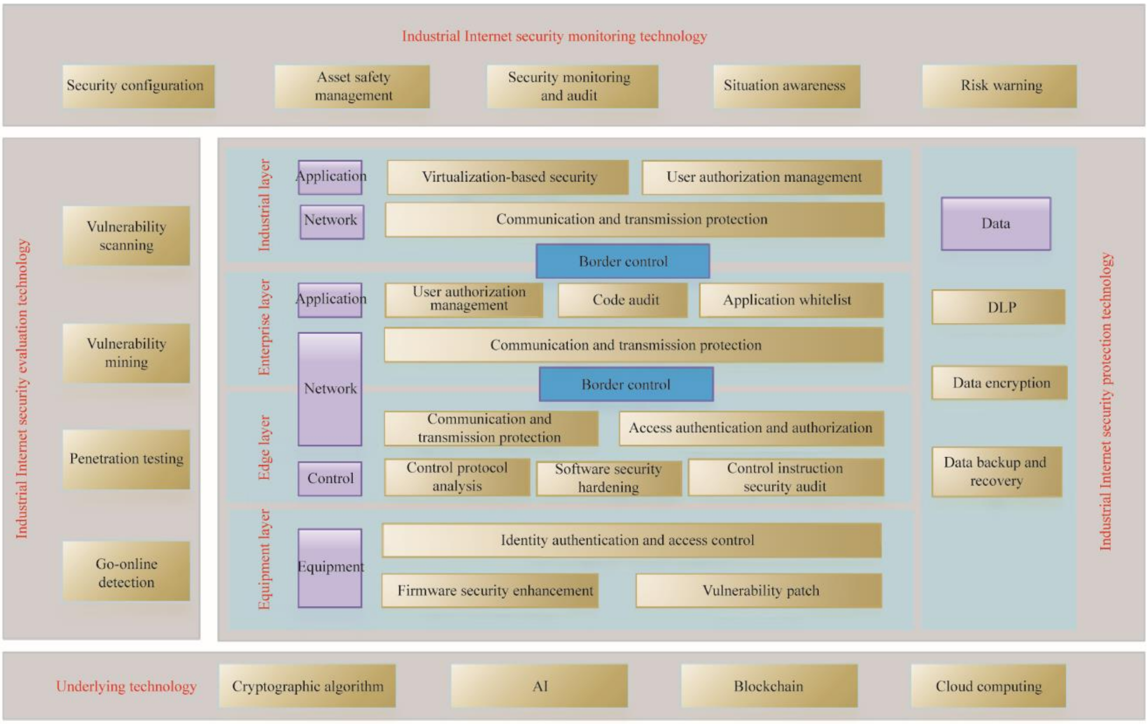

Industrial Internet security monitoring technology
Security configuration
Asset safety management
Security monitoring and audit
Situation awareness
Risk warning
Industrial Internet security evaluation technology
Vulnerability scanning
Vulnerability mining
Penetration testing
Go-online detection
Industrial layer
Application
Virtualization-based security
User authorization management
Network
Communication and transmission protection
Border control
Enterprise layer
Application
User authorization management
Code audit
Application whitelist
Network
Communication and transmission protection
Border control
Edge layer
Communication and transmission protection
Access authentication and authorization
Control
Control protocol analysis
Software security hardening
Control instruction security audit
Equipment layer
Equipment
Identity authentication and access control
Firmware security enhancement
Vulnerability patch
Data
DLP
Data encryption
Data backup and recovery
Industrial Internet security protection technology
Underlying technology
Cryptographic algorithm
AI
Blockchain
Cloud computing

Fig. 3. View of industrial Internet security technologies.

3 Development status of industrial Internet security technologies

3.1 industrial Internet security protection technologies

industrial Internet security protection technologies are basic technologies focusing on the long-standing confrontation between attack and defense. Key technologies mainly include white-listing, network border protection, and industrial mainframe security protection technologies [15].

3.1.1 Security mechanism

industrial Internet involves important links in industrial production and requires high system availability and real-time performance. However, the original industrial control network is relatively closed, and industrial control equipment lacks a flexible security strategy. As a result, the security and reliability of the equipment and operating software connected to the industrial Internet cannot be guaranteed. In traditional IT networks, the security mechanism generally adopts blacklisting technology, which can effectively prevent known rather than unknown attacks. In traditional ICSs, the industrial business process is relatively fixed and does not require frequent upgrades. White-listing technology is adopted in traditional ICSs to allow trusted and correct content to pass. If the trusted content changes, the security strategy is readjusted. In the industrial Internet, a security protection mechanism based on white-listing technology and supplemented by blacklisting technology can be adopted. This is because the industrial control process and business are relatively fixed, and security requires high availability and real-time performance. Therefore, white-listing technology is more suitable. Furthermore, blacklisting technology is introduced in the open network for supplementary protection.

3.1.2 Border protection

As traditional ICSs have reached the stage of industrial Internet where the networks are interconnected, OT and IT continue to integrate. The OT network is no longer closed and reliable but involves multiple network borders. In traditional IT networks, IT firewall technology is usually used for border protection. However, traditional IT firewall technology does not support any resolution of object linking and embedding for process control (OPC) protocol. To ensure normal connection of OPC clients to OPC servers, all ports should be configured to be accessible on the firewall, which exposes the production control network to attackers. The industrial firewall deployed at the borders of the industrial control networks can perform in-depth resolution of the OPC protocol, track the dynamic port established by the OPC connection, and monitor the transmission instructions in real time. Therefore, industrial Internet border protection requires the deployment of different firewalls based on the protection situations of different network borders. To meet the deployment requirements in the industrial environment and support the in-depth resolution of common industrial protocols, border protection products should have high reliability and low latency.

3.1.3 Industrial mainframe protection

Industrial mainframes are the breakthrough points of industrial Internet security incidents and the transmission carriers of many industrial viruses. Due to the demand for high stability of industrial configuration software, if the industrial mainframe does not update the system patches in time, it will not be able to obtain comprehensive security protection. On the Internet, traditional IT mainframes usually use anti-virus technology to upgrade the virus database through access to the Internet. As cloud-based anti-virus technology is being promoted, the efficiency of new virus scanning and removal continues to increase, but the virus database requires real-time update and upgrade. In the industrial Internet, industrial mainframes can adopt mainframe reinforcement technologies based on closing irrelevant ports, performing account authentication with least privileges, and setting mandatory access control to improve the operating system security of the mainframes. Therefore, the security protection level of industrial mainframes can be improved via the comprehensive use of protection technologies (i.e., based on mainframe reinforcement technology and using anti-virus technology as an important supplementary means).

3.2 industrial Internet security evaluation technologies

industrial Internet security evaluation technologies refer to the use of technical means to test and evaluate industrial Internet security protection objects to understand their security status. Such technologies mainly include vulnerability mining and penetration testing.

3.2.1 Vulnerability mining

With the increasing openness of ICSs, attacks and secret theft attempts via vulnerabilities, back-doors, etc. have become a significant threat to the security of the industrial Internet. Traditional IT system vulnerabilities mainly include malware, password attacks, and denial of service. However, ICS vulnerabilities differ from vulnerabilities in traditional IT systems. There are three reasons for this: (1) Most ICSs are imported from outside China, making it impossible to independently control the operation and maintenance of related systems. (2) ICS vulnerabilities have a wide range of sources, covering vulnerabilities in security computing environment concerning network security, vulnerabilities in control protocols, vulnerabilities in application systems, and vulnerabilities and back-doors in controllers such as PLC. (3) ICSs are relatively closed, and their system communication protocols are relatively private, making it difficult to study the communication protocols and security features in depth. Therefore, the vulnerability mining technology in the industrial Internet needs to analyze the network characteristics, production process control, and control protocols of the ICSs, and adopt the targeted fuzzy testing technique [16]. On the industrial Internet, the thinking of vulnerability mining in the convergent environment of IT and OT is recommended. It is necessary to adopt a combination of multiple vulnerability mining technologies that are deeply integrated.

3.2.2 Penetration testing

Penetration testing is a technique of testing and evaluating the network system security of the industrial Internet by simulating the attack means and methods commonly used by malicious attackers from outside the network. The penetration testing technology in the industrial Internet should first take into consideration the actual requirements of penetration testing in ICSs. Its implementation should comply with the guidance on the penetration testing and security testing processes such as the Penetration Testing Execution Standard (PTES), *Technical Guide to Information Security Testing and Assessment* (NIST SP800-115), *Open Source Security Testing Methodology Manual*, *Open Web Application Security Project (OWASP) Testing Guide*. After ICS penetration testing and analysis, key processes, steps, and technologies are extracted. industrial Internet security penetration testing is not a simple combination of multiple penetration testing security tools, but requires a sophisticated integration of multiple penetration tools.

3.3 industrial Internet security monitoring technologies

industrial Internet security monitoring technologies are used for discovery and identification, understanding and analysis, and response and handling of security threats. Key technologies mainly include security monitoring and audit and security situation awareness. As the industrial Internet has numerous equipment assets and software

DOI 10.15302/J-SSCAE-2021.02.009

systems, the management, operation, and maintenance workload of production personnel is complex and heavy. Related equipment and platforms suffer from various limitations such as a significant number of security vulnerabilities, difficulty in grasping security threats, and proneness to network attacks. The situation awareness technology for industrial Internet security adds asset characteristics of ICSs and industrial control equipment on the basis of cyberspace search engines. It uses software codes to simulate common ICS services or industrial control dedicated protocols such as Modbus protocol, PROFINET protocols, and Factory Interface Network Service protocol. The deep packet inspection technology is employed to resolve and restore network and application layer protocols (e.g., industrial control dedicated protocols and general protocols) layer by layer. Finally, security testing operations such as access log synthesis, industrial control equipment asset testing, industrial control vulnerabilities, and security incident identification are completed [17]. In the future, the industrial Internet security situation awareness technology is expected to strengthen the capability of identifying industrial Internet protocols and equipment on the basis of traditional online monitoring, honeypot simulation, and network traffic analysis technologies. Capabilities such as the monitoring and warning of industrial Internet security incidents, handling and source tracing, and security situation analysis are also expected to be developed.

4 Development trends of industrial Internet security technologies

4.1 industrial Internet security architecture developing from border security to zero-trust security

The security architecture of the network borders in traditional factories is secure inside the borders by default. Border devices such as firewall, anti-virus software, intrusion detection system, and DLP system act on the physical borders, and perform protection and surveillance based on the behavior on the borders. With the advancements made in industrial Internet technology in terms of bringing computing power closer to edges and migrating the business to cloud, the security borders of the industrial Internet have changed, requiring the reconstruction of the network security architecture (Fig. 4). In the future, the industrial Internet security architecture will focus on building a zero-trust security architecture integrating cloud, pipe, edge, and device. This architecture will be based on identity, including the key capabilities of business security access, continuous trust assessment, and dynamic access control.

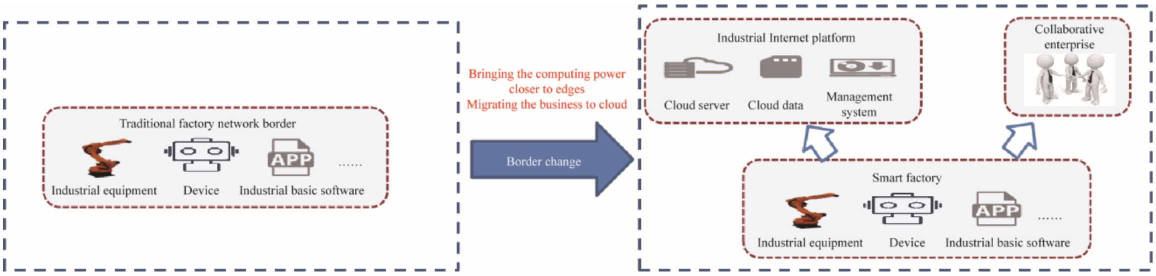

Traditional factory network border
Industrial equipment
Device
APP
Industrial basic software
......
Bringing the computing power closer to edges
Migrating the business to cloud
Border change
Industrial Internet platform
Cloud server
Cloud data
Management system
Collaborative enterprise
Smart factory
Industrial equipment
Device
APP
Industrial basic software
......

Fig. 4. Changes of the security borders of industrial Internet.

4.2 Concept of industrial Internet security protection changing from passive protection to active advanced protection

Although ICSs have set up relevant security equipment to improve system security, the number of network attack methods continues to increase. Passive defense has certain limitations. Active defense can avoid, reduce, or transfer risks before malicious intrusions exert influence on the information system in the industrial Internet, showing the characteristics of one-to-many defense. Multiple techniques such as active detection, traffic analysis, and passive trapping can support the security situation awareness and risk warning of the industrial Internet. The use of these techniques will finally aid in the transition from passive security protection to active defense.

4.3 industrial Internet security technologies developing from traditional analysis to intelligent awareness

In the early stages, the situation awareness technology mainly collects and analyzes massive security data, discovers valuable information in the data, and aggregates the valuable information into easy-to-understand reports and charts, thereby identifying vulnerabilities that may threaten system security [18]. Nowadays, the integration of security technology with big data and AI technology has enhanced the system's security detection and analysis capabilities. It has also promoted the development of security situation awareness, which is mainly manifested in APT interception, threat awareness, and threat intelligence sharing. industrial Internet security technologies are developing toward intelligent awareness. In particular, reasoning based on logic and knowledge is conducted to deduce unknown threats from known threats, thereby realizing prediction and judgment of security threat events. In the future, the levels of precise warning and accurate handling of security risks can be elevated with the aid of emerging technologies such as AI and big data analysis, thereby making network attacks and major network threats known, visual, and controllable.

5 Difficulties and challenges faced by industrial Internet security technologies

5.1 Difficulties faced by industrial Internet security technologies

Overall, China’s industrial Internet security technologies are currently on a track of continuous improvement and are being integrated based on traditional network security technologies. However, certain technological difficulties remain: (1) Industrial protocols are complex and diverse, making in-depth resolution quite difficult. Only through in-depth awareness of industrial Internet business traffic and in-depth resolution of the industrial protocols in the traffic can industrial security protection products provide security protection at the instruction level and range level for industrial protocols. (2) Industry barriers make it difficult to develop a security model with a wide coverage. There are many industrial sectors, and the businesses vary considerably even in the same sector. Therefore, specific industrial scenarios must be considered when developing industrial Internet security technology products. In other words, customized development is required when necessary. (3) The security technology reserve for new technologies such as 5G is insufficient, and as a result, various risks are still present; for example, 5G-related protocols and device vulnerabilities can be used to control industrial Internet devices and factories.

5.2 Challenges faced by industrial Internet security technologies

The in-depth application of the industrial Internet has increased the security risks of network attacks and virus spreading on industrial enterprise networking equipment. In addition, there are also objective issues, such as weak security awareness of some enterprises, generally low protection levels, and insufficient security industry support capabilities. All this translates to the fact that industrial Internet security technologies are faced with many challenges. (1) Industrial enterprises have insufficient security awareness and insufficient investment in industrial Internet security. They generally focus on the upgrading and transformation of traditional production systems and manufacturing models but ignore network security risks and hardly invest in security. They also rarely consider developing IT security together with OT security, which is not conducive to industrial Internet security protection. (2) The industrial Internet security industry constitutes a relatively low proportion of the core industrial Internet industries. Although its installed stock scale has increased from 1.34 billion CNY in 2017 to 2.72 billion CNY in 2019 (with a compound annual growth rate of 42.3%), it makes up only 0.5% of the core industrial Internet industries [19]. Additionally, there is a lack of enterprises leading in industrial Internet security, and the related products and services are relatively loosely coupled. Products and services are mostly related to border and terminal device security protection. (3) There is a great shortage of available security talent to support the development needs of the industrial Internet characterized by the deep integration of industry and informatization. Security talent should not only master network security, but also be familiar with the application scenarios of the factory environment.

6 Approaches for overcoming the difficulties in key industrial Internet security technologies

Key industrial Internet security technologies can be broadly divided into two categories: core security technologies for industrial control and core technologies for Internet security that are applied in the industrial sectors. These technologies include cryptography; security orchestration, automation, and response (SOAR) technology; and highly interactive simulation technology.

6.1 Application of cryptography

The adoption of cryptography, which is a cost-effective and widely used technique, started late in China. Although some industrial products in China are pre-integrated with foreign cryptography algorithms (e.g., cipher replacement technology), they face problems such as high replacement costs and long market adoption cycles. For this reason, information security companies in China have proposed an industrial Internet security solution based on Chinese proprietary cryptography. That is, SM9 cryptographic algorithms are used to achieve encrypted

DOI 10.15302/J-SSCAE-2021.02.009

transmission and storage of industrial device data and cloud server data. Corresponding cryptographic support systems for industrial information security are established to provide a safe and reliable network environment and an overall solution of data encryption services for the industrial Internet platform. The industrial Internet identification and resolution system has application requirements for identity authentication, sensitive data protection, and privacy protection. To this end, research should be conducted to tackle key problems in SM9/SM2-based technologies such as cryptographic modules, digital signatures, and privacy data desensitization. It is also necessary to build an industrial Internet identification and resolution system that integrates digital certificate-based cryptography, identify-based cryptography, and certificate-less cryptography.

6.2 Application of SOAR technology

SOAR is an intelligent collaboration system that integrates personnel, processes, and technologies. Its objective is to achieve security capability orchestration among products and components, so as to shorten the time of response to security incidents and improve the accuracy of security incident response. Targeted at heterogeneous enterprises and heterogeneous security equipment in the industrial sectors, SOAR technology is used to build a unified and standardized security interface system, break the island form of security equipment of various security enterprises, and establish a trusted security linkage system.

SOAR technology has been put in practical applications in the field of industrial security in countries other than China. For example, Siemens AG has realized the customization of security policies for different business scenarios, as well as the selection and deployment of security policies for different security requirements and businesses. The SOAR products of Israel Cyberbit have also been applied to the field of industrial control security. At present, although major enterprises in the manufacturing industry in China have deployed relevant security equipment, they do not have a unified and standard security interface. As a result, the security capabilities of equipment and products cannot be integrated to implement automated response and handling. Therefore, the manufacturing industry in China needs to urgently apply SOAR technology, as the coordination among various security capabilities will lay the foundation for an integrated response in the network security field.

6.3 Application of industrial highly interactive simulation technology

Industrial highly interactive simulation technology refers to the highly interactive virtual simulation of industrial Internet mainframes, control and edge devices, industrial protocols, industrial Internet platforms, and related businesses and applications. It provides a more realistic attack system, collects and analyzes attack data, and accurately grasps the attack behavior characteristics of industrial Internet, in turn supporting the decision-making for security protection work. Outside China, there have been mature products in the field of industrial Internet equipment and protocol simulation such as highly interactive industrial control honeypots (e.g., CryPLH and Xpot), which support the regulatory authorities in effectively grasping threat intelligence information. Related technologies in China are presently in R&D and product pilot stages, but there is no mature product.

industrial Internet equipment complies with a wide variety of protocols and has strong technical barriers. For example, equipment mostly uses wireless protocols for communication and fails to perform highly interactive simulation. The core of industrial highly interactive simulation technology is to support multiple industrial control protocols such as Modbus protocol, distributed network protocol version 3, and Siemens S7 protocol and the highly interactive simulation capabilities of industrial control equipment such as SCADA, DCS, and PLC. The technology can relatively comprehensively capture attackers’ access traffic and perform forensic analysis on attack behavior, thereby providing data support for the early warning and prediction of industrial Internet security incidents.

7 Countermeasures and suggestions

7.1 Developing customized services based on industrial characteristics and scenarios

industrial Internet security technologies should be tailored to the protection objects based on the industrial characteristics and scenarios and with reference to related approaches in traditional Internet security technologies. It is recommended that industrial protocol protection at the instruction level be implemented. The instruction-level protection should be deployed on an instruction-level industrial firewall at the border between the enterprise management network and the production control network. The OPC protocol should be resolved in depth and expanded to the instruction level to trace the dynamic port negotiated between the OPC server and the OPC client. The ports of the production control network need to be minimized to improve the network security of OPC-based

ICSs. It is also necessary to customize security technologies that are suitable for different industries and industrial scenarios. For example, the deployment of security technologies in the power industry follows the general principles of “security zoning, network dedication, horizontal isolation, and vertical authentication.” In the ICSs related to petroleum refining, security protection should be performed on network borders, regions, and mainframes to improve the anti-attack and anti-interference capabilities of the production network so as to protect the safe and stable operation of the production system.

7.2 Continuously integrating new technologies to achieve active defense

The development of technologies such as blockchain, AI, big data, and trusted computing has empowered industrial Internet security. These technologies have potential advantages in various aspects, such as discovering advanced threats, detecting malicious files, identifying malicious families, monitoring encrypted attacks, actively discovering threats, assisting in rapid investigations, and ensuring the security of the industrial Internet. industrial Internet security technologies should be closely integrated with these new technologies to customize suitable security strategies. Rapid development of industrial Internet security situation awareness based on big data is suggested, which can be achieved through massive industrial data retrieval, log collection, traffic analysis, automatic positioning, and visual tracing. Technologies such as AI should be used to intelligently and automatically detect advanced threats and potential security issues, which can ensure the security of the industrial Internet.

7.3 Building endogenous security capabilities to support industrial Internet security development

The traditional local and external security protection capabilities can no longer meet the security requirements. Therefore, it is urgent to improve the endogenous security capabilities of the industrial Internet to achieve the integration of network security capabilities and the industrial information environment. It is recommended that the simultaneous construction of security capabilities should be considered in the process of industrial Internet system planning, development, and operation and maintenance. Furthermore, network security enterprises should cooperate with system equipment providers and leading industrial enterprises to jointly develop equipment and products embedded with security functions for better convergence of industrial production systems and security systems. Enterprises should take into consideration their business characteristics and security requirements while developing security capabilities. In this manner, enterprises can achieve the self-adaptation and self-growth of industrial Internet security, and therefore, witness dynamic improvements in their industrial Internet security capabilities.

References

[1] Xu K, Qin R, Wang Y, et al. Industrial game-changing strategy in the Internet+ area： Win the war of industrial Internet [M]. Beijing: Posts & Telecom Press Co., Ltd., 2015. Chinese.

[2] Zhang N, Liu L R, Tian Z H, et al. Progress and trend of industrial Internet security [J]. Journal of Guangzhou University (Natural Science Edition), 2019, 18(3): 68–76. Chinese.

[3] Du L, Chen S Y, Jiang Y Z, et al. Research on the protection of national basic data [J]. Information and Communications Technology and Policy, 2018 (10): 10–13. Chinese.

[4] Li T. The consideration on security posture analysis and security defense suggestion in the industrial Internet of Things [J]. Network Security Technology & Application, 2020 (4): 126–128. Chinese.

[5] Li Q, Tian H R, Du L, et al. The strategic research on industrial Internet of Things [J]. World Telecommunications, 2016 (4): 16–19. Chinese.

[6] Liu X M, Du L, Yang D M. The analysis on security posture of industrial Internet of Things in 2019 [J]. Secrecy Science and Technology, 2019 (12): 27–31. Chinese.

[7] Guo X, Liu J J, Yu Z K, et al. The security expectation on industrial Internet of Things in 2019 [J]. China Information Security, 2019 (6): 51–52. Chinese.

[8] Wan M, Zhang S Y, Li J W, et al. Analysis on security in industry Internet of Things [J]. Automation Panorama, 2021, 38(1): 62–66. Chinese.

[9] Sun X D, Qin H L, Liang Z J, et al. New technology of intelligent industrial firewall [J]. Automation Panorama, 2018, 35(5): 80–83. Chinese.

[10] Zhao Z X, Shi Y J, Yu H C, et al. Research on vulnerability discovering in IIOT system [J]. Control and Instruments in Chemical Industry, 2020, 47(2): 160–164. Chinese.

[11] Chen K H. The research on security permeation test in industrial Internet of Things [J]. Network Security Technology &

DOI 10.15302/J-SSCAE-2021.02.009

Application, 2020 (4): 124–126. Chinese.

[12] Xie X D. Research on industrial Internet security monitoring audit and situation awareness technology [J]. Journal of Information Security Research, 2020, 6(11): 996–1002. Chinese.

[13] China Academy of Information and Communications Technology, Alliance of industrial Internet. Report on industrial Internet security situation for the first half of 2020 [R]. Beijing: China Academy of Information and Communications Technology, Alliance of industrial Internet, 2020. Chinese.

[14] Liu X M, Quan X R, Li S. The development on security of overseas industrial Internet of Things [J]. Secrecy Science and Technology, 2020 (5): 20–26. Chinese.

[15] Kang S Y, Hu W L. Research on industrial Internet security technology and analysis on the development of industrial Internet security industry in China [J]. Secrecy Science and Technology, 2020 (5): 27–31. Chinese.

[16] Sun Y A, Hu R H. Research on vulnerability scanning and discovering technology of industrial control system [J]. Cyberspace Security, 2017, 8(1): 75–77. Chinese.

[17] Nanjing Sinovatio Technology Co., Ltd. The solution on security detection and situation awareness in industrial Internet of Things [J]. Automation Panorama, 2020, 37(2): 28–31. Chinese.

[18] Tao Y, Huang T, Zhang M H, et al. Research and development trend analysis of key technologies for cyberspace security situation awareness [J]. Netinfo Security, 2018 (8): 79–85. Chinese.

[19] China Academy of Information and Communications Technology. Report on industrial Internet industry economic development (2020) [R]. Beijing: China Academy of Information and Communications Technology, 2020. Chinese.