DOI 10.15302/J-SSCAE-2021.02.010

Paths for Improving Public Service Capability Regarding Industrial Internet Security

Zhou Hao, Li Jun, Wang Chonghua, Yin Libo, Zhao Qian

China Industrial Control Systems Cyber Emergency Response Team, Beijing 100040, China

Abstract: The industrial Internet security public service ensures the healthy development of the industrial Internet, as it is important for the output of the industrial Internet security capability. In this article, we elaborate on the importance of the industrial Internet security public service while analyzing its development status, as well as the challenges faced during its development. The path to improving the basic capabilities of the industrial Internet security public service is proposed based on the basic resource database construction, information sharing and exchange, situation awareness capability, and an emergency response mechanism. Subsequently, the path to promoting the innovative development of its security is proposed in terms of the compatibility and adaptation of information technology application innovation, combination and arrangement of security service capabilities, as well as a standards and evaluation mechanism. Finally, the development of the industrial Internet security public service is prospected from the intelligent security service, integrated public service platform, and new generation information technology.

Keywords: industrial Internet security; security-related public service; cybersecurity; industrial information security; innovative development

1 Introduction

The highly open and interconnected characteristics of the industrial Internet have broken the relatively closed pattern of the original industrial control system. This has exposed objects at all levels of the industrial Internet to the Internet, interweaving the security risks of information technology (IT) and operation technology (OT) and the security situation is quite grim [1]. As an important part of national security, industrial Internet security should be planned, designed, and promoted simultaneously with the industrial Internet. At present, the construction of industrial Internet security is in its infancy. The promotion of security service capacity-related work is lagging, resulting in problems such as an imperfect service mode system and a weak level of security technology capability. Thus, it is urgent to improve the overall security service capacity.

To guide and standardize the development of the industrial Internet, China has successively issued a number of policy documents, as follows: *Guidance on Deepening the Development of "Internet + Advanced Manufacturing" for the Industrial Internet*; *Guidance on Strengthening the Security of the Industrial Internet*; and *Action Plan for Innovation of the Industrial Internet (2021–2023)* to accelerate the construction of its security system. In 2018, China released the first national standard for security information sharing *Information Security Technology—Cyber Security Threat Information Format* (GB/T 36643—2018), which enables organizations to share and utilize security information through a unified and standardized description of network security threat information [2]. Relevant

Received date: January 13, 2021; **Revised date:** February 24, 2021

Corresponding author: Wang Chonghua, senior engineer of China Industrial Control Systems Cyber Emergency Response Team. Major research fields include industrial Internet security, network and system security, network attack and defense. E-mail: chonghuaw@live.com.

Funding program: CAE Advisory Project "Research on Development Strategy for Next-Generation Industrial Internet Security Technology" (2020-XZ-02)

Chinese version: Strategic Study of CAE 2021, 23(2): 074–080

Cited item: Zhou Hao et al. Paths for Improving Public Service Capability Regarding Industrial Internet Security. *Strategic Study of CAE*, https://doi.org/10.15302/J-SSCAE-2021.02.010

academic research summarizes the development trend and key technologies of industrial Internet security and provides basic security strategies and specific defense measures [3]. The research and discussion on key technologies of security intelligence collection, extraction, and reasoning are strengthened [4]. In terms of visibility, knowability, manageability, controllability, traceability, and early warning, this paper proposes a path toward network security situation awareness [5]. Further, in cases of network security emergencies, the paper provides countermeasures from the aspects of security monitoring, overall guarantee, talent team construction, etc. [6].

To explore the development of industrial Internet security services, this paper aims to do the following: summarize the development status of industrial Internet public services; explain the challenges faced by this stage of development; propose a path to improve the industrial Internet security public services ability from the dimensions of basic ability and innovative development; and explore the development of industrial Internet security public services in the future. This is with the aim of providing a reference for the development of a new generation of industrial Internet security technology.

2 Importance of the industrial Internet security public service

2.1 Definition of public service for industrial Internet security

This paper defines the public service of industrial Internet security as: the general name of resources and technical services related to the security capability of the industrial Internet provided by the state, local, third-party organizations, or operating enterprises for social industrial Internet users; and, giving full play to the network security capability through state guidance. The industrial Internet security public service performs the whole process of the preparation stage of industrial Internet security, including pre-, in, and after the process. This covers the following: equipment access and security control on the edge side; security protection of the upper industrial software operation; and vulnerability scanning, flow monitoring, threat report, data forensics, leak tracing, privacy protection, and other complex data side security services on the application side. Typical public services of industrial Internet network security include a basic resource base service, an information sharing service, a situation awareness service, an emergency response service, a security crowd test service, and an attack and defense drill service, along with others.

To build the industrial Internet security system, China has taken various measures to comprehensively improve the public service capability of Industrial Internet security from the aspects of policy guidance and fund support. Since 2018, the Ministry of Industry and Information Technology has selected a number of industrial Internet security and public service platforms through industrial Internet innovation and development projects and network security pilot demonstration projects. Based on new-generation information technologies such as big data, cloud computing, artificial intelligence (AI), block chain, and so on, these platforms provide real-time monitoring and emergency responses for all kinds of social units or organizations including extortion viruses, Trojan worms, security vulnerability, malicious attacks, and other security threats through remote or online services. At the same time, a combination of online and offline methods are used to carry out network security services such as threat information sharing, data security protection, malicious code detection, and so on [7].

2.2 Public service is an important measure to ensure the security of the industrial Internet

The network public service has played a positive role in promoting the development of other industries. For example, during the Coronavirus disease 2019 pandemic, pandemic prevention and control materials were in short supply. The public service platform of pandemic data, the State Council material scheduling platform, and other public service platforms established links between different fields, industries, and enterprises that supported the resumption of production under normal pandemic prevention and control. Security companies have been comprehensively studying in different fields, constantly filling in the shortcomings of the industrial Internet security public service. They have developed a number of platforms such as the industrial Internet security public service platform of Qianxin Technology Group Co., Ltd., the Telecom DamDDoS of China Telecom Group Co., Ltd., and the Data Security Threat Intelligence Platform of Chengdu Thinking Century Technology Co., Ltd.

The security public service has far-reaching significance in promoting the development level of industrial Internet security. On one hand, the public security service is an important part of the industrial Internet security system. Public utilities are of an outstanding nature, and the spillover and pulling effect are clear. It is difficult to achieve significant improvement by relying only on commercial mechanisms. Therefore, it is necessary to effectively integrate all kinds of security resources in the market and optimize use efficiency of the resources through the guidance of industrial policies, standards formulation and implementation, and project fund support. To improve

DOI 10.15302/J-SSCAE-2021.02.010

resource sharing, a good interaction mode between the security industry and the industrial Internet industry must be formed, which will provide better services. On the other hand, industrial Internet security public services can help the security ecology form a good interaction mechanism and market model. The public service of industrial Internet security can provide more accurate and efficient security services for industrial Internet users, help industrial Internet enterprises establish effective security protection, reduce the security investment of small- and medium-sized enterprises and their risk of attack, improve the overall security capability of the industrial Internet, and comprehensively improve the security level of the industrial Internet in China.

In conclusion, concerning the importance of public service for industrial Internet security, comprehensive and systematic technological innovation should be carried out with requirements for cross-domain resource sharing, full chain technology iteration, customized on-demand service, and flexible dynamic reconstruction. The sharing capacity of information resources such as security loopholes, threat information, general security tools, standards and specifications, and solution practice should be integrated, to form whole process service capabilities such as online monitoring, malicious code detection, and active reinforcement and protection. Further, public security services should be provided to industrial Internet users; the technical bottleneck of cross-domain sharing of network security resources should be opened; and an intelligent and open public service system for industrial Internet security should be established to improve the level of industrial information security in China. We will ensure the stable operation of the industrial system, as well as the normal production and life of the people, and effectively safeguard the safe and reliable operation of the industrial Internet in China.

3 Challenges of the industrial Internet security public service

3.1 Challenges of the industrial Internet security infrastructure resource library

The industrial Internet security infrastructure resource library mainly includes industrial asset type knowledge, industrial/network protocol fingerprints, vulnerabilities, malicious code samples, network security threat intelligence, security assessment and inspection tools, and other security infrastructure resources. It provides the public with security tools and sharing of various resource libraries. At the same time, it provides resource sharing and protection capability invoking for industrial Internet enterprises. Since 2012, the United States has begun to build a security infrastructure resource sharing system covering rail transit, energy and power, production and manufacturing, and other key areas, and has formed a security infrastructure resource sharing capability. At present, China has built national vulnerability databases such as the China National Vulnerability Database (CNVD) and the China National Vulnerability Database of Information Security (CNNVD), and enterprise vulnerability databases including the Butian vulnerability database and Lvmeng security vulnerability database. In addition, in 2019, the construction of the China Industrial Control System Vulnerability Database (CICSVD) was launched to collect relevant vulnerabilities and patches covering key industrial fields such as automobiles, aviation, aerospace, and petrochemicals. In terms of threat intelligence, in 2017, the Institute of Information Engineering of the Chinese Academy of Sciences led the construction of the China National Cyber Threat Intelligence Collaboration (CNTIC) to strengthen the integration and utilization of threat intelligence through the cooperation of enterprises and the government. At the same time, the Qianxin Technology Group Co., Ltd., the Beijing ThreatBook Online Technology Co., Ltd., and other enterprises have built a threat intelligence database to provide support for network attack tracing, security incident emergency disposal, and other businesses. Even though the construction of the industrial Internet security infrastructure is gradually developing, there are still some shortcomings.

There is no unified standards in the identification, description, classification, and hazard level of the existing basic resource database. Further, the description of the same field in each resource database is not unified, which is not conducive to data synchronization or sharing between different vulnerability databases. For example, the CNVD divides vulnerability causes into 10 types, such as input verification error and access verification error, while the CICSVD divides vulnerability causes into 10 different types, such as code injection, command injection, and cross site scripts.

The construction of a basic resource pool is insufficient, while the degree of external dependence is high. Currently, China has only built a large-scale resource base in a vulnerability database and a threat intelligence database, and has formed a national resource base based on the CNVD, CNNVD, CICSVD, CNTIC, etc., which is highly dependent on common vulnerability disclosure (CVE). The main vulnerability information comes from foreign vulnerability databases such as the National Vulnerability Database and the Industrial Control Systems Cyber Emergency Response Team of the United States. Affected by the domestic vulnerability mining ability,

understanding of the principle and mechanism of software and hardware, and the incentive mechanism for vulnerability reporting, the number of vulnerabilities submitted independently is small, and thus there is a certain security risk in the supply chain of the vulnerability repository. At the same time, there is a wide variety of industrial Internet security infrastructure resources that are difficult to gather. Other security infrastructure resources, such as asset directory, protocol rule, malicious code virus, and security tool libraries have not yet formed a national resource platform.

3.2 Challenges of industrial Internet security information sharing

The capability of multi-source, heterogeneous security information extraction is insufficient. Security information is characteristically multi-source, heterogeneous, redundant, and complex, and includes various types of semi-structured and unstructured data. Information sources may be network traffic, internal and external threat intelligence centers, professional institutions, industry alliances, and even the underground black market. At present, there are some semi-automatic collection frameworks for security information extraction, which are mostly conducted through manual analysis, submission, and collection. Its efficiency is unfortunately low. Because of the ability level of security analysts, it is difficult to extract high-value security information accurately, efficiently, and without omission from a massive amount of security data, and the ability to automatically extract and generate security information lacks.

There is a lack of relevance among various resource databases. Although there are security information description and sharing standards such as the Structured Threat Information eXpression (STIX), the Trusted Automated eXchangeof Indicator Information (TAXII), and the Cyber Observable eXpression (CybOX) in all kinds of resource databases, the development of vulnerability databases, threat intelligence databases, and malicious code virus databases is still relatively independent at this stage. This leads to vulnerability, threat intelligence, malicious codes, and other security information being distributed discretely, as well as a lack of association fusion analysis with protocols, assets, and dependent software and solutions, all of which fail to form an effective association knowledge map. In addition, even for the same resource pool, the degree of association and sharing between different operating agencies is low. For example, there are more than 10 types of security vulnerability libraries built by security enterprises, but there is no design interface or associated attribute information between them. Moreover, there is no unified third-party sharing platform to integrate and gather vulnerability information. This makes the comprehensive utilization rate of security information low and the phenomenon of an “information island” serious.

There is also a lack of credibility and privacy protection for security information. Trusted verification and effective privacy protection of this information is the premise for establishing a trusting relationship between information sharing parties, as well as the foundation for promoting the healthy development of security information sharing. On one hand, due to the different sources and degrees of reliability of security information, there are conflicts, false or misleading security information, and incorrect content of security information in different resource databases, reducing credibility and making it difficult to give full play to the overall value of security information resource sharing. On the other hand, in the process of security information sharing, we should pay attention to privacy protection, anonymity, and desensitization of the shared security information. Although there are some privacy protection technologies such as digital watermarking and differential privacy protection, some enterprises lack security awareness or privacy protection. The distrust of the sharing party creates a psychological conflict within the enterprises regarding the open sharing of security information.

3.3 Challenges of industrial Internet security situation awareness

In recent years, the construction of industrial Internet security situation awareness has made some progress. Based on traditional Internet solutions, a national industrial Internet security situation awareness and risk early-warning platform has been established. Relying on the unique three-level national, provincial, and enterprise architecture, the national network security situation awareness platform has been built, and a closed-loop processing mechanism covering security threat monitoring, notification, disposal, and other links has been constructed. However, there are still some technical bottlenecks in the industrial Internet security public service based on the situation awareness of the national platform.

It is difficult to obtain data of industrial Internet security situation awareness. There are many kinds of devices and interaction protocols in the industrial Internet operating environment. There are more than 100 common industrial protocols, along with a large number of unrecognized industrial devices and private protocols, which makes it difficult to obtain sensing data such as traffic, logs, and system states. In addition, the data quality of the

DOI 10.15302/J-SSCAE-2021.02.010

network security situation awareness platform is uneven, much null information still exists, and the data validity is weak. The data types and formats of industrial equipment and protocols are quite different, making them difficult to deal with. While it is necessary to develop different data types and formats, the cost of doing so can be quite high.

Furthermore, it is difficult to process and analyze the data of industrial Internet security situation awareness. Compared with traditional network security situation awareness, the industrial Internet security situation awareness is more difficult in data analysis and decision processing. It needs to consider the characteristics of multi-type industrial protocol analysis and multi-semantic data normalization. To effectively analyze security attack events or potential security risks from existing security data, it is necessary to use a malicious behavior code base along with a multi-semantic data normalization threat information base, as well as other types of high-precision professional knowledge bases. Currently, due to the lack of a security knowledge base and understanding of the characteristics of industrial Internet security attacks, an efficient security analysis capability has not yet been formed.

3.4 Challenges of industrial Internet security emergency response

As a systematic work combining technology and management, the industrial Internet security emergency response includes three parts: the construction of an industrial Internet security emergency response process; the disposal of security incidents; and the optimization and reconstruction of a security response system. This forms a closed loop for the industrial Internet security emergency response [7]. On a technical level, the industrial Internet security emergency response is meant to detect and deal with incidents through automatic or semi-automatic ways to ensure that availability can be restored shortly after incidents, as well as prevent future incidents as much as possible. At present, there are still some challenges in the response and management mechanisms of the industrial Internet security emergency response.

The industrial Internet security emergency response system or platform has not yet formed a standardized and automated response plan. The process of creating the industrial Internet security emergency response involves resources or platforms such as commands, scheduling, decision-making, and a security resource library when guiding or implementing emergency response behavior. Non-standardized and non-automated emergency plans are usually inefficient and limited by the technical ability level and response judgment time of emergency decision-makers. It also affects the speed and efficiency of the industrial Internet security emergency response, thus prolonging response time of security incidents.

In China, all kinds of subjects of industrial Internet security emergency response management do not cooperate closely. In the event of security incidents, due to the influence of network division, geographical ownership, management responsibilities and other factors, the cooperation of various subjects of an emergency response is scattered, making it difficult to form an emergency linkage mechanism.

4 Industrial Internet security public service basic ability promotion path

4.1 Improve the construction of the industrial Internet security base

The perfect industrial Internet security base should have good expansibility and compatibility, as well as rich, comprehensive, and valuable security data and tools. Therefore, the path to upgrading the industrial Internet security base should be carried out from the following aspects.

By means of government or third-party authorization, we will establish and improve industrial Internet assets and network protocol fingerprints, vulnerabilities, malicious code samples, network security threat intelligence, security assessment and inspection tools, and other basic resources. While continuing to strengthen the construction of the existing basic security resources, we will make up for the missing basic security resources. We will continue to expand industrial Internet Security forensics, risk assessment, emergency response, and other tool sets for typical industries, and implement incentive mechanisms in aspects of submission, reporting, and sharing so as to continuously increase the reserves of basic industrial Internet security resources and enhance their richness.

We also aim to strengthen the depth and breadth of cooperation between industrial Internet enterprises, security enterprises, industrial software enterprises, security research institutions, and all kinds of resource database construction and operators, and form a good situation of close cooperation. Each has its own advantages and complements each other, and can improve the process management of the industrial Internet security basic resource database in aspects of collection, verification, release, and repair. Major security incidents then can be warned about and repaired in a timely manner.

Scientific research institutions and security enterprises are encouraged to strengthen key technologies such as

industrial Internet security vulnerability mining, malicious code analysis, and software reverse engineering, along with improving the depth and breadth of research on industrial Internet security software, hardware, firmware and other basic elements. They are also encouraged to support public testing of industrial Internet security, and help motivate security enterprises or individuals to actively submit zero-day vulnerabilities.

4.2 Enhance the sharing and exchange of industrial Internet security information

Information sharing is an effective means to connect and enable the industrial Internet security infrastructure, and it is a natural demand following its construction.

The participants, sharing scope, format specification, interface standard, privacy protection, and other contents of industrial Internet security information sharing should be constantly updated and improved. The resources and technical advantages of governments, scientific research institutes, universities, and enterprises should be integrated in industrial Internet vulnerability mining, threat intelligence, evaluation tool development, and protocol analysis. An industrial Internet security information sharing mechanism that is relatively complete in content, clear in system, long-term, and continuous should be gradually established.

Under the unified leadership and coordination of industry authorities and relying on the of national, provincial, industry, and enterprise levels, the industrial Internet security information sharing platform should be constructed at different levels to gather security information in different fields, industries, and regions, and to protect the privacy and credibility of shared information based on block chain, privacy computing, and secure multi-party computing. Relevant standards and specifications of security information sharing data, formats, and protocols should be researched and formulated, and the interconnection, interoperability, and sharing of security information should be realized through standardized methods.

4.3 Focus on improving the ability of industrial Internet security situation acquisition, understanding, and prediction

Currently, situation awareness is mainly used to provide data analysis results and network security risk warnings for security personnel, and to assist managers in making strategic security decisions. However, situation acquisition, understanding, and prediction need to be improved. It is urgent to improve the aggregation and analysis of multi-source heterogeneous data, as well as the situation prediction model, and comprehensively measure situation awareness application scenarios.

The ability to obtain the security situation of the industrial Internet should be enhanced. Based on a variety of data sources, it obtains and perceives all kinds of security information in the industrial Internet environment, breaks through the fusion and aggregation technology of massive multi-source heterogeneous data, and mines the potential association between data through attribute fusion, correlation analysis, graph clustering, etc., so as to provide data support for the next gait analysis.

Understanding the industrial Internet security situation should also be improved. Driven by security data, this paper further integrates and analyzes network traffic data, system log data, threat intelligence and other security data, mines the security knowledge hidden in the data, establishes comprehensive models of security data awareness, algorithms, reasoning, and detection, and constructs the associated knowledge map and security situation knowledge base. The machine data is then transformed into readable and understandable security situation data.

Further, industrial Internet security situation prediction should be improved. Based on the security data, this paper makes a comprehensive analysis of the industrial Internet security environment information, and carries out the tracking and tracing work of security events in combination with the basic security resource database, security knowledge database, and big data analysis. Further, it reconstructs the attack path of security events, so as to provide a basis for forensics and countermeasures.

4.4 Improve the security emergency response system of industrial Internet

As the last barrier to overcome to ensure the safe and reliable operation of the industrial Internet, an emergency response operates as an important embodiment of the basic ability of the network security public service, as well as a strong support in ensuring the safety of the industrial Internet.

We will improve the industrial Internet security emergency response mechanism and build a professional, automated, and comprehensive security emergency response plan system. Based on the perfect industrial Internet emergency response mechanism, we will realize the networking and intelligence of all kinds of resource allocation and improve emergency response coordination.

DOI 10.15302/J-SSCAE-2021.02.010

We will also promote construction of the industrial Internet security emergency response technology; integrate the existing security emergency response resources including data, platform and system; form a cross-industry, cross-department, cross-level, and cross-regional security emergency response capability; and improve the collection and analysis capability of the industrial information security vulnerability database at the same time.

Further, we will promote the establishment of a normalized security emergency drill mechanism, enhance the emergency response capability of industrial Internet enterprises in a practical way, and enrich the emergency response experience of industrial Internet security practitioners. We will also develop an emergency response capability evaluation model and tool set, test and improve in the process of actual combat, and comprehensively evaluate the effectiveness and adequacy of the emergency response.

5 Innovative development and promotion path of industrial Internet security public service

5.1 Based on the application of information technology innovation, cross-compatibility adaptation is carried out to synchronously improve the innovation level of the supply chain

On one hand, based on Feiteng, Kuntai, Kunpeng and other IT innovation and application products, the cross-compatibility and adaptation of the industrial Internet security public service system and platform are carried out, covering key chips, operating systems, databases, core software, etc., forming the ability of combined operation, adaptation, and optimization. On the other hand, we should improve the environment for innovating and developing industrial Internet security technology, focus on solving the “lifeline” problems of industrial Internet supply chain, such as key industrial Internet security products and core technology research, focus on national strength and resources, and increase R&D investment in core electronic devices, high-end general chips, and basic software products. It will bring changes in the underlying technology for the basic software and hardware of industrial Internet security public service and supply chains, and effectively improve innovation and development of the industrial Internet security public service.

5.2 Combine and arrange safety service capability to form innovative and developed safety service and on-demand capability

The development of industrial Internet Security innovation needs to gradually gain the ability to independently develop key chips, operating systems, databases, and software and network equipment, and fundamentally move away from depending on imported technology. The industrial Internet security public service needs to abandon the status quo of moat-type security products such as encryptions, firewalls, intrusion detection, and identity authentication, innovate and explore active and intelligent security service technologies, reorganize and arrange the existing security service capabilities, and focus on breaking through key security technologies such as behavior analysis, service arrangement, and automatic response. We will continue to improve the industrial Internet security service mechanism and form an innovative and developed security service with an on-demand capability.

5.3 Explore the public service standards and evaluation mechanism to form a sustainable industrial chain

Starting from the demand side of industrial Internet security, this paper puts forward a standards system and an evaluation system of the industrial Internet public service capability. The standard system is the basis for the establishing of the evaluation system. Without establishing the standards system and related standards, promoting the evaluation system will encounter bottlenecks. Therefore, on one hand, under the guidance of national authorities, we should establish an industrial Internet security public service standards system with a wide range of capabilities, strong service capabilities, and standardized processes. We should also establish a positive, interactive closed loop between standards and evaluation. On the other hand, we should explore the establishment of an industrial Internet security public service effect evaluation mechanism, start from system construction, implement key practical standards and evaluation work, and avoid disorderly development.

6 Conclusion

With the high integration and rapid development of the industrial Internet and new-generation IT, the future industrial Internet security public service can develop in the direction of intelligence, integration, and specialization.

Security services based on AI will develop rapidly. With the explosive growth of industrial Internet data, the optimization of deep learning algorithms, and the substantial improvement of computing power, industrial Internet

security technology will present a more efficient, accurate, and intelligent development trend. Based on AI's strong ability of self-learning and self-evolution, a comprehensive and intelligent security identification, detection, response, and recovery capability can be constructed and supplemented by a basic security resource library for security situation analysis. This can help promote the development of a security defense system in the direction of comprehensive awareness and intelligent collaboration, and effectively resist evolving high-level threats.

The integration of security technology gives birth to a public service platform with tightly coupled functions. In the future, the industrial Internet security public service platform will further integrate security information and event management, user behavior analysis, and other security analysis functions as a tightly coupled and scalable security operation and analysis platform. The service form of the industrial Internet security service platform will also develop from providing single security function service to integrated service with multiple functions. A threat intelligence database, security vulnerability database, and a malicious code virus database will be closely related or integrated to form a unified security infrastructure resource database. Security services such as security diagnosis and evaluation, security consultation, data protection, code checking, system reinforcement, and cloud protection will be provided by a micro service or other means in the form of an industrial Internet security public service platform.

The new-generation IT further enables the public service of industrial Internet security, continuously improves integration, innovation, and its professional level. With the rapid and steady development of the industrial Internet, advanced technologies such as the fifth-generation mobile communication, cloud computing, big data, block chain, and trusted computing will be gradually implemented in industrial Internet security, promoting the formation of a professional service platform, a comprehensive service platform, and a common technology platform for the industrial Internet security public service. At the same time, it will also promote and guide the exploratory application of industrial Internet enterprises and users in risk identification, threat detection, security reinforcement, operation management, and other processes, and give birth to professional consulting services and solution providers for industrial Internet security public services.

References

[1] Wang C H, Zhou H. Research on industrial Internet security technology. [EB/OL]. (2020-03-02) [2020-12-25]. https://mp.weixin. qq.com/s/5tvsJ_wdlJtnCf57tf8DQQ. Chinese.

[2] State Administration for Market Regulation, Standardization Administration of the People's Republic of China. Information security technology—Cyber security threat information format: GB/T 36643—2018 [S]. 2018. Chinese.

[3] Xing L W. He Jifeng: Development trend and key technologies of industrial Internet security [J]. Information Construction, 2016 (11): 38–40. Chinese.

[4] Dong C, Jiang B, Lu Z G, et al. Knowledge graph for cyberspace security intelligence: A survey [J]. Journal of Information Security, 2020, 5(5): 56–76. Chinese.

[5] 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.

[6] Yu Q, Yang L F, Gao G J, et al. Emergency and response for cyberspace security [J]. Strategic Study of CAE, 2016, 18(6): 79–82. Chinese.

[7] China Industrial Control Systems Cyber Emergency Response Team, National Industrial Security Industry Alliance. White paper on industrial Internet platform security (2020) [R]. Beijing: China Industrial Control Systems Cyber Emergency Response Team, National Industrial Security Industry Alliance, 2020. Chinese.