DOI 10.15302/J-SSCAE-2021.02.011

Network Security Management and Protection of Industrial Internet Equipment

Ma Juan[1], Yu Guangchen[1], Ke Haoren[1], Yang Dongmei[1], Wushour Silamu[2]

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

Abstract: The new generation of information and communications technology is highly integrated with industrial systems. The industrial Internet promotes ubiquitous and deep interconnections and the comprehensive perception of human, machines, and things. Industrial Internet equipment has become increasingly networked, digital, and intelligent; therefore, the network security design,application management, and protection of these equipment have also become increasingly important. In this study, we clarify the connotation, protection scope, and requirements of industrial Internet equipment and summarize the development status of industrial Internet in China and abroad from the aspects of security control and security certification. Moreover, problems regarding the network security of industrial Internet equipment in China are analyzed, and specific implementation paths regarding network security management and protection for industrial Internet equipment in China are discussed. Furthermore, several development suggestions are proposed. Specifically, the network security access mechanism of industrial Internet equipment should be improved at the national level, a network security testing and certification system for the equipment should be established, research on the network security architecture and engineering application of the equipment should be promoted, and network security risk monitoring and perception of the equipment should be strengthened.

Keywords: industrial Internet equipment; network security; management; protection; certification

1 Introduction

The industrial Internet is a product of the integration of next-generation information and communication technology and the industrial system. A secure guarantee for industrial integration and transformation and the construction of an industrial Internet security assurance system are the preconditions for the development of industrial Internet security. Under the trend of internetworking and data sharing, the industrial system experiences an increasingly fast opening and integration. Because the traditional industrial system is relatively closed and isolated, its safety management and operation and maintenance (O&M) models, which are oriented through production safety, cannot adapt to the complicated and volatile application environment of the industrial Internet. In addition, industrial control systems and equipment have vulnerabilities and backdoors. They also are vulnerable and require a highly real-time performance. For these reasons, they cannot adopt the same security protection pattern as traditional information systems. It is therefore important to build relevant network security capabilities.

With the deepening integration of information technology and traditional industrial operation technology, the network security protection capabilities of industrial Internet equipment will directly influence industrial production and business operations and become an important part of network security policy control and industrial protection practices. In recent years, equipment and product security has gradually become a focus among traditional powerful industrial countries and are regarded as key content for strengthening network security control and ensuring supply chain security and industrial development. For example, the United States (U.S.) has established a supply chain control system that takes network security review as a means and formulated the *Internet of Things Cybersecurity Improvement Act*. At present, extensive research and applications have been carried out in terms of industrial equipment measurement, operation, maintenance, and quality management. In particular, various methods, such as equipment quality control, predictive maintenance, high-precision measurements, failure analysis, and remote monitoring are used to ensure the functional safety and performance of equipment [1–4]. Active efforts have been made to conduct application research on the functional security of equipment, focusing on new technologies such as industrial big data and artificial intelligence (AI) [5–8]. Overall, existing research on the network security of industrial Internet equipment is still lacking. The network security issues faced by industrial equipment should not be ignored, whether guaranteeing the security of the functional performance of the equipment or using new technologies to strengthen the equipment health management and monitoring.

In this study, the requirements and problems are analyzed, the development status is summarized, and the implementation paths concerning the network security of industrial Internet equipment are demonstrated. Several development suggestions are also proposed, with the aim to provide a mode of thinking for basic policy research related to the industrial Internet equipment.

2 Concept and requirement analysis of security protection for industrial Internet equipment

2.1 Concept of the security protection for industrial Internet equipment

Industrial Internet equipment refers to devices or equipment that connect to an industrial Internet network in a wired or wireless manner during the process of integrating next-generation information technology with industrial production, manufacturing, operation, and management. Such equipment is characterized by diverse types, functions, and application forms. Industrial Internet equipment falls in various categories: industrial control equipment, such as a programmable logic controller (PLC) and remote terminal unit; industrial network and security equipment, such as industrial switches and industrial firewalls; and industrial intelligent terminal equipment, such as data acquisition gateways, video surveillance equipment, and Internet of Things (IoT) related equipment. From the perspective of equipment security and security protection during the equipment application process, the security protection of industrial Internet equipment is subdivided into hardware security, network communication security, system service security, application development security, and data security (Fig. 1).

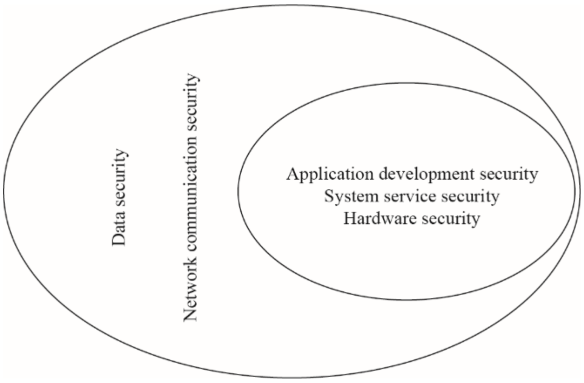
Data security
Network communication security
Application development security
System service security
Hardware security

Fig. 1. Scope of the network security of industrial Internet equipment

Hardware security consists of rights control on the debugging interface of equipment, chip security protection, and prevention of threats and risks associated with a statistical analysis of the equipment power consumption and other information. At present, most network and IoT equipment retains a hardware debugging interface. Some interfaces can even obtain permission to operate without verification and are therefore extremely likely to become an ingress for malicious attacks and data theft, leading to the leakage of equipment information such as key and authentication information.

Network communication security includes communication authentication and communication encryption. The latter is further divided into network layer encryption, transport layer encryption, and application layer data encryption. If the equipment has insufficient access rights control during a network communication, attackers can initiate man-in-the-middle attacks among the equipment and between the equipment and the host system through identity forgery. In this case, the attacks are extremely likely to spread quickly and form a botnet, which then acts as a controlled end to launch massive attacks on the network. In addition, the communication encryption capability of the equipment is also insufficient, making it easy for hackers to steal identity information of users or equipment, resulting in a leakage of important industrial data.

System service security consists of operating system rights control, baseline security configuration, a security mechanism for system updates, system intrusion prevention, and malicious code prevention. Attackers can use vulnerabilities or defects in the equipment system (or firmware) to intrude into the equipment and implant malicious

DOI 10.15302/J-SSCAE-2021.02.011

code during an upgrade, which increases the difficulty in attack source traceback and investigation.

Application development security includes access control among component resources, user authentication and authorization, external interface security, security protection for configuration files and important data, communication protocol encryption, vulnerability and risk investigation for third-party component libraries, and security code design. If the equipment has an underperforming security mechanism, attackers can use application security vulnerabilities or defects to intrude into the equipment and system and initiate a targeted attack.

Data security consists of the protection of data integrity, privacy, and availability, which prevents data from theft, monitoring, and tampering. To accelerate a digital transformation, industrial enterprises are beginning to deploy IoT and intelligent equipment such as data acquisition and edge computing equipment on a large scale. The openness, sharing, and mobile utilization of industrial production process, business data, and user information shows an exponential growth. Many industrial equipment and industrial networks still witness a plaintext data transmission, and thus they have difficulty detecting non-intrusive and passive data monitoring activities on the equipment. If the equipment has underperforming data protection and privacy protection mechanisms, information such as key process parameters and process data is prone to leakage or malicious tampering.

2.2 Analysis of security protection requirements for industrial Internet equipment

Differentiated management and protection need to be applied to security issues such as the functional, network, and data security of industrial Internet equipment based on the application cycle and intelligent attributes of the equipment. The prevention, investigation, and resolution of network security vulnerabilities in actual application forms should also be taken into consideration during security management and protection.

Some equipment does not consider network security issues in the design and development process. A long-term uninterrupted operation makes it difficult to conduct in-depth security inspections or deploy security protection measures, rendering varying degrees of vulnerability and potential problems. According to the statistics of the China National Vulnerability Database (CNVD) [9], vulnerabilities related to industrial control systems and equipment reached 2955 as of December 2020, and 593 of such vulnerabilities were newly added during the year. According to the results of the security evaluation and monitoring of industrial Internet equipment by the China Academy of Information and Communications Technology, a considerable amount of industrial Internet equipment has medium- to high-risk vulnerabilities such as instruction tampering, sensitive information acquisition, and rights bypass. Some industrial security equipment even has high-risk vulnerabilities and apparently insufficient security protection capabilities. In China, some industrial Internet equipment systems constantly suffer from targeted scanning and malicious infections from outside China, as well as from botnets, Trojan horses, worms, and viruses. The frequency and number of attacks on web pages and systems continue to increase in China. In China’s industrial sector, commonly used systems such as Rockwell PLC and Siemens Windows Control Center all have severe high-risk vulnerabilities. Therefore, all industrial enterprises and equipment suppliers have found it necessary to achieve in-depth vulnerability detection, particularly non-destructive security detection and protection, in industrial Internet equipment.

From the perspective of equipment application cycle and applicable network security protection measures, industrial Internet equipment requires differentiated, categorized, and hierarchical network security management and protection. One category of industrial Internet equipment is the “inventory” equipment deployed. Owing to their specific resource and performance constraints and long-term operation, it is extremely likely that network security testing has not been carried out for a lengthy period of time, making it difficult to fully grasp any potential problems. Regarding the security protection for this category of equipment, various measures such as a superimposition of protective measures and monitoring and awareness should be taken based on an analysis of actual application situations to strengthen risk prevention and control. The other category is “incremental” equipment newly placed into application, particularly intelligent equipment with remote control, data acquisition and analysis, and computing and processing functions. Such equipment usually uses common operating systems (e.g., embedded Linux), which to some extent makes it less difficult for attackers to intrude into the systems. If some pieces of intelligent equipment are maliciously controlled and attacked, they may have the ability to spread the attack on a large scale and turn into a “stepping stone” before becoming part of an intelligent attack. Regarding security protection for this category of equipment, it is necessary to integrate the functions, application scenarios, and supporting business needs of the equipment. In addition, the design of various mechanisms such as hardware security protection, network communication, and data security mechanisms should be enhanced. Moreover, measures such as network security perception, monitoring and warning, and emergency handling need to be taken.

3 International development status of industrial Internet equipment security

3.1 Security supervision and review

Traditional powerful industrial countries have been constantly upgrading their network security laws and regulatory measures to gradually strengthen network security reviews. Such laws and measures involve reviews on security and security capabilities of related equipment and products, as well as the security mechanisms throughout the entire cycle (including equipment and product development, design, and application) and in each link.

The U.S. has upgraded its network security review to a national strategy and an international competitive tool, covering government procurement, critical information infrastructure protection, foreign investment, and the supply chain. The U.S. has also established relatively complete review institutions, procedures, and standards. The supply chain review system, as a key aspect of the U.S. network security review, is representative. In the U.S., the security review content and scope for the supply chains of related technologies, equipment, and products is reaching completion. In addition, a series of mandatory security review specifications have also been issued, and companies are required to sign network security protocols. In 2000, the U.S. National Security Telecommunications and Information Systems Security Committee issued its *National Security Telecommunications and Information Systems Security Procurement Policy*. According to this security policy, products in terms of intrusion detection, firewalls, operating systems, and database management must pass a risk assessment and certification under the framework of the Common Criteria Evaluation and Validation Scheme (CCEVS) of the National Information Assurance Partnership (NIAP)[10]. In 2015, the U.S. Department of Treasury and Department of Commerce required the National Institute of Standards and Technology (NIST) to conduct a supply chain security risk review in accordance with relevant technical standards [11]. In 2020, the U.S. promulgated the *Internet of Things Cybersecurity Improvement Act*, which prohibits federal agencies from purchasing any IoT equipment that does not meet the lowest security standards and requires the NIST to issue standards and guidelines on the use of IoT equipment for federal governments [12].

The United Kingdom requires related equipment and products to pass the Communications-Electronics Security Group (CESG) security certification established by the Government Communications Headquarters before they can be sold. The Ministry of Industry and Trade of Russia focuses on security reviews of strategic industrial transactions by which foreign capital can be introduced [13].

3.2 Security testing and certification

Network security testing and certification is an important link before equipment and products are put into use in the market. It is also a mandatory link stipulated by law in certain countries. At present, the international network information security certification and evaluation system is becoming stable, and common international certification criteria are gradually being established. The international common criteria for certification (CC) coexist with the information technology security evaluation criteria (ITSEC) created in Europe.

Network security testing and certification in various countries are mostly entrusted by relevant institutions or associations (which are in charge) with laboratories, enterprises, and professional agencies. The evaluation system usually consists of one evaluation and certification coordination organization, one evaluation and certification entity, and multiple technical testing agencies. In the U.S. for example, network security testing and certification is managed by NIAP and authorized to relevant evaluation agencies such as laboratories and enterprises; only CC certificates are currently issued. In the United Kingdom, network security testing and certification is in the charge of the CESG. In Germany, network security testing and certification, provided by the Federal Office for Information Security, is authorized to commercial evaluation agencies; both ITSEC and CC certificates are issued.

All countries focus on the formulation of evaluation and certification standards in terms of safety compliance, functions, security assurance, and controllability of equipment and products. The functional and assurance levels are divided to meet the needs of different departments, industries, and users. Among them, an evaluation of the functions and security assurance is the core content of the evaluation and certification. The U.S., Europe, and the International Organization for Standardization (ISO) are all making an effort to establish evaluation-based protection profiles, emphasize function and security evaluations, and give corresponding grades. The international common criteria introduced by the ISO are currently the most comprehensive evaluation criteria, and have become a general evaluation method along with ITSEC. In addition, the U.S. and Germany have attached importance to the implementation of a shared evaluation system for defense, government, and commercial use, which can meet the security requirements of different objects by means of grading and profiles.

DOI 10.15302/J-SSCAE-2021.02.011

In terms of security evaluation and certification for industrial Internet equipment, international organizations and certain countries have established certification systems with their own focus. (1) The ISA Secure certification system is an international accreditation system promoted and set up by the ISA Security Compliance Institute (ISCI). ISCI aims to provide common certifications for industrial equipment, deal with security requirements of industrial equipment, and simplify the equipment procurement process for owners and the equipment insurance process for equipment suppliers [14]. ISA Secure independently certifies industrial automation and control products and systems to ensure network attack prevention capabilities and eliminate known vulnerabilities. (2) The NIST certification system refers to the standard certification system led by NIST and jointly established by relevant industry authorities and industry associations, covering national standards, industry norms, and testing and certification. In terms of implementation, efforts have been made to promote the formation of a security standard certification system covering power, natural gas, petroleum, nuclear energy, and other industries and turn the system into a *de facto* standard and authoritative guide widely recognized by the U.S. and even the international security community. (3) The Rheinland certification system refers to the security certification and quality assurance evaluation and review of industrial equipment and technical products carried out by the German Technical Monitoring Association (authorized and entrusted by the German government). It provides certification services for embedded systems and equipment, as well as for intelligent electronic equipment. It also offers various services related to industrial information technology, such as security inspections, penetration testing, risk analysis, security manuals, and security training. This certification system covers a wide range of fields such as aerospace, automotive transportation, chemicals, energy, manufacturing and industrial machinery, and power.

4 Development status and problems of industrial Internet equipment security field in China

4.1 Basic information on security supervision and review

In terms of security supervision, national laws and regulations such as the *Cybersecurity Law* and *Cybersecurity Review Measures* have been promulgated one after another in China. Network security review measures for critical information infrastructure have been gradually set up. Mandatory testing and certification requirements have been formulated for critical network equipment and network security-dedicated products. According to the *Critical Network Equipment and Special Network Security Products Catalog (First Batch)*, the equipment or products listed in the catalog shall comply with the mandatory requirements of the relevant national standards and can be sold or provided only after they are certified by a qualified agency or their security tests meet certain requirements [15]. In terms of policy requirements, the *Guiding Opinions on Strengthening Industrial Internet Security* requires that the secure access and protection of equipment such as industrial production, mainframes, and intelligent terminals be strengthened, and the security assurance of control network protocols, devices and equipment, and industrial software be enhanced. In addition, efforts should be made to encourage increasing cooperation among equipment suppliers, automation integrators, and security companies, and the intrinsic safety of equipment and control systems should be improved [16].

4.2 Basic information on security testing and certification

The evaluation and certification system for network and information security is mainly operated by the Certification and Accreditation Administration of the People's Republic of China. Its implementation is promoted jointly by the National Information Security Evaluation and Certification Administration Committee of China, the China Cybersecurity Review Technology and Certification Center, and related laboratories and evaluation agencies. A promoting system that integrates the regulatory institution, national certification entities, and authorized evaluation agencies has basically been derived. It should also be noted that the existing evaluation and certification system focuses on general basic equipment and products and special critical equipment in certain industry sectors represented by medical care. The existing system lacks normative and universal network security evaluation and certification for critical industrial Internet equipment such as industrial control equipment, large automation equipment, and industrial network communication equipment.

In terms of standards and evaluations related to the security of industrial Internet equipment, China has issued relevant national and industry standards such as the *Technical Requirements of Industrial Control System Dedicated Firewall*, *Information Security Technology—Security Requirements for Measurement and Control Terminals of Industrial Control Systems*, and *Provisions on Security Protection of Power Monitoring Systems*. In terms of terminal security protection of IoT equipment, China has also issued standards or guidelines such as the *Information Security*

Technology—Guide to Password Protection for Intelligent Networking Equipment, and *Information Security Technology—Technical Requirements for the Security of Isolation Components of Network and Terminal Equipment*. In recent years, the China Academy of Information and Communications Technology and other institutions, while considering the application security needs of the industrial Internet industry, have promoted the release of standards such as *Security Protection Requirements of Industrial Internet Equipment*, carried out security testing and evaluation of industrial Internet equipment, and established industrial Internet security evaluation agencies and teams.

4.3 Problem analysis

First, there is a lack of special management methods and testing and certification systems for industrial Internet equipment security. Although industry administrations have formulated relevant policies and standards, their requirements and degrees of systematization are insufficient, and they lack requirements for the network security adaptability of new technologies and new application forms. The security protection of industrial Internet equipment is basically at the level of industry self-discipline.

Second, the Catalog of Critical Network Equipment and Security Products does not cover critical industrial Internet equipment, and products that are not included in the catalog lack necessary and systematic network security reviews. It is difficult to guarantee the security and protection capability of critical equipment and products, such as industrial production equipment, critical equipment, and industrial Internet security products. As a result, industrial production and business operations face security threats, and there are unknown risks in the equipment supply chain.

Third, there are many types and large quantities of industrial Internet equipment. The current security protection capabilities and guarantee levels cannot meet the needs of industrial transformation and upgrading. The security operation requirements of industrial equipment such as PLCs, industrial mainframes, and industrial firewalls are not yet clear. The security standards and specifications of equipment in the process of networked and digital applications are relatively lacking. Special evaluation specifications and implementation systems need to be improved. The existing network security testing and certification system has failed to meet the requirements of practical applications, market demand, and network security reviews of other countries.

Fourth, there are few national standards related to the security of industrial Internet equipment and products. Mandatory network security standards are absent. In addition, evaluation and testing process methods, institutional personnel, and certification systems are apparently lacking. At present, the security of industrial Internet equipment itself has difficulty meeting the requirements of different industries and market levels. In addition, industrial Internet equipment and products made in China lack authoritative evaluation and certification when entering the international market, and thus they cannot adapt to the requirements of international mutual recognition and network security reviews of other countries.

5 Implementation paths of security protection for industrial Internet equipment in China

In view of the diversified types, large quantities, decentralized security management, and different industry self-discipline levels of industrial Internet equipment, overall planning should be conducted from the perspectives of the country, industry, and application so as to strengthen national supervision, industry certification, and network security engineering applications. This study demonstrates the implementation paths of network security management and protection for industrial Internet equipment in China (Fig. 2). It aims to improve the adaptability and capabilities of industrial Internet equipment, implement security assessment and management by category and level, and optimize standards and specifications, testing and certification, and the risk management and emergency handling mechanism.

The first step is to establish a security strategy and basic capability set for the equipment, including the basic requirements for an equipment security architecture design, security baseline configuration, root of trust verification, and categorized and hierarchical protection. The security baseline established for the equipment strengthens the endogenous security capabilities of the equipment.

The second step is to carry out categorized and hierarchical assessments for industrial Internet equipment of different types and application scenarios based on the network security risks, protection value, and security impact of incidents with the equipment. A categorized and hierarchical catalog is set up to sort out key protection equipment and formulate corresponding security strategies, which are then included in a catalog of critical network equipment and network security products. With this catalog, mandatory security testing, as well as certification and review, can be efficiently carried out.

The third step is to improve the security protection specifications and the requirements for categorized and hierarchical protection of industrial Internet equipment. For equipment of different categories and protection levels, efforts can be made to improve the technical protection requirements for application development security, system service security, hardware security, network communication security, and data security, among other factors to form a differentiated and refined management mode for the network security of the equipment.

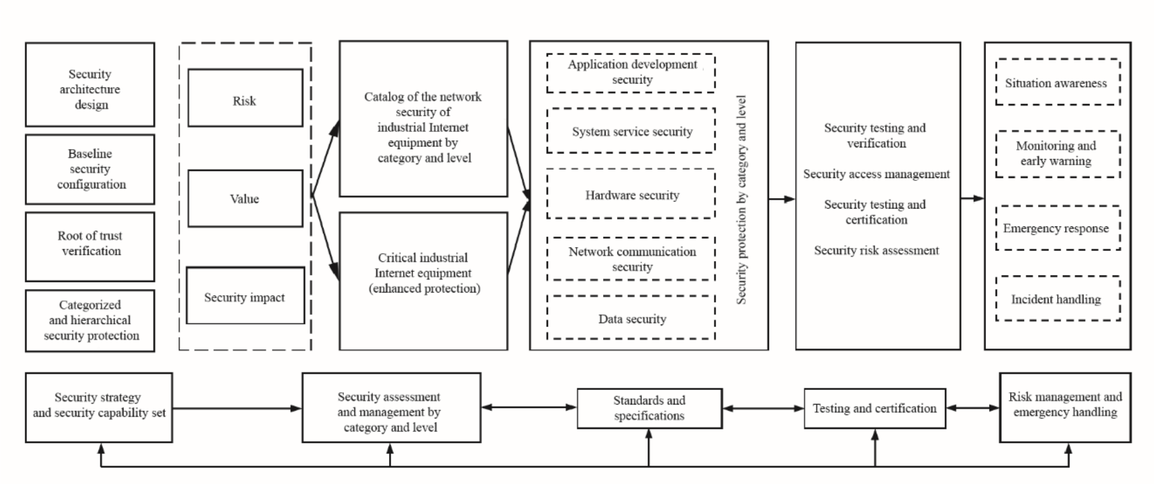
Security architecture design
Baseline security configuration
Root of trust verification
Categorized and hierarchical security protection
Risk
Value
Security impact
Catalog of the network security of industrial Internet equipment by category and level
Critical industrial Internet equipment (enhanced protection)
Application development security
System service security
Hardware security
Network communication security
Data security
Security protection by category and level
Security testing and verification
Security access management
Security testing and certification
Security risk assessment
Situation awareness
Monitoring and early warning
Emergency response
Incident handling
Security strategy and security capability set
Security assessment and management by category and level
Standards and specifications
Testing and certification
Risk management and emergency handling

Fig. 2. Implementation paths of security protection for industrial Internet equipment

The fourth step is to establish a network security testing and evaluation system for industrial Internet equipment. The network security test verification, access review, testing and certification, and normalized security risk assessment in the application process before the equipment enters the market are strengthened. With the assessment promoting construction, a closed loop of equipment security protection can be formed.

The fifth step is to strengthen the risk management and emergency response for industrial Internet equipment security, including situational awareness and monitoring and early warning for network security of critical industrial Internet equipment, industry-side/enterprise-side emergency response, and tool platforms and mechanisms for incident handling. A real-time grasp of equipment security situation and risk view provides a normalized technical means for early risk warning and emergency tasks.

6 Countermeasures and suggestions

6.1 Improving network security access mechanism of industrial Internet equipment at the national level

It is recommended that the administrations study and formulate management measures related to the security of industrial Internet equipment and promulgate mandatory standards and industry norms for its security. Network security specifications and requirements should be strengthened for the entire industrial Internet equipment lifecycle (including the design, development, implementation, and O&M) to provide a basis for enterprise product security development, testing and certification by third-party organizations, and equipment deployment and operation. After the *Critical Network Equipment and Special Network Security Products Catalog (First Batch)* was issued, testing and certification for the equipment and products listed in the catalog has been gradually carried out; however, unlisted equipment such as industrial Internet equipment is still beyond supervision. It is therefore necessary to study and sort out the critical industrial Internet equipment, list it as critical network equipment and network security-dedicated products and classify the equipment by category and protection level. It is also necessary to improve the relevant security standards and specifications and establish a sound industrial Internet equipment security supervision and security access mechanism. In this case, the equipment must undergo strict security testing before entering the market for sale or use.

6.2 Establishing a network security testing and certification system for the equipment

It is recommended to establish a security testing and certification system for industrial Internet equipment and strengthen security testing and verification, particularly the security testing and verification, non-destructive testing, and industrial-grade security protection applications of industrial equipment in an industrial onsite environment. Promoting the construction of industrial Internet equipment security evaluation and certification centers is also recommended. In addition, categorized hierarchical network security management and differentiated protection should be carried out based on the designed security certification levels, such as equipment security and protection levels. It is necessary to provide security level options for different departments, industries, and enterprises, and accurately classify the equipment security capability levels. In this way, a healthy market competition environment can be enhanced, and manufacturers are encouraged to upgrade the security of their own equipment. It would be appropriate to promote improvements to the security testing and certification as well as the equipment capabilities. The requirements for the applicability of industrial Internet equipment to an industrial environment, hardware security, system/firmware security, application security, data security, and access security should be matched. In addition, security functions and various security capabilities, such as anti-penetration, malicious code prevention, anti-distributed denial of service attacks, and vulnerability protection should be established.

6.3 Promoting research on network security architecture and engineering application of the equipment

During the design phase of industrial Internet equipment, security factors should be fully considered to enhance the comprehensive security protection capabilities of the equipment, including hardware security, access authentication security, data transmission security, code security, and system service security. It is also necessary to establish a trusted computing environment for the equipment and introduce the hardware root of trust to perform a credible verification for various behaviors such as a system startup, application operation, and parameter modification. In terms of the baseline configuration for equipment security, equipment manufacturers are urged to clearly indicate safe use guidelines to users during product deployment and use technical means to ensure the baseline configuration security of the equipment. Industry-related equipment manufacturers and automation integrators should strengthen their cooperation with research institutions and security enterprises to accelerate the application of new technologies such as blockchain, domestic cryptography, and trusted computing and to promote the research and innovation of the intrinsic safety of the equipment and its technical products.

6.4 Strengthening network security risk monitoring and perception of the equipment

There is a great variety of industrial Internet equipment available. The protection technology capabilities vary greatly with industries and scenarios. For the industrial sector (particularly the manufacturing industry), it is recommended that the testing and assessment of security concerning industry-specific equipment procurement and the application and network transformation be promoted, and that the security monitoring and management of industrial production equipment, industrial mainframes, and related intelligent terminals be strengthened. The administrations should guide the industry in strengthening the security monitoring and emergency handling capabilities of industrial Internet equipment. In particular, the security monitoring and perception, situation investigation, information sharing and notification, and emergency handling of the equipment should be enhanced, and timely warnings should be provided in case of cyberattacks such as Trojan horse infections, viruses, or host control. It is also necessary to establish tool libraries for security detection and emergency response of Industrial Internet equipment and security knowledge bases such as vulnerability and threat intelligence databases. Emergency handling should be implemented as quickly as possible to prevent hackers from exploiting vulnerabilities and initiating more extensive attacks.

References

[1] Zhang Y. Discussion on high-precision measurement methods in the installation of industrial equipment [J]. Technology and Economic Guide, 2019, 27(24): 72. Chinese.

[2] Zhang B, Teng J J, Man Y. Application research of improved parallel fp-growth algorithm in fault diagnosis of industrial equipment [J]. Computer Science, 2018, 45(S1): 508–512. Chinese.

[3] Samigulina G, Samigulina Z. Diagnostics of industrial equipment and faults prediction based on modified algorithms of artificial immune systems [J]. Journal of Intelligent Manufacturing, 2021 (1): 1–18.

[4] Compare M, Baraldi P, Bani I, et al. Industrial equipment reliability estimation: A bayesian weibull regression model with covariate selection [J]. Reliability Engineering & System Safety, 2020, 200: 1–10.

[5] Yu P Y. Research and application of equipment health and failure analysis based on industrial big data [D]. Shenyang: University of Chinese Academy of Sciences(Master’s thesis), 2017. Chinese.

[6] Jin H J. Research on remote monitoring system of industrial equipment based on Internet of things [J]. Industrial & Science Tribune, 2020, 19(14): 35–36. Chinese.

[7] Dai R Z. The application of artificial intelligence technology in the intelligent operation and maintenance of industrial equipment and systems [J]. China Information, 2020 (7): 52–53. Chinese.

DOI 10.15302/J-SSCAE-2021.02.011

[8] Mourtzis D, Angelopoulos J, Panopoulos N. Intelligent predictive maintenance and remote monitoring framework for industrial equipment based on mixed reality [J]. Frontiers in Mechanical Engineering, 2020, 6(12): 1–12.

[9] Critical Infrastructure Security Response Center. Industrial control system vulnerabilities [EB/OL]. (2020-12-01)[2021-01-05]. https://ics.cnvd.org.cn/. Chinese.

[10] Committee on National Security Systems. Frequently asked questions (FAQ) [EB/OL]. (2001-10-16)[2021-01-05]. https://www.niap-ccevs.org/Ref/FAQ.cfm#cat32.

[11] Department of Homeland Security. National strategy for global supply chain security [EB/OL]. (2017-07-13) [2021-01-05]. https://www.dhs.gov/national-strategy-global-supply-chainsecurity.

[12] Warner S, Mark R. S.734 - Internet of Things cybersecurity improvement act of 2019 [EB/OL]. (2019-06-19)[2021-01-05]. https://www.congress.gov/bill/116th-congress/senate-bill/734.

[13] Cyberspace Administration of China. Cyberspace security review system and case analysis for several countries. [EB/OL]. (2015-04-17)[2021-01-05]. http://www.cac.gov.cn/2015-04/17/c_1114990146.htm. Chinese.

[14] ISA Secure. IEC 62443 conformance certification certifying industrial control system equipment and systems [EB/OL]. (2021-01-05)[2021-01-05]. https://www.isasecure.org/en-US/Certification.

[15] Cyberspace Administration of China. Announcement on the issuance of the *Critical network equipment and special network security products catalog (first batch)* [EB/OL]. (2017-06-09) [2021-01-05]. http://www.cac.gov.cn/2017-06/09/c_1121113591.htm. Chinese.

[16] Ministry of Industry and Information Technology of the People's Republic of China. Guiding opinions on strengthening industrial Internet security work [EB/OL]. (2019-08-28)[2021-01-05]. https://www.miit.gov.cn/zwgk/zcwj/wjfb/txy/art/2020/art_c41cb8a2f6e74e239bae96068a2dc024.html. Chinese.