DOI 10.15302/J-SSCAE-2021.02.008

Security Development Path for Industrial Internet Supply Chain

Fan Peiru, Li Jun, Wang Chonghua, Zhang Xueying, Hao Zhiqiang

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

Abstract: While an effective industrial Internet supply chain improves production efficiency and reduces operating costs of enterprises, it broadens the attack surface of industrial control systems and production equipment, introducing new security risks. This study focuses on the security development path of the industrial Internet supply chain. First, the current status of the industrial Internet supply chain is introduced. Subsequently, typical security problems are summarized and challenges for China are analyzed. Furthermore, an innovative security development path is proposed for the industrial Internet supply chain. Considering the full range of manufacturing, China should further enhance the layout of intellectual property for the industrial Internet and construct an industrial system for information innovation. Moreover, its capabilities to technically guarantee channel security for the industrial Internet supply chain should be promoted. Furthermore, coordinated development between upstream and downstream enterprises should be encouraged, and a secure development environment should be optimized for the industrial Internet supply chain.

Keywords: industrial Internet; supply chain; network security; development path

1 Introduction

With the deep integration of the manufacturing industry and the new generation of information technology, the industrial Internet emerged. The industrial Internet has increasingly become the key support of the new industrial revolution and an important cornerstone of Chinese strategy: deepening Internet Plus Advanced Manufacturing. As an indispensable organizational form in the industrial field, the supply chain also plays a critical role in manufacturing. The supply chain takes customer demands as the guide, improves quality and efficiency as the goal, and integrates resources to achieve efficient collaboration during the process of product design, procurement, production, sales, and service. The industrial Internet has continuously enhanced the driving force of industrial transformation. Abundant new models and new formats emerged in the industrial field [1]. With the continuous integration of the industrial Internet and the real economy, the industrial supply chain has gradually carried out digital transformation, forming the industrial Internet supply chain.

In this paper, the industrial Internet supply chain is defined as a network composed of a group of processes and resources involved in industrial design, research, development, raw material procurement, processing, assembly, manufacturing, transportation, and sales under the industrial Internet architecture. It includes manufacturers, wholesalers, logistics providers, distributors, and other enterprises involved in industrial manufacturing. It also includes information and communication products, and services involved in data aggregation, analysis, and management among enterprises. The industrial Internet supply chain can meet the needs of aggregation, analysis, and reuse of enterprise data promptly while promoting production efficiency and reducing operating costs. However, the industrial Internet supply chain also expands the attack area of the industrial control system and

Received date: January 16, 2021**; Revised date:** February 23, 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): 056–064

Cited item: Fan Peiru et al. Security Development Path for Industrial Internet Supply Chain. *Strategic Study of CAE*, https://doi.org/10.15302/J-SSCAE-2021.02.008

production equipment. Therefore, this introduces new security risks.

At present, there are frequent security incidents with the industrial Internet supply chain worldwide [2–4], threats such as supply interruption, and intensified network attacks. These include major production accidents, important economic loss, and even the endangerment of social stability and national security. It poses a significant hidden threat to the information construction of industrial enterprise. In this context, the security problem in the supply of key technology products in the industrial field has become the focus of attention for multiple sectors in society. Currently, some scholars have analyzed the development and security problems of chips, basic software, industrial Internet platform, industrial applications, etc., and put forward some countermeasures and suggestions [5–8]. However, deficiencies remain in research conducted for security development in the industrial Internet supply chain.

Given this, in 2020, the Chinese Academy of Engineering launched the consulting project Research on Development Strategy of the New-Generation Industrial Internet Security Technology. This project analyzes the technology and development trends in international industrial Internet security and innovatively explores the development path of China’s industrial Internet security technology. As an academic exhibition of the research direction of Industrial Internet Supply Chain Security, this study summarizes the development and security problems of the industrial Internet supply chain and proposes an innovative development direction given the practical challenges for the Chinese industrial Internet supply chain. It provides a reference for the new industrial Internet generation to develop and further improve security.

2 Development situation of industrial Internet supply chain

Against the background of deepening integration of the industrial Internet and manufacturing industry, digitization and globalization are the inevitable trends for developing the industrial Internet supply chain.

2.1 Digitalization

With the development of the Internet Plus action plan in China, new business models continue to emerge. The requirements for industrial on-demand customization, flexible supply, and efficient configuration continue to grow. The production and manufacturing technology system and supply capacity continue to mature. The digital demand and willingness of the industrial supply chain accelerate to release, and the comprehensive digital transformation has become a consensus.

Through the information management and digital information connection of upstream and downstream industrial enterprises, the industrial Internet supply chain fulfills the digitization of all links by providing products and services for information communication. These include demand analysis, raw material sourcing, intelligent manufacturing, warehousing, and risk management of industrial products. Nowadays, competition between industrial enterprises has evolved into competition between industrial Internet supply chains. Based on the docking of various internal and external information systems, the industrial Internet supply chain can improve the accuracy of product technology interaction and procurement plans, and the efficiency of material supply and financial settlement. In addition, it reduces inventory accumulation through real-time acquisition and sharing of business process data such as procurement, warehousing and production, and cooperation with external suppliers. This reduces costs and improves industrial enterprise efficiency. The industrial Internet supply chain breaks the barrier of traditional information, opens up all links from industrial production demand, material supply, logistics, transportation to sales and after-sales. It achieves comprehensive information coverage, resource allocation, sharing, and efficient collaborative operation.

2.2 Globalization

Since China’s reform and opening up in 1978, industrial enterprises have increasingly globalized product research and development (R&D), material procurement, manufacturing, logistics distribution, sales and services, forming a supply chain system with global characteristics. With this change in the global Internet and industrial chain, a core component may contain various key technologies and products, produced and supplied by multiple core enterprises. Simultaneously, these core enterprises may be distributed across multiple countries and purchase raw materials globally.

The industrial Internet supply chain connects multiple industries and realizes efficient cooperation and seamless information transmission of different roles through new technologies such as artificial intelligence, big data, and the Internet of Things. It changes the traditional manufacturing supply chain from a single-link chain to a

DOI 10.15302/J-SSCAE-2021.02.008

networked, multi-level, and all-around link, helping enterprises shorten the supply chain links and reduce costs. According to the *2019 China Import Development Report* issued by the Yangtze River Institute of Industrial Economics of Nanjing University, China has been the second-largest importer globally since 2009, with import sources covering more than 230 countries and regions worldwide. According to the statistics of import and export commodities of China’s General Administration of Customs, the total import volume of industrial products in 2019 was 9.26 trillion CNY, accounting for 64.69% of the total import volume of commodities. This continues to grow compared with the import volume of some commodity categories in 2018. For example, power machinery and equipment increased by 3.8%, general industrial machinery, equipment, and parts increased by 1.5%, and electrical machinery, appliances, and electrical parts increased by 0.8%. In 2019, UPS released the *2019 UPS Ssia Pacific Industrial Buying Dynamics Study*. After investigating the industrial purchasers of enterprises in China, Japan, Thailand, and other countries, they discovered an increasing trend in the modern industry to purchase internationally. About 33% of enterprises in Asia purchase from suppliers outside the region.

3 Analysis of typical security issues in industrial Internet supply chains

The activity diversity and complex structures of industrial Internet supply chain components, such as system and entity, provide an expanded area for potential attacks. Many security incidents have occurred worldwide in the industrial Internet supply chain. In this paper, the main risks are divided into two categories, supply chain breakdown and network attacks.

3.1 Supply chain breakdown

There is a structural and long-term competitive relationship between China and the United States in science, technology, and manufacturing. Meanwhile, China’s industrial Internet supply chain is highly dependent on the United States and other developed countries for some essential technology products. The international situation is changing rapidly. An industrial Internet supply chain break would significantly threaten China’s industrial ecological stability.

With the increasing economic and trade frictions between China and the United States, the United States regularly introduce restrictive measures to block the supply chain of critical areas in China. In 1990, the United States upgraded China on the Priority Watch List. In 1991, China launched a Special 301 investigation, and the *Special 301 Report* published since then included China in the blacklist for key investigation. In 2017, unilateral sanctions were imposed on China. According to the statistics published in the Federal Register of the United States, as of January 2021, the United States has listed 484 Chinese entities in the Entity List to control the export of key emerging technologies, basic technologies, and related products. In 2020, 145 Chinese entities were added to the Entity List. Circumstances such as the absence of chips, memory ban, and shortage of ventilator key components show that the development of China’s science and technology manufacturing industry remains constrained by the weakness of the industrial Internet supply chain.

The distrust among countries increased after the new COVID-19 outbreak; global economic turmoil, unilateralism, and trade protectionism prevailed, significantly affecting the existing global supply chain. It will be necessary for all countries to build a more independent, complete, and secure industrial Internet supply chain. In April 2020, the United States and Japan openly encouraged their enterprises to withdraw from China, and Europe guided the “four for one” plan through the *Free Trade Agreement* (replacing China’s world factories with Japan, South Korea, Vietnam, and India). With the increase in labor cost, trade friction, and other factors, China’s manufacturing industry is at risk of losing its original international competitiveness. China should be alert to the de-sinicization of the global supply chain and industrial chain and make targeted long-term preparations.

3.2 Network attacks to supply chain

With the globalization of the industrial Internet supply chain, the number of suppliers and service providers who can access the core technology products, core components and sensitive data of industrial enterprises has greatly increased. As a result, the attack area of industrial enterprises has substantially expanded. Supply chain attacks against external partners, suppliers, or third-party service providers have become a new threat. Recently, key technology products of the industrial Internet have suffered many attacks in development, delivery, use, and other aspects. Moreover, the key infrastructure damage, sensitive data leakage, information system intrusion, and other network security incidents caused by external partners’ security negligence and defects emerge in an endless stream.

First, industrial manufacturers reserve backdoors. Suppose a manufacturer forgets to delete the debugging backdoor in the test version or the super backdoor reserved for the convenience of after-sales management or other purposes in the development process. In that case, an attacker may discover this and log in directly to gain control of the industrial product. In June 2013, the PRISM scandals revealed the top-secret electronic monitoring plan launched by the United States. In August 2017, the modem produced by Arris, a well-known telecom equipment manufacturer, had three hardcoded backdoor account vulnerabilities, which could be used by attackers to obtain device controllers, install malicious firmware, and set up botnets.

Second, the basic software is polluted. When the development tools, protocol stack, and other basic software are implanted with malicious code or through a backdoor and compiled into other applications for distribution, the threat will spread, which is difficult to find and eradicate by ordinary users after the event. In September 2015, the XcodeGhost event caused concern. The attacker added and spread malicious modules into Xcode, an integrated development tool on the Mac operating system. When developers compile applications with contaminated software versions, malicious logic will be implanted, leading to pop-up attacks and remote control. In China, the number of users infected with the malicious program reached 2.14×10^7 in the same month. In 2018, the OpenSSH tracking report released by ESET, a security company, pointed out that the compiled OpenSSH embedded with backdoor code can be used by attackers to steal legitimate login accounts and passwords.

Third, there are loopholes in industrial products. Attackers use industrial product vulnerabilities to achieve remote device control, denial of service attacks, etc. In March 2018, Cisco issued an early warning of remote code execution vulnerability (CVE-2018-0171) in smart installation clients. Subsequently, the vulnerability was used to attack multiple Internet data centers and organizations in China, resulting in the paralysis of the switch due to the emptying of configuration information and the unavailability of the business network. In February 2019, the refrigeration control system developed by the remote monitoring system manufacturer in Scotland was found to have major security defects. Attackers log in to the system by using the default account and password, and can modify the temperature, alarm threshold, and other refrigeration system parameters, thus affecting the normal operation of equipment.

Fourth, the supply channels of industrial products are hijacked. Industrial products are hijacked and tampered with in purchasing, sales, logistics, and other supply channels, and attackers construct backdoors or loopholes in products to achieve intrusion. In 2009, data industrial control system suppliers, centrifuge manufacturers, and parts suppliers of Iran’s nuclear facilities were attacked by national forces and implanted with a Stuxnet virus. The virus was successfully introduced into Iran’s nuclear facilities and caused damage, which delayed Iran’s nuclear program for several years. In 2015, Kaspersky Security Laboratory disclosed the super information weapons library owned by Equation Group, including malicious modules that can reprogram ten kinds of common brand hardware firmware. The attack can be achieved by modifying the hard disk firmware program while purchasing or repairing the host or hard disk of a specific target. The targets included China, Russia, India, and a few other countries. In 2017, Wikileaks exposed the Vault7 arsenal of the US Central Intelligence Agency. It can be speculated that it hijacked through logistics channels and swiped firmware into the brand-new iPhone to achieve the purpose of invasion.

The fifth security network issue is industrial software upgrade hijacking. Software products need to be updated throughout their lifecycle, including function upgrades and patch repair. However, attackers can plant malicious codes in industrial software by hijacking update modules or download links during a software upgrade progress. For example, in 2017, the upgrade program of Ukraine’s special accounting software, MeDoc, was hijacked. When users updated the software, their devices were infected with the Petya blackmail virus variant NotPetya, which affected the governments, banks, power systems, and communication systems of Ukraine, Russia, India, France, Britain, and other countries to varying degrees.

In recent years, some countries have implemented various dimensions of supply chain blockade on the leading enterprises in China’s communication industry. The absence of hardware will lead to the shutdown of enterprises, and the lack of software will stifle the hardware design and the experimental trial production capacity of enterprises. Typical global network security incidents show that the number of attacks against the industrial Internet supply chain is less than traditional network security incidents. Still, once the attack is successful, it may affect hundreds of millions of users, cause huge economic loss, and potentially threaten national security. Some industries rely on the import of foreign information technology products to alleviate the supply-demand of key parts, which can achieve rapid development in a short time. However, hidden threats remain for China’s industrial Internet security. Therefore, it is necessary to pay attention to the security risk of the industrial Internet supply

DOI 10.15302/J-SSCAE-2021.02.008

chain and explore a targeted development path to address current critical security problems.

4 Security challenges for the industrial Internet supply chain

The security risks of industrial Internet supply chain, such as supply interruption and network attack, are attributed to the following two practical challenges faced by China's industrial Internet supply chain at this stage: Some key technology products are controlled by others, and the network security protection is insufficient.

4.1 Key technology parts and products being controlled by foreign countries

First, China still lags in basic industrial technology. Although China has established an extensive and comprehensive industrial system and has become a world leader in high-speed railways, launch vehicles, and other major equipment, it continues to fall behind other countries with regard to basic industries such as developing essential parts, materials, and technology. A large number of low-end products are exported, while high-end products rely on imports. There is a significant gap with developed countries in some high-end fields, and key core technologies are monopolized. The complexity of basic industrial technology is high, which requires long-term R&D investment. Foreign enterprises have been deeply cultivated in the field for many years, forming high technical barriers. In contrast, China's basic industry started late, and the core technology is backward. For example, in the process of industrial software development, there are many problems, such as the difficulty of building the top-level system architecture, the high threshold of using the design and development program, the high cost of building the hardware environment, the limitation of intellectual property rights, and the tedious maintenance in the later stage. Most enterprises either conduct the secondary development of localization based on foreign technology or integrate other functional applications based on foreign software. However, the core technology property rights of secondary development and agent integration still belong to foreign enterprises, and foreign restrictions are difficult to break.

Second, some key products are highly dependent on foreign enterprises. In terms of industrial software, Chinese aircraft, shipbuilding, metallurgy, chemical industry, biomedicine, electronic information manufacturing, and other key manufacturing fields have long since been accustomed to using foreign industrial software. They do not understand the design principles behind these software and lack the long-term accumulation of basic process R&D data, which leads to a significant gap in the expansion of basic technology. Industrial control systems and software are highly dependent on foreign technical products, and basic industrial software, R&D and design software, production control software, information management software, and industrial embedded software, are imported. Industrial operating systems, industrial software development platforms, real-time industrial databases, and other important fundamental software are not available throughout the industry chain, resulting in almost no industrial control application software. A real-time industrial database must support industrial software; however, there is a lack of domestic industrial real-time database products in China. In terms of computer aided design, analysis, manufacturing, process planning, and other tool software, foreign manufacturers represented by Dassault and Siemens still have absolute advantages. In the manufacturing execution system, industrial automation system, and other key areas of production control, General Electric Company (GE), the Asea Brown Boveri Ltd. (ABB group), and other companies maintain the leading position. In information management software such as supply chain management, customized application integration platform system, and collaborative office system, SAP and Oracle still occupy a considerable share. In industrial hardware, foreign products occupy most of the domestic market for core components (such as industrial microcontroller units, digital signal processing, and the field-programmable gate array) and systems (such as the supervisory control and data acquisition system, programmable logic controller, and the distributed control system). Ultra high precision machine tools, high-end industrial robot technology, and other technology products are essentially in the hands of foreign manufacturers.

Third, the standards of industrial agreements are dominated by foreign standardization organizations and manufacturers. The key core protocols used in industrial Internet infrastructure are formulated mainly by international organizations such as the International Organization for Standardization, International Electrotechnical Commission (IEC), the OPC Foundation, and other major industrial manufacturers. Foreign organizations control various fieldbus communication protocol standards and OPC protocol standards. All types of automation manufacturers, research institutes, and standardization organizations worldwide have launched hundreds of fieldbus protocols, industrial Ethernet protocols, and wireless protocols around equipment networking, with many and relatively closed protocol standards. Siemens Co., Ltd., Schneider Electric Co., Ltd., Rockwell Automation Co., Ltd., and other enterprises have formed a de facto standards monopoly by bundling private agreements, industrial control equipment, and manufacturing equipment. In the fieldbus, Rosemount, Honeywell, ABB, GE, Siemens, etc., have long controlled the development of international standards. In terms of industrial Ethernet, domestic manufacturers mainly choose industrial Ethernet protocols suitable for proprietary industrial control products, such as Siemens Profinet, Schneider Modbus TCP/IP, and Rockwell Ethernet/IP.

4.2 Defects in network security protection

First, the means of network attacks vary, leading to increased risk. The network attack risk in the industrial Internet supply chain comes mainly due to negligence in security and the shortcomings of external partners. Attackers use it to invade enterprise systems and destroy enterprise data. Attacks on the industrial Internet's supply chains involve developing, delivering, and using industrial products. These include four typical elements: (1) polluting of software development, testing, deployment, and maintenance environment or tools, (2) preloading malware on devices, (3) infection of legitimate applications to distribute malware, and (4) theft of legitimate certificate signature. In the face of increasingly common and complex industrial Internet supply chain attacks, raw material procurement, processing, packaging, transportation, quota, after-sales, and many other links may be attacked; network security risks are more prominent. Once the industrial Internet supply chain is attacked, it is difficult to find, but has huge destructive power covering a wide area. It is challenging to manage the high cost and consistent cycle involved in preventing attacks by recalling or upgrading products.

Second, industrial Internet security technology products remain in the research stage. The industrial Internet supply chain includes communication networks, software, hardware equipment, and other information systems involved in industrial products or services from development to delivery, with expanded security protection objects and broader connection scope. The protection objects and traditional network security technology methods are not completely consistent with the industrial Internet supply chain. Direct application without considering the difference will inevitably lead to poor protection effects and security risks. Currently, most security companies in China are mainly engaged in the network security business. They are still at the stage of tackling key problems due to a lack of product accumulation and service experience in industrial information and Internet security. The existing security capabilities focus on improving the single-point security defense capabilities of industrial equipment, industrial control systems, and industrial enterprises, making it difficult to guarantee the security of the entire set of industrial Internet supply chain links. To resist the increasing organized, targeted, and cost-free network attacks, it is necessary to reevaluate the security architecture and boundary of the industrial Internet supply chain. A security technology system covering monitoring perception, collaborative defense, and response recovery must be developed.

Third, the security management ability of the industrial Internet supply chain is insufficient. The industrial Internet supply chain involves manufacturers, suppliers, system integrators, service providers, and other entities; also technology, law, policy, and other soft environments. At present, most enterprises in China have problems, such as poor awareness of network attacks, inadequate security management systems, inadequate security detection and evaluation mechanisms, and insufficient guidance in the industrial enterprises' network security. The security of the industrial Internet supply chain depends on the cooperation of all partners in the chain, and significant challenges remain in terms of achieving collaborative development.

5 An innovative development path for industrial Internet supply chain security

China attaches great importance to the security of the industrial Internet supply chain. Since 2016, China has successively issued several policy papers such as the *National Cyberspace Security Strategy*, *Cyberspace International Cooperation Strategy*, *Guidance on Actively Promoting the Innovation and Application of Supply Chain*, and *Notice on Further Doing a Good Job in the Pilot Work of Supply Chain Innovation and Application*. They have also issued several policy documents, such as *Measures for Network Security Review* and *Suggestions of the Central Committee of the Communist Party of China on Formulating the 14th Five-Year Plan for National Economic and Social Development and the Long-Term Goals for the Year 2035*.

Given the practical challenges for China's industrial Internet supply chain security, according to the relevant national policy requirements, this paper proposes an innovative development path for industrial Internet supply chain security (Fig. 1). Based on the advantages of a complete range of manufacturing industries in China, this paper first offers suggestions on three aspects: the layout of intellectual property rights, the construction of information and creative industries, and the technical security guarantee, and then deals with the supply chain interruption and network attacks of industrial Internet through technological means. Second, solutions are provided from three perspectives: paying attention to channel security, upstream and downstream enterprise collaboration, and optimizing the development environment. The effective implementation of security technology for the industrial Internet supply chain is guaranteed through three aspects of security management: supply channel, enterprise collaboration, and overall environment.

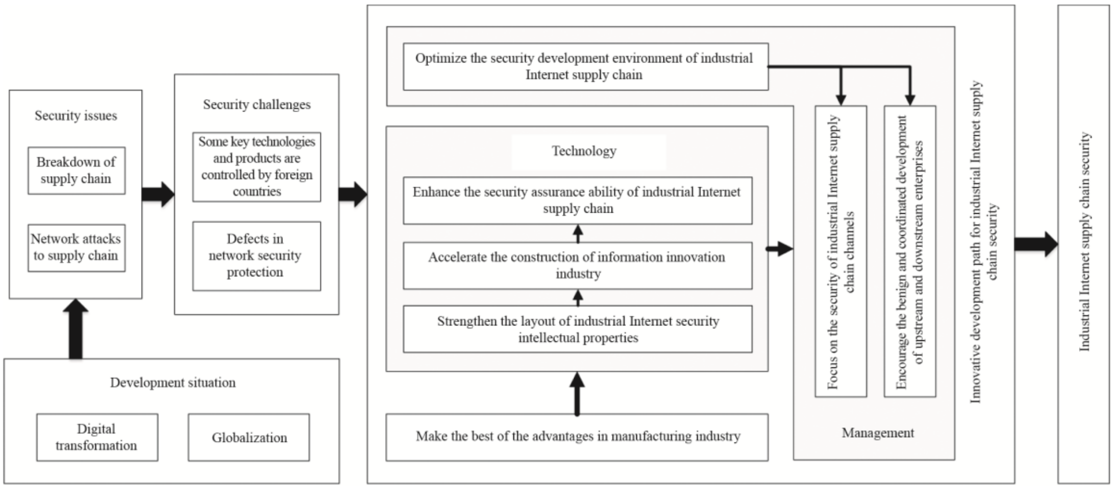
Security issues
Breakdown of supply chain
Network attacks to supply chain
Security challenges
Some key technologies and products are controlled by foreign countries
Defects in network security protection
Development situation
Digital transformation
Globalization
Optimize the security development environment of industrial Internet supply chain
Technology
Enhance the security assurance ability of industrial Internet supply chain
Accelerate the construction of information innovation industry
Strengthen the layout of industrial Internet security intellectual properties
Make the best of the advantages in manufacturing industry
Focus on the security of industrial Internet supply chain channels
Encourage the benign and coordinated development of upstream and downstream enterprises
Management
Innovative development path for industrial Internet supply chain security
Industrial Internet supply chain security

Fig.1. Innovative development path for industrial Internet supply chain security.

5.1 Utilizing advantages in the manufacturing industry

Since the reform and opening up in 1978, China’s manufacturing industry has developed continuously and rapidly. It has built a complete and most extensive industrial system, organically embedded in the global supply chain, forming a significant industrial advantage, providing new opportunities for the security development of China’s industrial Internet supply chain. First, based on China’s super large-scale, multi-level, and diversified domestic demand market, we should take full advantage of China’s complete industrial categories, strong production capacity, complete supporting capacity, and flexible adaptability. We must expand consumption levels and improve the traditional manufacturing industry. The second step is to form a joint force in the middle and downstream industries of various industries, strive to make up for the weaknesses, remove the stasis and blocking points in the industrial Internet supply chain, and promote the smooth flow of all links, industries, and regions in China. Third, we should promote domestic and foreign economic connectivity, build a new development pattern of domestic and international mutual promotion, improve the adaptability of supply and demand in the manufacturing system, drive a high-value, high-level, and systematic supply and demand cycle, and build a complete, safe and reliable industrial Internet supply chain system.

5.2 Strengthen the arrangement of industrial Internet security intellectual properties

Based on industrial-scale advantages, supporting advantages, and first-mover advantages in some fields, China can address the weaknesses in industrial Internet supply chain security. New ideas, theories, methods, models, and discoveries can be used to improve the layout of the industrial Internet Security intellectual property rights. In this manner, China can forge longboard advantages from the foundation and alleviate the threat of supply breakdown. First, China should strengthen the research on fundamental theory and cutting-edge technology, pay attention to originality, and give full play to the source supply and leading role of basic research in the security of industrial Internet supply chain. Second, standards development should be strengthened. The synchronous development and synchronization of safety standards for the industrial Internet supply chain concerning industrial Internet supply chain digitalization and globalization requirements, should be promoted. The following aspects must be enhanced: the standards quality of applicability, level of advancement, standardization, standards information service levels, compliance testing, and the participation level in shaping international standards. Third, we should improve the intellectual property risk assessment system, strengthen the patent layout of all links and supply chain fields, and explore the establishment of an improved intellectual property risk assessment approach. Also, we should maximize the due role of intellectual property in security patent licensing, technology transfer, open-source software risk assessment, industrial data, and trade secret protection, to effectively improve risk response capability.

5.3 Accelerate the construction of information innovation industry

It is necessary to realize the innovation and development of information technology applications in the entire industrial chain from the basic IT software and hardware to upper application software, focusing on industrial system construction. Based on the advantages of complete types of industrial manufacturing industries and good information establishment in China, we should accelerate the construction of the information innovation industry system. We must avoid the potential risks pertaining industrial manufacturers' reserved backdoor or development tools that may exist in the direct use of foreign technology products. One option is to formulate and develop an innovative industrial plan for information technology application, promote the innovation and development of key products of the industrial Internet supply chain security from two aspects of technology system introduction and industrial foundation strengthening, focus on breaking through high-end manufacturing and high-tech products, and consider intelligent manufacturing as a new direction for industrial upgrades. Second, promote the large-scale deployment of key technologies and products of the application innovation industry, conduct pilot applications, and form scalable, replicable, and portable solutions and pilot demonstration by industry and scene. The third is to build an application innovation industry chain of information technology, build a regional industrial cluster, and build a complete industrial Internet supply chain. These systems must cover chips, servers, storage, switches, operating systems, databases, middleware, industrial operating systems, government software, office software, etc., so as to ensure the security of industrial intelligent chips, industrial control systems, and other industrial equipment during industrial design, production, processing, and sales.

5.4 Enhance the security assurance ability of industrial Internet supply chain

The industrial Internet supply chain involves a variety of entities and links. The direct application of traditional network security technology will lead to a poor protection effect. Therefore, it is necessary to conduct core technology research for security protection of the industrial Internet supply chain to resist increasingly complex network attacks. First, it is necessary to analyze the new characteristics and requirements of the security protection objects for the industrial Internet supply chain, and learn from the traditional network security technology ideas and methods to develop a technical system that can consider all aspects of the industrial Internet supply chain security. The second enhancement is to study the safety detection technology of industrial products, and increase resource investment in open-source code security detection, vulnerability mining and analysis, malware identification and removal, network hijacking detection, intelligent intelligence, and dynamic early warning, thereby maximizing the role of technological innovation in the safety protection of industrial products. The third recommendation is to study the safety defense technology of industrial products and improve the safety control ability through safety identification, safety review, product traceability, counterfeit product investigation, threat monitoring, situation awareness, and attack and defense drills of industrial products. Fourth, it is necessary to integrate and apply new technologies to ensure the security of the industrial Internet supply chain, and study the application of artificial intelligence, blockchain, trusted computing, threat intelligence, knowledge mapping, and basic security resource library in security technology to promote security technology systems. Fifth, China should promote enterprise-side industrial software and hardware security protection measures and track enterprise information assets. To ensure protection, the following aspects should be strengthened: safe access and protection of industrial production, mainframes, intelligent terminals and other equipment; network protocol, equipment, and industrial software; and the security of the industrial Internet platform and applications. It is also necessary to strengthen the security protection of key information and data in the application process, implement the requirements of relevant network security standards, and improve enterprise internal and external network security protection ability.

5.5 Focus on the security of industrial Internet supply chain channels

The transfer process of products, components, and software in the industrial Internet supply chain from upstream to downstream depends on the Internet. If any link is attacked, software defects or loopholes may be introduced into final industrial products, presenting a security risk. Attention should be paid to industrial Internet supply chain channel security and the handling of attacks on the supply channel for industrial products and software upgrades. One option is to design targeted security measures for various channels in the supply chain, focusing on ensuring the security of centralized distribution channels responsible for software and product delivery and supporting software suppliers and users in the timely identification of malicious channels. Second, technology

DOI 10.15302/J-SSCAE-2021.02.008

or products should be released through regular channels to provide users with verifiable data. When installing or upgrading the software, the signature of the corresponding installation package or upgrade module should be checked to prevent software upgrade hijacking and other risks. Third, it is necessary to purchase and download software and hardware from regular channels, adopt trusted third-party open source, commercial libraries and algorithms, and purchase safe and reliable software outsourcing services. Attention should be paid to the security information of the components used. Serious security problems that have been disclosed should be controlled by configuring or adding other security measures and upgrading related components on time to alleviate the security impact. Fourth, it is necessary to strengthen the safety management of the cooperative third party, clarify the safety responsibilities of both parties in the contract or agreement, and request cooperative third parties to conduct self-evaluation regularly and feed back the evaluation results on time. Fifth, we should actively introduce professional security professionals and set up full-time network security technical posts and security operation service posts. It is also necessary to establish safe operation and maintenance management systems, strengthen the network security training and audit of enterprise employees, enhance the safety awareness of internal enterprise personnel, and avoid the hijacking risk of industrial Internet supply chain channels introduced by personnel.

5.6 Encourage the benign coordinated development of upstream and downstream enterprises

The industrial Internet supply chain involves various entities and links and is widely attacked. Based on the assumption that some links are bound impacted, it is necessary to promote the linkage and coordination, integration and symbiosis, and collaborative development of upstream and downstream enterprises to resist the endless network attacks jointly. The first is to conduct in-depth investigation and research on key technologies of industrial Internet and the relationship between upstream and downstream supply chains of core enterprises, and integrate and optimize various resource information such as suppliers, manufacturers, distributors, and independent intellectual property rights. Second, China should comprehensively identify and organize the blocking points and difficulties, implement targeted policies, open up the upstream and downstream links, and smooth the supply chain circulation. It should concentrate on the weak links, short supply and demand board of the supply chain and focus on the enterprise’s demand for labor, raw material supply, logistics, and financing. The third is to strengthen the production and marketing docking of the upstream and downstream enterprises of the industrial Internet. It is necessary to encourage chain partners to establish a benign interactive relationship, insist on ensuring the safety of this link, form an ecological community of benefit sharing, risk sharing, and common growth among enterprises, and promote the coordinated and safe development of the industrial Internet supply chain. The fourth is to establish checkpoints in all aspects of industrial production. We should list security assessment as a necessary review item, strictly abide by security norms, and prevent security threats such as backdoors and loopholes caused by configuration errors. Before software and hardware independently developed or purchased are used, independent internal or external evaluation organizations should evaluate them to solve problems promptly.

5.7 Optimize the security development environment

China has issued relevant laws and regulations and relevant security standards to ensure the security of the industrial Internet supply chain. However, compared with the industrial powers, there is still a lack of mechanisms and means to review and evaluate effective network security risks. Besides, the special policies and regulations, supporting measures, organization, and implementation must be improved. Specifically, one option is to establish a targeted management framework for industrial Internet supply chain security, clarify the responsibilities and obligations of all parties in supply chain attack protection, and ensure the security development of the industrial Internet supply chain at a national level. The second is to establish and improve the security supervision system, formulate relevant review and evaluation specifications, test the key industrial software and hardware products, evaluate their safety and compliance, form a responsible supplier list, and manage the suppliers at different levels. The third is to formulate the evaluation standard of the security of the industrial Internet supply chain network suitable for China’s national conditions, focus on the security risks brought by new technologies and applications, strengthen investigation and research, strengthen early warning in the risk assessment of open-source software, enhance industrial data security protection and other aspects, and improve risk response capacity. Fourth, China should promote and support enterprises to establish sound security management systems for industrial Internet supply chains, guide enterprises to develop a supplier audit system, conduct safety assessment of suppliers from the perspectives of industry qualification, management system, technical ability, product quality, network security protection ability, and implement targeted control measures to eliminate unqualified suppliers on time. Fifth, it is necessary to strengthen international cooperation in industrial security, carry out international exchanges in technology, standards, testing, and certification, and establish a multi-channel and multi-level supply chain security system to enhance resilience and form a more innovative, higher value-added, and safer industrial Internet supply chain.

6 Conclusion

At present, the international environment has become increasingly complex, and uncertainty of the world economic and trade pattern has increased significantly. Therefore, the security of China’s industrial Internet supply chain is facing a critical test. As a significant manufacturing country, China has the world’s most complete industrial categories, the most industrial equipment, a rich industrial Internet ecology, and significant industrial and information talent. China should take full advantage by strengthening the layout of intellectual property rights. In addition, China should accelerate the construction of information technology applications and innovation industry systems, enhance the capability to ensure technology security, attach importance to channel security, encourage the benign collaborative development of upstream and downstream enterprises, and optimize the security development environment. By combining technology and management, the security development path of China’s industrial Internet supply chain should be revolutionized to ensure that a positive and constructive approach to the development of the industrial Internet is maintained.

References

[1] He W, Zhang W D, Wang C X. Strategic updating of Internet plus considering digital transformation [J]. Strategic Study of CAE, 2020, 22(4): 10–17. Chinese.

[2] HE X X, Zhang Y Q, Liu Q X. Survey of software supply chain security [J]. Journal of Cyber Security, 2020, 5(1): 57–73. Chinese.

[3] Zhu G B, Chen J. The status and countermeasure suggestion of software supply chain security [J]. China Information Security, 2018 (11): 44–47. Chinese.

[4] Luszcz J. How maverick developers can create risk in the software and IoT supply chain [J]. Network Security, 2017, 2017(8): 5–7.

[5] Gao Q S, Liu H L. Research on industrial chain security of key nodes in the chip industry with deeply interconnected global supply chain [J]. Economic Tribune, 2020 (3): 11–21. Chinese.

[6] Xie J S, Fu X B, Zhao W H. Research on the basic software and hardware ecology for development of information industry [J]. Information Technology and Network Security, 2020 (9): 1–5. Chinese.

[7] Wang C, Song L, Li S K. The industrial Internet platform: Trend and challenges [J]. Strategic Study of CAE, 2018, 20(2): 15–19. Chinese.

[8] Ning Z B. Build the foundation of industry, recast the soul of intelligent manufacturing [J]. Software Guide, 2021, 20(1): 1–5. Chinese.