NSFOCUS

2019 ICS Information Security Assurance Framework

NSFOCUS

About NSFOCUS

Founded in April 2000, NSFOCUS Information Technology Co., Ltd. (NSFOCUS) is headquartered in Beijing. With more than 40 branches and subsidiaries at home and abroad, the company provides most competitive security products and solutions for governments, carriers, and financial, energy, Internet, education, and medical sectors, ensuring customers' business continuity.

Based on years of research in security protection, NSFOCUS has set foot in intrusion detection and prevention, security assessment, security platform, remote security O&M service, and security SaaS service areas. The company provides the intrusion detection/prevention system, anti-DDoS system, remote security assessment system, and web security protection products as well as professional security operations services for customers.

NSFOCUS Information Technology Co., Ltd. started trading its shares at China's Nasdaq-style market, ChiNext, in Shenzhen on January 29, 2014, with the name of NSFOCUS and code of 300369.

Special Statement

All data used for analysis has been anonymized and no customer information appears in this report to avoid information disclosure per GDPR.

CONTENTS

1

Development of ICS Security

1.1 Development of Industrial Intelligence

The following figure shows the development history of industrial control systems (ICSs).

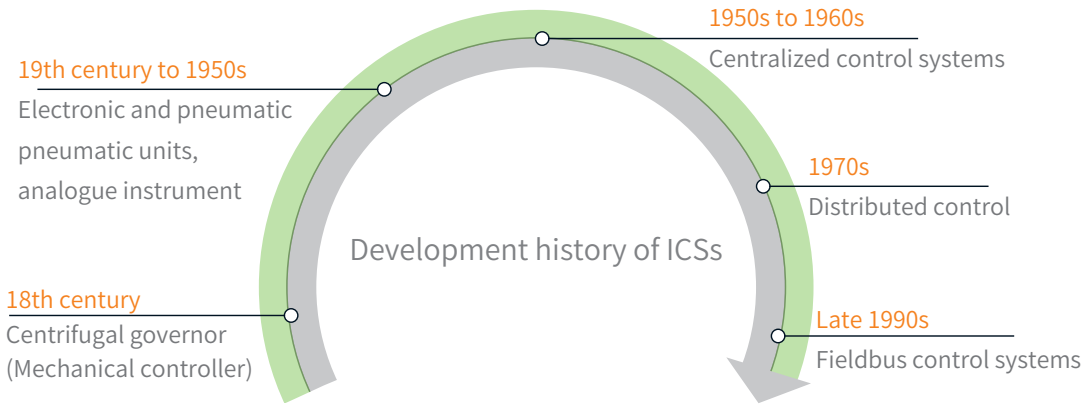


Figure 1-1 ICS development history

The history of ICSs can date back to the 18th century when James Watt improved the steam engine by adding a throttling controller, i.e., a centrifugal governor. The centrifugal governor works like this: It obtains feedback signals by using a shaft around which it rotates with the steam engine. Also, it adjusts the positions of flyballs with the aid of centrifugal force, so as to regulate the steam throttle for control of the rotational speed of the steam engine. It is believed that this kind of centrifugal governor marks the beginning of automatic regulation and automatic control.

Within more than one century since the advent of centrifugal governor, most of industrial control systems were focused on the control of temperatures, pressure, liquid level, and rotational speed of machines. With the development of industrial systems and emergence of a lot of control issues in the military area in World War II, the period from mid-19th century to mid-20th century saw all-round development of control theories (such as negative feedback and control system stability theories) and control systems (including industrial control devices like pneumatic control devices, relay control devices, servers, and feedback loop control components).

In 1950s to 1960s, computer technologies started to be integrated into ICSs where analog control

circuits were gradually replaced by digital control circuits and electrical control circuits were superseded by Programmable Logic Controllers (PLCs). As control systems were digitalized in an all-round way, they can implement more complex control procedures with more sophisticated control algorithms, witnessing a qualitative leap in performance. However, up to now, ICSs are still centralized control systems.

In the mid-1970s, as large-scale industrial equipment emerged, process continuity became increasingly important, and more parameters needed to be controlled, centralized control systems were inadequate to meet ICS requirements, and thus were gradually replaced by distributed control systems. More and more industrial control sectors like mechanical manufacturing, petrochemical, metallurgy, automobile, and light industry, gradually employed distributed control systems.

In late 1990s, fieldbus control systems (FCSs) arrived, integrating computer technologies, network technologies, and control technologies. Compared with distributed control systems, FCSs have higher reliability, stronger functions, more flexible structures, and higher adaptability.

1.1.1 ICS Architecture

Industrial control system (ICS) is a general term that encompasses several types of control systems used in industrial production, including Supervisory Control and Data Acquisition (SCADA) systems, distributed control systems, and other minor control systems like PLCs. The following figure shows the logical architecture of ICSs.

Development of ICS Security

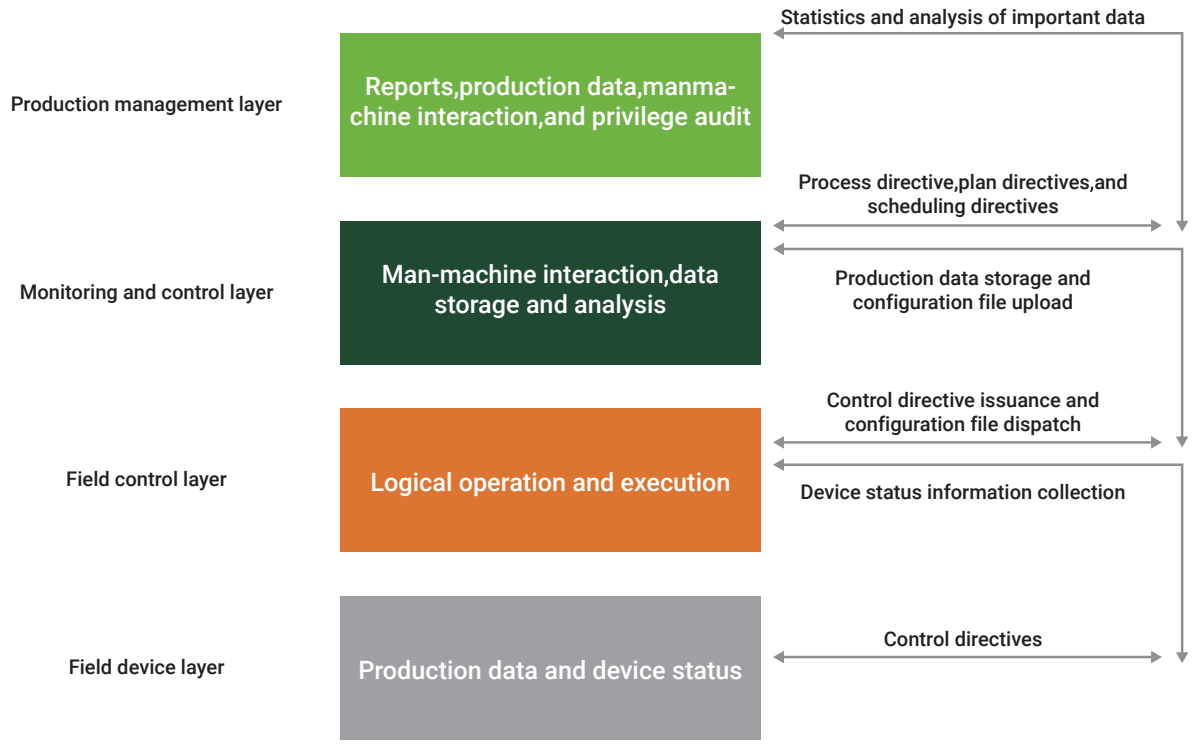


Figure 1-2 Architecture of ICS architecture

The field device layer mainly collects analog and digital values of field instruments, including the force, temperature, and humidity. Those values have different definitions in different scenarios. The field control layer collects data of field i¬nstruments and monitors the operating status of these instruments by following the established logic. In scenarios involving closed-loop control, this layer adjusts and handles the collected data. The monitoring and control layer, based on the computing environment of IT computers, collects, handles, and presents controller data, through various connections to controllers. Configuration ¬¬software configures data indicators of business objects to implement business logic control. Meanwhile, for adaptation to different application scenarios, such software, through screen configuration, matches I/O points for data collection with business scenarios for analysis and presentation of historical production data. The production management layer primarily handles production schedules, optimizes business process directives, and controls scheduling directives. We can see that this layer puts emphasis on management of scheduled tasks.

1.1.2 Industry 4.0

Germany put forward a concept of industry 4.0 at Hanover Fair, noting that it planned to invest 200 million euros to push forward industrial revolution which is based on cyber-physical system (CPS) and characterized by highly digitized, networked, and self-organizing production. By improving computerization, digitalization, and intelligence for the manufacturing sector, Industry 4.0 aims to set up adaptive and resource-efficient smart factories and integrate customers and business partners in the business process and value process.

According to the industrial development history, the steam engine technology sped up the popularization of mechanized production, bringing the human society to the industry 1.0 era; the emergence of electrical power promoted scale production, thus ushering in industry 2.0; the application of informatization technologies made automated production possible, leading the human society to the industry 3.0 era; the in-depth integration of new technologies such as the Internet of things (IoT) and industrial technologies contributes to an intelligent industrial era, i.e., industry 4.0. Driven by requirements for individualized intelligent products, industry 4.0 will enable a new generation of industrial innovations with the strong support of new technologies such as IoT and big data.

Industry 4.0 has the following characteristics:

- Vertical integration: integration of automatic control systems of machines and product lines, the factory's manufacturing execution system, and the enterprise resource planning system. The purpose is to bridge the historic gap between information systems and automation systems to improve the production capability of factories and enterprises.
- Horizontal integration: integration of business systems that are within the enterprise and across enterprise borders. In this way, information sharing and business functions can be integrated across organization borders, thus increasing the overall competitiveness of the value chain.
- Digital integration of the end-to-end value chain: This aims to implement the vision of "intelligent manufacturing cloud". In this case, users can acquire the desired product as long as they submit requirements. Also, manufacturing and business capabilities of enterprises of the related value

chain in the cloud are released in the form of API. This makes fast and flexible combination and secure scheduling and execution possible, thus giving full play to the ecosystem's comprehensive capabilities in multiple aspects such as design, manufacturing, and service.

As new technologies including IoT are becoming mature, traditional industries will be gradually moving toward industry 4.0 after going through a three-stage revolution: manufacturer to manufacturer (M2M), business to business (B2B), and customer to manufacturer (C2M). Transitioning to industry 4.0 will comprehensively boost the business value and capabilities, as demonstrated in accelerated product innovations, optimized production operations, and delivery of brand new services:

- Enterprises, with a high flexibility in production and manufacturing, are more adaptable to production processes of the market.
- If different stages in the value chain interconnect and interact with each other throughout a sound product lifecycle, enterprises have been capable of focusing on user requirements in a professional way.
- The overall competitiveness will be increased on a value chain basis.
- New services and business models will be launched to open up new markets.

Industry 4.0 allows manufacturing enterprises to respond to customer requirements at an unprecedented rate. Emerging technologies implemented in this era will improve the flexibility, speed, efficiency, and quality of production processes. In addition, industry 4.0 brings new commercial modes, production processes, and other innovations. As more and more manufacturing enterprises implement or enhance product customization by putting investment in industry 4.0 technologies, a higher level of massive customization will be a possibility.

1.1.3 Industrial Internet

Industrial Internet is a high-level integration of the global industrial system with advanced computation, analysis, and sensor technologies, and the Internet. Through connections between intelligent machines and finally human-machine connections, the industrial Internet, in combination with software and big

data analysis, will reshape the global industry and increase the production efficiency, contributing to a cleaner, faster and securer world. In traditional ICSs, though most industrial control scenarios have information technologies implemented, real-time information interactions are seldom seen between industrial enterprises, between industrial enterprises and users, and between suppliers. As a result, coordination is conducted in an inefficient way between traditional industrial enterprises and between enterprises and users. Industrial Internet, however, can effectively integrate information resources in industrial systems to increase the production efficiency at a lower cost and implement individualized and intelligent industrial production.

Industrial Internet platforms are actually service systems to collect, aggregate, and analyze massive data, so as to address digitalization, networking, and intelligence requirements of the manufacturing sector. These platforms provide support for industrial cloud platforms that feature ubiquitous connections between manufacturing resources, flexible supply, and efficient configuration. Industrial Internet platforms are essentially built into precise, real-time, and efficient data collection and interconnection systems to provide development environments that encompass industrial big data storage, integration, access, analysis, and management. Such platforms can implement modeling of industrial technologies, experience, and knowledge, standardization, and reuse in the form of software. By constantly optimizing the R&D design, production and manufacturing, operation and management to increase the resource allocation efficiency, enterprises will finally use industrial Internet platforms to build a new manufacturing ecology that features rich resources, multi-party engagement, win-win cooperation, and collaborative evolution. Industrial Internet platforms are positioned as follows:

1. Industrial Internet platforms are an iterative upgrade of traditional industrial cloud platforms. The evolution from industrial cloud platforms to industrial Internet platforms is to achieve a five-stage process: cost reduction, application integration, capability trading, innovation leading industrial development, and ecology building. In addition to software tool sharing and business software integration of traditional industrial cloud platforms, industrial Internet platforms add functions such as open manufacturing capabilities, knowledge and experience reuse, and developer aggregation, significantly increasing the industrial knowledge production, dissemination, and utilization efficiency, constituting an ecology characterized by mutual promotion and bidirectional iteration between a

great number of applications and industrial users.

2. Industrial Internet platforms are "operating systems" of the new industrial system. As industrial Internet platforms rise and develop, the original closed, isolated, and fixed industrial systems will be phased out and flat, flexible, and efficient organizational structures will become the mainstream form of the new industrial system. Equipped with an efficient device integration model, a powerful data processing engine, open development environment tool, and componentized industrial knowledge micro-services, the industrial Internet platforms connects to a large number of downstream industrial equipment, instruments, and products and provides support for rapid development and deployment of upstream industrial intelligent applications, playing an important role that can compare with Microsoft's Windows systems, Google's Android systems, and Apple's iOS systems.
3. Industrial Internet platforms are a kind of efficient carrier for resource aggregation and sharing. Industrial Internet platforms aggregate the information flow, capital flow, talent creativity, and manufacturing tools and capabilities in the cloud; gather industrial enterprises, information communication enterprises, Internet enterprises, third-party developers, and other entities in the cloud; fuse data science, industrial science, management science, information science, and computer science. In this way, such platforms promote integration and sharing of resources, entities, and knowledge, forming a socialized collaborative production mode and organizational model.
4. Industrial Internet platforms are key to enterprises' gaining new competitive advantages. Currently, international leading enterprises including General Electric Company (GE) and Siemens, have introduced an "intelligent machine+cloud platform+industrial app" architecture to integrate "platform provider+application developer+a mass of users" ecological resources to scramble for controlling power over the input of industrial data. Besides, they train a large number of developers and increase user stickiness to constantly gain and consolidate new data-driven industrial intelligence advantages by using platforms as carriers, with the ultimate goal of gaining the vantage point in the new industrial revolution.

1.1.4 ICSs in China

Since the founding of new China, especially the reform and opening up, China has seen rapid development of the manufacturing sector and has built a broad range of integrated industrial systems in various sectors. Since 2013, China has promulgated a whole set of policies to encourage the development of industrial clouds. In 2015, the country put forward the manufacturing strategy, Made in China 2025, in a bid to transform the country from a manufacturer of quantity to one of quality. However, China remains in the course of industrialization and there still exists a pronounced gap compared with advanced countries. To be specific, China's manufacturing sector has the following problems: 1. The manufacturing sector covers a wide range of fields but fails to provide high-quality products, because of weak independent innovation capabilities and less perfect enterprise-oriented manufacturing innovation systems, both leading to a high dependence on key core technologies and high-end equipment from abroad; the quality of homegrown products needs to be improved and few well-known brands originate from China; the resource and energy utilization efficiency is relatively low and environmental pollution is serious; the industrial structure is improper and the high-end equipment manufacturing industry and producer service are lagging behind; informatization is at a low level and not deeply integrated with industrialization; China's industrial enterprises remain at a low level of internationalization and their international operation capacity is relatively weak.

1.1.5 Ubiquitous Industrial Facilities

Ubiquitous technology, also known as ubiquitous network technology, refers to widespread networks. Being omnipresent, all-inclusive, and omnipotent, this technology is intended to help anyone and anything smoothly communicate with each other anytime, anywhere. Industrial facilities can be ubiquitous upon application of the ubiquitous technology to ICSs, to take the development of ICSs to a higher level. Traditional ICSs largely refer to production control systems and process control systems deployed in factories. With the development of Internet technologies and information technologies, ICSs are not just used in factories, but have been widely applied in various fields such as streetlamp control and maintenance, intelligent building, and Internet of vehicles (IoV).

The streetlamp system is characterized by dense and broad distribution of nodes. Specifically, streetlamp facilities are usually obsolete, with numerous lamps and lanterns of various forms. It is too much of an expense to maintain such streetlamp facilities each year if the costs incurred by streetlamp control, routine inspection, lighting replacement and the labor and vehicle costs are counted. Using an intelligent controller, instead of traditional clock-control manual control systems, to automatically control when to turn on or turn off lights can lower the labor cost while effectively saving electrical power. Connecting the streetlamp system to the Internet to combine the Internet of Things (IoT) and the energy saving technology can reduce the expenses on routine inspection and maintenance of streetlamps. In this manner, streetlamp inspection and management are conducted by a computer system which automatically generates fault reports and alerts on-duty personnel to any faults. This greatly increases the streetlamp management efficiency and lowers the maintenance expenses, thus elevating streetlamp management to a new level and contributing positively to the country's low-carbon economy management and energy conservation and emission reduction.

Intelligent building is also a future trend. Like industrial production devices that are scheduled and managed in an increasingly intelligent manner, devices deployed in buildings, including the heating, ventilation and air conditioning (HVAC) system, lighting system, security and protection system, firefighting system, and smart grid system, should be scheduled and coordinated in an intelligent way. For example, the HVAC system and lighting system can be adapted to suit individual tastes, providing individualized life and production environments. The intelligent firefighting system are conducive to efficient personnel evacuation and fire control once there is a fire. The smart grid system can automatically adjust the proportion of clean energy in use in real time according to the building's power load and status of devices like photovoltaics, fans, and cogeneration, thus fulfilling the purpose of energy conservation and emission reduction. Meanwhile, intelligent buildings are a part of smart cities. In a smart city, buildings will exchange information such as energy consumption, new energy output, and availability of parking space. This kind of information interaction allows resources in buildings to be coordinated in an efficient way, achieving low-carbon environmental protection.

The above-mentioned intelligent streetlamp systems, intelligent buildings, and smart cities are all distributed systems which depend on cloud computing and edge computing technologies for their

running. Cloud computing technologies can streamline IT applications and business for enterprises and end users, but, when used by data centers, cannot properly cater for delay-sensitive applications which need to complete computation at nearby nodes to achieve the required minimal delay. To address this issue, edge computing emerges and expands the network computing paradigm characterized by cloud computing, and thus will be applied to more and more extensive service forms and types. Edge computing has the following characteristics: low delay and location awareness, wider geographical distribution, broader mobility, and suitability for scenarios with more nodes. Edge computing plays an important role in wireless access applications and is more useful for real-time applications and streaming media applications.

Edge computing provides a more complete solution for industrial Internet systems. As cloud computing technologies cannot address the timeliness requirement of the industrial Internet, the industrial Internet will generally adopt the edge computing technology to place certain computing tasks required by analysis and control at the network edge to meet the timeliness requirement of industrial systems. Meanwhile, distributed intelligent systems and autonomous systems at the edge will collaborate with each other, instead of reliance on centralized intelligence, to ensure the local survivability of the entire system and improve its stability.

Take IoV as an example. For IoV application and deployment, a rich variety of connection methods and interactions are required: vehicle to vehicle, vehicle to access point (AP, including wireless network connections, 3G/4G/5G, roadside units, and smart traffic lights), and AP to AP. Along with the development of artificial intelligence (AI), the automated driving era is coming. In the course of driving, self-driving vehicles need to perceive road conditions and keep abreast of the latest traffic flow situation before dynamically planning routes. To learn what is happening on the road ahead in real time, vehicles need to communicate with roadside infrastructure. When a self-driving car gets on a toll road, it needs to communicate with roadside infrastructure to pay the toll without stopping. IoV contributes to more secure and reliable self-driving, thanks to its very high timeliness. Edge computing technologies can provide, in more real time, information and data analysis capabilities and graphical distribution of roads (map of the entire city and roadside conditions) required by IoV. Arguably, edge computing lays a solid technical foundation for the future IoV.

In a word, traditional ICSs and their working principles have moved beyond factories to reach all walks of life. Also, cloud computing and edge computing technologies provide technical support for ubiquitous industrial facilities.

1.2 Development of ICS Information Security

As industrial informatization advances at a rapid pace and the industrial Internet, industrial clouds, and other new technologies spring up, information and network technologies and IoT technologies have found wide application in smart grid systems, intelligent transportation systems, and industrial production systems. For the sake of inter-system collaboration and information sharing, ICSs are breaking out of the traditional model of previous dedicated systems that run in a closed-off manner and begin to incorporate some standard and universal communication protocols and software and hardware systems. Some ICSs can even connect to the Internet in one way or another, thus breaking the protection barrier formed by the enclosed network, but exposing those systems to more threats. As ICSs are most commonly seen in a country's critical industries such as electricity, transportation, petrochemical, and nuclear sectors, cyberattacks targeting those systems will cause a more serious social impact and economic loss. Out of political, military, economic, and religious reasons, adversary organizations and countries and terrorist criminals can make industrial control systems their attack targets for malicious intents.

Information security incidents against ICSs, typically the Stuxnet virus, demonstrate that attackers are generally adopting a new attack means dubbed advanced persistent threat (APT). For APTs, attackers collaborate with each other to strike specific targets in an organized way. As China's ICSs and their operating environments are relatively enclosed, security research teams in this country, who are overly concerned about the Internet and traditional information systems, fail to accumulate a lot of research findings and practical experience in ICS protection. Besides, ICS providers focus too much on system functions and too little on security factors. In particular, as owners tend to fail to put forward explicit security requirements, security solutions, though available, are not proactively implemented for ICSs in China to protect them.

Many countries have realized the vulnerable security situation of ICSs and increasingly serious attack threats faced by them, and begin to promote ICS security to the national security strategy level and take proactive measures by introducing policies, standards, technologies, and solutions. While putting forward information security management requirements for ICSs in key realms, many governments are carrying out ICS security assurance work regarding policies and scientific research.

1.2.1 Difference Between ICSs and IT Information Systems in Information Security

With the rapid development of industrial informatization, ICSs have also employed up-to-date computer network technologies to promote inter-system integration, networking, and informatization management. This will allow IP-based communications to become basic communication means for ICSs, as demonstrated by the introduction of IT products such as PC servers and general-purpose operating systems and databases and the adoption of TCP/IP-based Ethernet ring networks and OPC communication protocols. To ensure the compatibility of ICSs, the application layer of the network will gradually use dedicated industrial control protocols. Applying Internet technologies will break the barriers between enterprises' production systems to implement centralized enterprise management and control and improve informatization, thus laying a solid foundation for efficient integration of production systems and management systems of enterprises. However, ICSs and traditional IT information systems are built for different purposes, and therefore they differ greatly in such aspects as technology, management, and service. Table 1.1 describes typical differences between the two types of systems.

Table 1.1 Differences between ICSs and traditional IT information systems

Item	ICS	Traditional IT Information System
Building Goal	Computer, Internet, micro-electronics, and electrical technologies are introduced to ICSs to make factories' production and manufacturing process more automated, efficient, precise, as well as controllable and visualized. ICSs focus on the industrial automation process and intelligent control, monitoring, and management of related devices.	Computer and Internet technologies are used for data handling and information sharing.

Development of ICS Security

Item	ICS	Traditional IT Information System
Architecture	An ICS mainly consists of a Programmable Logic Controller (PLC), Remote Terminal Unit (RTU), and supervisory control and data acquisition (SCADA) system.	Computer systems which communicate with each other through Internet protocols, constitute a computer network.
Operating System	Embedded operating systems such as VxWorks, uCLinux, and WinCE are widely used, with functions tailorable or customizable as required.	General-purpose operating systems (Windows, UNIX, and Linux) are used, especially Windows series systems which have powerful functions.
Data Exchange Protocol	Proprietary communication protocols (including OPC, Modbus, and DNP3) are used directly or at the application layer of TCP/IP.	TCP/IP protocol stack (application-layer protocols: HTTP, FTP, and SMTP).
Data Confidentiality	Except in some special industries, confidentiality of control data is not so important.	High data confidentiality is required.
Storage Space	Not too much system storage space is available and only several functions are provided.	Large storage space is available and more complicated functions are implemented.
System Timeliness	A high real-time capability is required for system transmission and information handling, and therefore downtime and restart for restoration are not allowed.	There is a moderate real-time requirement for information transmission and a tolerable transmission delay is accepted. Downtime and restart for restoration are allowed.
System Failure Response	Unexpected interruptions may incur an economic loss or disaster, and therefore emergency response must be made to handle system failures.	Unexpected interruptions may incur a task loss. The level of the response for system failures is determined according to requirements of IT systems.
System Upgrade Difficulty	These dedicated systems have poor capability and it is relatively difficult to upgrade the software and hardware. Therefore, if system upgrade, which is seldom performed, is required, the entire system needs to be upgraded.	Generic systems, which are highly compatible, are used. Software and hardware can be upgraded easily, with the software system upgraded more frequently.
Connection to Other Systems	Generally, such systems need to be physically isolated from the Internet.	These systems need to connect to the Internet.

In the traditional information security realm, confidentiality, integrity, and availability, which are collectively referred to as CIA, are regarded as three basic security attributes. In most cases, confidentiality matters the most. However, this is not the case in the ICS domain which highlights the degree of industrial automation and intelligent control, monitoring, and management capabilities of related devices. ICSs are quite different from common IT information systems in terms of system architecture, device's operating system, and data exchange protocols and are focused more on system's real-time capability and business continuity. Therefore, it is essential to ensure the availability and integrity of the equipment on which ICSs are installed. The data transmitted in ICSs is typically control commands and collected raw data, which are mostly real-time data and need to be analyzed together

with the context. Therefore, we have the lowest requirement for confidentiality of such data.

ICSs, as core production and operations systems of industrial enterprises, usually operate in an environment where a strict management mechanism is established. Except ICS suppliers, other external personnel are not admitted to ICSs' physical operating environment. Meanwhile, measures are typically in place to isolate ICSs from office networks (ordinary IT systems) of enterprises. Also, ICSs are physically isolated from the Internet. Obviously, ICSs' operating environment is relatively enclosed. ICSs are mainly composed of a wide variety of industrial control devices and systems, like PLC, RTU, DCS, and SCADA, which function on embedded operating systems (VxWorks, uCLinux, and WinCE) that are different from general-purpose Internet operating systems and communicate with each other through proprietary communication protocols or standards (including OPC, Modbus, and DNP3).

These proprietary industrial control systems and devices and communication protocols as well as relatively enclosed environments make it hard for Internet hackers or hacker organizations to obtain useful data concerning ICS defense research environments and related systems. This is why hackers' defense research is mostly limited to Internet-facing systems or ordinary IT information systems, but seldom on ICSs. Therefore, security defects (or vulnerabilities) are rarely discovered in ICSs and related communication protocols. In addition, ICS providers fail to give sufficient considerations to security issues and protective measures or inform security in O&M policies, while putting too much energy on system availability and timeliness.

Since 2000, there have been numerous ICS operations problems resulting from information security issues. Security incidents represented by Stuxnet uncovered in 2010 and a series of subsequent ICS incidents all suggest that ICSs are no longer immune from security risks but faced with increasingly serious threats which lead to even more adverse impact.

In view of above, ICSs and traditional IT information systems are immensely disparate in security threats, security issues, and security protections. Table 1.2 analyzes those differences.

Table 1.2 Comparison between ICSs and traditional IT systems in the security regard

Item		ICS	Traditional IT Information System
Security Threat	Threat source	• Mainly from organizations	• Individuals • Communities • Organizations
	Attack method	• Advanced persistent threats (including Stuxnet and Duqu) with an explicit purpose. • Collaborative attacks in an organized way	• Common attack means: denial of service, virus, malicious code, unauthorized use, compromise of three security attributes (CIA), and impersonation and spoofing. • In recent years, some organizations use APTs to target some important information systems.
Security Protection	System security	• Attention should be fixed on vulnerabilities and configuration defects in ICSs and proprietary operating systems used by industrial control devices. • Currently, system protection capabilities are insufficient: It is a difficult job to manage system patches and upgrade security mechanisms.	• More energy should be put into vulnerabilities, security configuration, and virus protection of general-purpose operating systems as well as unauthorized access to system resources. • Strong system protection capabilities (antivirus, patch management, configuration verification, peripheral equipment management and control, and other system-level security means).
	Network security	• Special attention should be paid to the security and timeliness of proprietary communication protocols and secure transmission capabilities. • There is a good range of proprietary protocols and specifications, but no uniform data communication protocols and standards for ICSs. • Proprietary communication protocols and standards are designed in such a way as to only emphasize communication timeliness and availability, but disregard security, as demonstrated by the lack of sufficient authentication, encryption, and authorization. • Physical isolation from the Internet is usually required.	• Significant efforts should be put into secure transmission, denial-of-service protection, and application-layer security of the TCP/IP protocol suite. There are only moderate timeliness requirements for data transmission. • Relatively mature security technologies, products, and solutions can provide excellent security protection capabilities. • Physical isolation with the Internet is usually not required.
	Data security	• More stress should be put on the security of ICS device status and control information during transmission, processing, and storage.	• Security and authorized use of data stored in servers.

Item		ICS	Traditional IT Information System
Security Management	Identity management	• Authentication and authorization management for system users are relatively simple. • Certain control devices are authenticated in hardware form, so it is difficult to change passwords on a regular basis.	• A sound authentication and authorization mechanism are used for IT users. • The user identity management system usually comes in software form, so it is convenient to change passwords on a regular basis.
	Patch management	• It is troublesome to manage ICS patches and fix vulnerabilities. • ICS administrators never are reluctant to install patches released by other vendors than ICS device manufacturers, considering the following factors: ICSs tend to have poor patch compatibility; the patch release cycle is long; the system availability and business continuity must be ensured. • Outdated systems may contain vulnerabilities that cannot be fixed because the vendor is no longer in business nor provides upgrade support for such systems.	• Traditional IT information systems have well-established vulnerability and patch management systems or tools which can address vulnerabilities in time.
	Behavior management	• Maloperation on or sabotage against ICSs should be prevented. • Typically, ICSs operate without security log audit and configuration change management mechanisms.	• Sound IT systems and network behavior audit mechanisms are available.
	Emergency response	• Emergency response plans should be developed to highlight rapid responses, serving as a guarantee of the business continuity of ICSs.	• Emergency response plans are established according to actual requirements.

1.2.2 Development of Industrial Control Information Security in China

Currently, as industrialization and informatization are well converged and IoT expands rapidly in China, ICSs are exposed to ever-increasing security risks. Meanwhile, as external threats evolve, security issues in ICSs have posed an even greater impact on business systems. Therefore, a great challenge for the ICS information security realm is to build a sound ICS information security assurance system to reduce insider and outside threats facing ICSs to provide security for thorough convergence between informatization and Industrialization and industrial transformation and upgrading.

Currently, China's ICSs face a grim security situation. Investigations reveal that about 80% of enterprises never upgrade ICSs or fix vulnerabilities in them, even though 52% of ICSs are connected to enterprises' management systems, intranets, and even the Internet. Besides, some vulnerable overseas industrial control products are still used on certain devices in China. What's more, China lacks technical means to

identify risk sources because too much research is focused on essential risk control technologies and methods for ICSs.

After the Stuxnet incident, various sectors in China have attached great importance to ICS security and established a set of standards and legal regulations.

- National Information Security Standardization Technical Committee (TC260) has developed the *Guide to Industrial Control Systems (ICS) Security: Supervisory Control and Data Acquisition (SCADA) Systems*.
- The Ministry of Industry and Information Technology (MIIT) released the *Circular on Strengthening Management of Information Security of Industrial Control Systems* (MIIT [2011] No. 451) in 2011 to put forward requirements for strengthening security management of ICSs of industrial enterprises in terms of connection management, networking management, configuration management, device selection and upgrade management, data management and emergency management.
- The State Council released the *Several Opinions on Promoting the Development of Information Technology and Ensuring the Security of Information* (SC [2012] No. 23) in 2012 to set out requirements for ICS security assurance. According to this document, China should strengthen security protection and management for ICSs deployed on nuclear facilities, oil and gas pipeline facilities, electric power systems, and urban facilities, as well as in the aerospace, advanced manufacturing, and petroleum and petrochemical sectors and other critical sectors, IoT applications, and digital city development by regularly conducting security checks and risk assessment; enhance the supervision of ICSs that are likely to endanger lives and security of public property; carry out security assessment for mission-critical products in key areas and establish a notification system for security risks and vulnerabilities.
- To implement the *Guidelines of the State Council on Deepening the Integrated Development of the Manufacturing Industry* and the Internet (SC [2016] No. 28) to ensure information security of ICSs of industrial enterprises, MIIT issued the Guide to Industrial Control Systems Security in 2016, putting forward guidelines on ICS security protection, covering security software selection and management, configuration and patch management, border security protection, physical

and environment security protection, identity authentication, remote access security, security monitoring and emergency plan drill, asset security, data security, supply chain management, and accountability.

As for ICS security product distribution, China has diverted its attention away from security gateways aimed at border protection to products providing security assurance throughout the lifecycle of ICSs. Currently, mainstream ICS security products can be classified as detection products, protection products, and monitoring and alerting products. In addition, some technologies like those concerning big data and perception used in traditional information systems begin to be adopted in ICS security products. Through analysis of technical characteristics of ICS products, we can see that China's enterprises with information security backgrounds provide ICS security products that inherit characteristics of configurations and applications of traditional information security products, but fail to consider usage habits in actual industrial fields, making them less easy to use on fields. However, ICS security products from enterprises with industrial backgrounds have a clear advantage in product forms and ease of use but provide less appropriate attack protection rule configurations as such enterprises lack an overall apprehension of basic functions for information security.

From above, we conclude that industrial information security technologies, only when taking into account both actual business characteristics and technical features of information security, can ensure business continuity and fit well into industrial environments. This way, such technologies can truly address security assurance requirements of ICSs and products and services relying on these technologies can really move onto the right track.

As for policies and regulations, China has developed a series of statutes and standards to direct and supervise ICS information security.

Policies and regulations

- Cybersecurity Law of the People's Republic of China
- Circular on Strengthening Management of Information Safety of Industrial Control Systems (MIIT [2010] No. 451)

- Guide to Industrial Control Systems (ICS) Security (MIIT ISS [2016] No. 451)
- Guidelines on the Emergency Management of Information Security Incidents (MIIT ISS [2017] No. 122)
- Administrative Measures for the Evaluation of ICS Protection Capabilities (MIIT ISS [2016] No. 451)
- Provisions on the Security Protection of the Electric Power Monitoring Systems (NDRC No. 14 Decree)
- Overall Plan of Security Protection for the Electric Power Monitoring Systems (NEA [2015] No. 36)

National Standards

1. **National Information Security Standardization Technical Committee (TC 260) has issued and plans to develop the following standards:**
    - Information Security Technology–Guide to Supervisory Control and Data Acquisition (SCADA) Systems Security Control
    - Information Security Technology–Security Indicator System of Security-Controllable Information Systems (Electric Power System)
    - Information Security Technology—Security Management Fundamental Requirements for Industrial Control Systems
    - Information Security Technology—Guide to Security Inspection of Industrial Control Systems
    - Information Security Technology—Industrial Control System Terminal Security Requirements
    - Information Security Technology—Industrial Control System Security Protection Technology Requirements and Assessment Methods
    - Information Security Technology—Information Security Classification Specifications of Industrial Control Systems
2. **Power Systems Management and Associated Information Exchange (SAC/TC 82) has established the following standards:**

- GB/Z 25320.1-2010 Power Systems Management and Associated Information Exchange—Data and Communications Security—Part 1: Communication Network and System Security Issues—Introduction to Security Issues (issued on November 10, 2010, effective from May 1, 2011)
- GB/Z 25320.2-2013 Power Systems Management and Associated Information Exchange—Data and Communications Security—Part 2: Glossary (issued on February 7, 2013, effective from July 1, 2013)
- GB/Z 25320.3-2010 Power Systems Management and Associated Information Exchange—Data and Communications Security—Part 3: Communication Network and System Security—Profile Including TCP/IP (issued on November 10, 2013, effective from May 1, 2013)
- GB/Z 25320.4-2010 Power Systems Management and Associated Information Exchange—Data and Communications Security—Part 4: Profiles including MMS (issued on November 10, 2010, effective from May 1, 2011)
- GB/Z 25320.5-2013 Power Systems Management and Associated Information Exchange—Data and Communications Security—Part 5: Security for GB/T 18657 and Derivatives (issued on February 7, 2013, effective from July 1, 2013)
- GB/Z 25320.6-2011 Power Systems Management and Associated Information Exchange—Data and Communications Security—Part 6: Security for IEC 61850 (issued on December 30, 2011, effective from May 1, 2012)
- GB/Z 25320.7-2015 Power Systems Management and Associated Information Exchange—Data and Communications Security—Part 7: Network and System Management (NSM) Data Object Models (issued on May 15, 2015, effective from December 1, 2015)

3. **National Technical Committee 124 on Industrial Process Measurement and Control of Standardization Administration of China (SAC/TC 124) has issued and plans to develop the following standards:**

- GB/T 26333-2010 Evaluation Specification for Security in Industrial Control Network (issued on January 14, 2011, effective from June 1, 2011)

- GB/T 30976.1-2014 Industrial Control System Information Security—Part 1: Assessment Specification (issued on July 24, 2014, effective from February 1, 2015)
- GB/T 30976.2-2014 Industrial Control System Information Security—Part 2: Acceptance Specification (issued on July 24, 2014, effective from February 1, 2015)
- Industrial Control Computer System—General Specification—Part 2: Security Requirements for Industrial Control Computer (under compilation)

4. **Ministry of Industry and Information Technology has issued the following standards:**
   - JB/T 11961-2014 Industrial Communication Networks—Network and System Security—Terminology, Concepts, and Models (issued on May 6, 2014, effective from October 1, 2014)
   - JB/T 11962-2014 Industrial Communication Networks—Network and System Security—Security for Industrial Automation and Control Systems (issued on May 6, 2014, effective from October 1, 2014)

Industry Standards

1. **National Technical Committee for Standardization of Electric Power Supervision (TC 296) has been developing the following standards:**
   - Electric Power Secondary System Security Protection Regulation (Mandatory)
   - Electric Power Information System Security Inspection Standard (Mandatory)
   - Information Security Level Evaluation Indicators for Electric Power Industry (Recommended)
2. **China Electricity Council has developed the following standards:**
   - GB/T 31991.1-2015 Technical Specification of Electric Energy Service Management Platform—Part 1: General Rules (issued on September 11, 2015, effective from April 1, 2016)
   - GB/T 31991.2-2015 Technical Specification of Electric Energy Service Management Platform—Part 2: Function Specification (issued on September 11, 2015, effective from April 1, 2016)
   - GB/T 31991.3-2015 Technical Specification of Electric Energy Service Management Platform—

Part 3: Interface Specification (issued on September 11, 2015, effective from April 1, 2016)

- GB/T 31991.4-2015 Technical Specification of Electric Energy Service Management Platform—Part 4: Design Specification (issued on September 11, 2015, effective from April 1, 2016)
- GB/T 31991.5-2015 Technical Specification of Electric Energy Service Management Platform—Part 5: Safety Protection Specification (issued on September 11, 2015, effective from April 1, 2016)
- GB/T 31960.1-2015 Technical Specification of Power Energy Efficiency Monitoring System—Part 1: General Rules (issued on September 11, 2015, effective from April 1, 2016)
- GB/T 31960.2-2015 Technical Specification of Power Energy Efficiency Monitoring System—Part 2: Function Specification of Master Station (issued on September 11, 2015, effective from April 1, 2016)
- GB/T 31960.3-2015 Technical Specification of Power Energy Efficiency Monitoring System—Part 3: Communication Protocol (issued on September 11, 2015, effective from April 1, 2016)
- GB/T 31960.4-2015 Technical Specification of Power Energy Efficiency Monitoring System—Part 4: Function Design Specification of Substation (issued on September 11, 2015, effective from April 1, 2016)
- GB/T 31960.5-2015 Technical Specification of Power Energy Efficiency Monitoring System—Part 5: Design Guidelines of Master Station (issued on September 11, 2015, effective from April 1, 2016)
- GB/T 31960.6-2015 Technical Specification of Power Energy Efficiency Monitoring System—Part 6: Technical Condition of Power Energy Efficiency Information Concentrate and Exchange Terminal (issued on September 11, 2015, effective from April 1, 2016)
- GB/T 31960.6-2015 Technical Specification of Power Energy Efficiency Monitoring System—Part 7: Technical Condition for Power Energy Efficiency Monitoring Terminal (issued on September 11, 2015, effective from April 1, 2016)

- GB/T 31960.8-2015 Technical Specification of Power Energy Efficiency Monitoring System—Part 8: Specification of Security Protection (issued on September 11, 2015, effective from April 1, 2016)

3. **State Tobacco Monopoly Administration has developed the following standards:**

   - State Tobacco Monopoly Administration Office's Notice About Forwarding the *2016 Work Plan of Law Enforcement on Cybersecurity Inspection* Issued by the Ministry of Public Security (STMAO [2016] No. 257)
   - Security Specification for Interconnection Between Production Network and Management Network of Tobacco Industry Enterprise (YC/T 494-2014)
   - Circular of the State *Tobacco Monopoly Administration on Issuing the Tobacco Industry Informatization Development Plan (2014—2020)* (STMAO [2014] No. 370)
   - Implementation Specifications for Classified Protection of Information System of Tobacco Industry (YC/T 495-2014)
   - Technical Specification on Network Security of Industrial Control Systems of Tobacco Industry (Revision Draft)

Industrial Alliances in China

On April 17, 2014, the Industrial Control Systems Information Security Industry Alliance (ICSISIA) was jointly launched by 24 organizations, including competent national authorities such as the Research Center of Information Security of China Electronics Standardization Institute, National Industrial Process Measurement, Control and Automation Standardization Technical Committee, Third Research Institute of the Ministry of Public Security, Electronic Technology Information Research Institute of MIIT, China Software Testing Center, and China Instruments Manufacturers Association, as well as ICS vendors, information security vendors, and industrial customers. This alliance is intended to be a platform for governments, users, enterprises, scientific research institutes, and universities and colleges to communicate on system building, classified protection, risk assessment, standards development, and product development and evaluation involved in the ICS information security industry of China. Playing

the role of bridge for these parties, this alliance aims to push forward the development of China's ICS information security industry and guarantee the secure and stable operating of critical infrastructure, thus providing effective support for sound and sustainable industrial development of China.

On June 8, 2017, National Industry Security Industry Alliance was set up.

Under guidance of MIIT, this alliance aims to accomplish the following tasks and missions: 1. Through full cooperation, this alliance will be built into a platform for collaboration between governments and the industrial information security industry; 2. For convergent development, this alliance will become a platform that integrates automation, informatization, and information security; 3. This alliance will develop into a platform for industrial resource integration, exchange, and promotion. MIIT will, together with other related departments, provide guidance and support for technical research, standardization, pilot demonstration, public service platform development, and international exchange of the alliance, forming a development pattern featuring efficient collaboration between governments, the industry, colleges and universities, scientific research institutes, and customers. Currently, 149 organizations have become the alliance's first batch of members, including 18 vice-chairman units such as Shenhua Group, China Railway Rolling Stock Corporation, Aviation Industry Corporation of China, China South Industries Group Corporation, and China Electronics Corporation, as well as 45 council member units like China National Nuclear Corporation, China Shipbuilding Industry Corporation, Sinopec Group, Sinosteel Group Corporation, and China National Tobacco Corporation.

ICS Security Status Quo of Various Sectors

In China, among all sectors, enterprises in the electric power area are the first to conduct ICS security development. Most large electric power enterprises have set up dedicated networks, defined security zones, and implemented horizontal separation and vertical cryptographic authentication, in alignment with the *China Electric Power Secondary System Security Protection Scheme*, No.5 Decree issued by the State Electricity Regulatory Commission. After 2014, as the National Development and Reform Commission (NDRC) issued No.14 order and the National Energy Administration issued the matching No.36 order, electric power enterprises, especially power generation enterprises, have implemented overall protection in addition to original security measures, thus enhancing security separation between

different areas and improving internal security protection of systems.

Enterprises in the tobacco sector have isolated the production network from the office network to better security of connections between both networks. In addition, pilot security programs have been implemented for the production system of China National Tobacco Corporation, as well as for logistics and sorting of commercial tobacco.

Among all industries, the petroleum and petrochemical industry takes the lead in carrying out ICS security construction in China. Currently, some major oil production plants, union stations, or workshops have isolated the control network from the MES network and some production units have carried out pilot programs for ICS security development of systems. In addition, as security issues keep popping up in control systems and pose an increasingly serious impact, the transportation, metallurgy, and critical manufacturing sectors are all stepping up efforts in improving ICS security to meet more and more regulatory requirements that are raised.

1.2.3 Development of ICS Information Security Outside of China

Since the Stuxnet virus explosion, countries all over the world have taken ICS security issues to a new height by actively working out and introducing related policies, standards, technologies, and solutions.

A look into ICS security developments around the world reveals that the USA is the first to research and implement ICS security standards. North America Electric Reliability Corporation has conducted security checks on electric power (including nuclear power) enterprises according to requirements defined in CIP series standards. Europe has inspected security of industrial control products in accordance with WIB standards. Some counties represented by Germany are diverting their efforts to ICS security in compliance with ISO 27009. Japan, in line with requirements of IEC 62443 and Achilles Certification, stipulated in 2013 that all ICS products can be applied in the country only after they are certified by national standards. Also, this country has conducted ICS security checks and construction in energy, chemical, and other critical sectors. Israel has set up a state-level ICS product security inspection center to perform security inspection on ICS products before they are connected to networks.

As a leader in information industry development, the USA has attached great importance to ICS security

since long ago, as demonstrated by the following: made national security a top national priority in 2003; took ICS products as critical infrastructure that should be put under special protection in 2008; issued the *Strategy for Securing Control Systems* in 2009, covering ICS security in 14 sectors such as energy, electric power, and transportation; set up the Industrial Control Systems Cyber Emergency Response Team under CERT (ICS-CERT) in 2009 to monitor ICS-related security incidents, analyze vulnerabilities and malicious code, and provide data support for incident response and forensics analysis. By launching information products, releasing security bulletins, and sharing vulnerability and threat information, ICS-CERT monitors for ICS security incidents, analyzes the ICS security posture, and releases security reports to the public on a quarterly basis. The U.S. Department of Homeland Security (DHS) has initiated the *Control System Security Program* (CSSP) to use ICSs to emulate a simulation platform to perform vulnerability analysis and verification for ICS products by conducting assessment both in the field and laboratory. The National Institute of Standards and Technology (NIST) and Department of Energy respectively issued the *Guide to Industrial Control Systems (ICS) Security* (SP800-82. The latest revision was released in 2013) and *21 Steps to Improve Cyber Security of SCADA Networks* and other documents concerning security development standards and best practices. Meanwhile, traditional information security vendors such as Symantec, McAfee and Cisco, traditional ICS vendors like Rockwell Automation and General Electric Company, as well as some emerging professional ICS security vendors have done intensive research, practice, and industrialization work regarding ICS security protection to provide excellent products and services, and have thus, by and large, secured a leadership position around the world.

However, ICS informatization, intelligence, and security issue resolving cannot be supported without support from ICS vendors. In Europe, ICS providers, represented by Siemens and Schneider Electric, provide security products, services, and solutions for customers. For instance, Siemens sets up an ICS security laboratory and provides ICS security advisory services, training, and products like ICS firewall. In the ICS realm, Siemens and Schneider Electric have absolute technology and market advantages, which enable them to dominate the ICS security realm for a long time in the future.

Among professional ICS security vendors, Tofino, a Canadian company, relies on its well-known ICS firewall to become a leading ICS security vendor to provide products that are widely applied in

various sectors including the petrochemical sector. With a fuzzing test tool for vulnerability discovery, Codenomicon has gained a leading position in the ICS security realm. Meanwhile, some open-source organizations also provide ICS security tools, including Nessus which is available in both professional (paid) and evaluation versions (free of charge). The professional version can use related ICS security plug-ins for detection and assessment of vulnerabilities in SCADA systems or PLC control devices.

As far as international standard research in ICS security is concerned, IEC/TC65/WG10 and the ISA 99 committee jointly developed IEC 62443 standards in 2007 which has been revised and renamed the *Industrial Process Measurement, Control, and Automation-Network and System Information Security* in 2011. This series of standards is divided into four parts which involve 12 documents in total:

- IEC 62443-1-1 Terminology, Concepts and Models
- IEC 62443-1-2 Master Glossary of Terms and Abbreviations
- IEC 62443-1-3 System Security Compliance Metrics
- IEC 62443-2-1 Establishing an Industrial Automation and Control Systems Security Program
- IEC 62443-2-2 Operating an Industrial Automation and Control Systems Security Program
- IEC 62443-2-3 Patch Management in the IACS Environment
- IEC 62443-2-4 Certification of IACS Supplier Security Policies and Practices
- IEC 62443-3-1 Security Technologies for IACS
- IEC 62443-3-2 Security Assurance Levels for Zones and Conduits
- IEC 62443-3-3 System Security Requirements and Security Levels
- IEC 62443-4-1 Product Development Requirements
- IEC 62443-4-2 Technical Security Requirements for IACS Components

To avoid conflicts, IEC 62443 standards have also integrated the WIB standard developed by an oil and gas organization from the Netherlands and the NERC-CIP standard enacted by National Electric Reliability Council (NERC). Research based on IEC 62443 standards is exemplified as follows:

1. In 2010, the USA initiated the ISA 99 industrial infrastructure certification program by setting up a laboratory in Nevada to do research in ICS vulnerability discovery, detection, and verification.
2. In 2013, Japan conducted security verification for ICSs based on IEC 62443 standards before such systems went live.
3. In 2015, IEC built a network security assessment system for ICS manufacturers, suppliers/system integrators, and operators/asset owners, as per IEC 62443 standards. This system provides network security verification for products, processes, and personnel, verifying that they conform to security requirements defined in IEC 62443 standards in a bid to provide security guarantee for asset owners.

1.3 Technical Trend of ICS Information Security

1.3.1 General Introduction

As the application of IT technologies in industrial fields is expanding in breadth and depth, ICSs are facing an increasing number of security risks. ICSs' original security protection systems which feature border separation and protection tend to be associated and integrated with business. With the emergence of new application forms such as industrial clouds and industrial big data, ICS security products need to surpass the existing products in terms of functions and application form, so as to better adapt to new applications.

1.3.2 Introduction to Major ICS Information Security Products

Currently, ICSs adopt the following categories of information security technologies: protection, isolation, monitoring, detection, and O&M management.

- **Protection**
  - Network protection: Unlike traditional IT firewalls, industrial firewalls make an in-depth analysis (from the IP layer to the application layer) of packets reaching industrial networks, using the whitelist mechanism to restrict access to resources such as IP addresses and protocol

function code, as well as restrict operation behavior.

- Host protection: A host whitelist mechanism or a trusted system for host application software is built to check whether related software or applications can run in the current system and prevent the execution of the software/applications outside of the whitelist and launch of the related processes.

- **Isolation**
  - GAP: In a 2+1 or 3+1 manner, two hosts communicate with each other through a Network Security Separated Card. Alternatively, another host is used to dispatch policies to both hosts to implement limited communication between them. Currently, GAPs are extensively used in the petroleum and petrochemical and metallurgy sectors.
  - Forward and reverse isolation devices: Internal and external hosts communicate with each other via a single-byte response mechanism as no TCP/IP connections are set up between the intranet and extranet. Such devices still need to perform verification based on digital certificates, and therefore limited communication needs to be established between the intranet and extranet. Currently, this kind of devices is widely used in the electric power sector.
  - Industrial isolation gateway: Currently, this kind of product adopts the 2+1 isolation method or alternatively two firewalls are directly interconnected to effectively filter and handle packets using OPC (OLE for Process Control), Modbus, and S9 protocols. This system is especially useful for fine-grained control of such operations as reading and modifying OPC's point tables.

- **Monitoring**
  - Industrial control audit: With a communication behavior baseline built through customization or automatic learning, this kind of product can identify abnormal communication behavior, alert for operations involving such behavior, and provide relevant handling suggestions.
  - IDS for ICSs: Through in-depth packet parsing, such products can perform signature analysis and anomaly detection to identify attack behavior of malware that gets into or hides in ICSs, in a bid to effectively perceive and spot attack behavior.

- Industrial monitoring and alerting platform: Through management and correlative analysis of security logs, network logs, and host logs, this kind of platform identifies and reproduces potential malicious behavior in industrial fields, by taking account of characteristics of industrial field operations.

- **Detection**
  - Scanning for Industrial control vulnerabilities: This kind of product probes IT operating systems, databases, application software, and devices (such as industrial controllers like PLC and DCS) which are commonly seen on industrial fields, in order to identify security vulnerabilities in them.
  - Discovery of industrial control vulnerabilities: This kind of product tests the protocol robustness via technical means like fuzz testing. By sending a malformed packet of a designated protocol to a device under detection, such a product checks whether this device can properly handle such packet, as demonstrated by discovery of vulnerabilities in systems through a denial of service (DoS).
- **O&M Management**
  - Industrial jump server: implementing security audit and identity management of the O&M process. Currently, if industrial software cannot be installed on the master device in industrial fields, an interface for connection to software like SCADA is integrated and configured to implement communication with the master device and monitor the O&M process.
  - Mobile industrial O&M auditing: This kind of product monitors operations of external onsite O&M personnel to spot potential malicious behaviors mingled with O&M operations, as well as record and block such behavior.

1.3.3 Issues and Difficulties Facing ICS Information Security Technologies

Currently, ICS information security enters a new epoch of converging information security and ICS security. ICS security products are still in the age of version 1.0 and lag far behind IT information security and IT systems in terms of adaptation, even though ICS security products are strongly associated with business application. Besides, due to inadequate integration with business and the lack

of innovative security detection ideas, ICS security products fail to perform adequate in-depth detection of attack behavior potentially existing in business, and thus cannot deliver security protection that truly works.

On the other hand, with the popularization of new applications (including industrial clouds and industrial big data) in industrial sectors, there are bound to be changes to industrial control forms. Information security technologies, when adapted to these new forms, definitely need to be integrated with business. However, integration of ICS information security technologies does not fully unfold until a breakthrough is made in the technological direction and applications.

2

ICS Information Security Landscape

2.1 Typical ICS Security Incidents

As ICSs are increasingly informatized and open, more and more attacks are hitting ICSs, doing an increasing harm. ICS-targeted attacks use the IT network as a springboard to affect the operating of OT systems. Currently, attacks against ICSs are carried out to achieve three purposes: disrupting the normal operating of ICSs, obtaining ICS data, and making financial gains.

The Stuxnet virus incident and Ukrainian power grid incident are typical attack cases to disrupt the normal operating of ICSs.

The Stuxnet virus is seen as the earliest attack against ICSs. During this attack, the hacker used the Stuxnet virus to target uranium enrichment devices in Iran, including the master devices and physical systems (i.e., centrifuges) so as to shorten the service life of the devices, slow down the uranium enrichment process, and finally wreck Iran's nuclear plan. The hacker expected to finally reach the SIMATIC WinCC system which is provided by Siemens and deployed in the dedicated internal LAN (local area network) for ICS data collection and monitoring. In the early phase, for penetration into the internal network, the hacker first infected an external host through social engineering, then infected a USB flash disk drive, and finally exploited a shortcut file parsing vulnerability to spread the virus to the internal network. Within the intranet, the virus exploited three different vulnerabilities to spread between networked hosts to finally reach the host installed with the SIMATIC WinCC software. Then the attack kicked off, which took advantage of three 0-day vulnerabilities and used many attack techniques and methods that are almost impossible to be implemented in common attacks.

Ukraine's power grid was hit many times in a year or so, causing power outages. These attacks used two types of malware, namely the BlackEnergy trojan and KillDisk, to compromise files, rendering the system unable to run plug-ins. Directly interacting with the system, the attacker sent power cut-off commands and used KillDisk to make power restoration more difficult. Likewise, the Industroyer malware uses industrial communication protocols used worldwide to control the energy switches and circuit breakers of substations all over the country, aimed at compromising the normal operating of ICSs. Arguably, attacks against ICSs no longer merely focus on general-purpose parts like PLC and OPC, but have turned to special-purpose parts (such as substation systems) as their targets.

Attacks aimed at obtain ICS data are mainly initiated to steal the production process, so as to spy on enterprises' or countries' industrial behavioral patterns. VPNFilter, a type of multi-stage modular malware which has infected at least 500,000 networked devices around the world, is a typical example of such attacks. Among malicious components added for extension in the third stage of this malware, some are used specially to sniff industrial control protocols, collecting intelligence based on the Modbus SCADA protocol as well as sniffing HTTP-based login credentials and authorization information.

The malware HAVEX infects the SCADA system and OPC among ICSs to steal information and data within the system, including the operating system, computer name, user information, files, and directory list of the infected host, before uploading such information to the remote command and control (C&C) server for the purpose of spying on enterprises' or countries' industrial behavioral patterns.

Attacks motivated by financial gains are a new type of attacks emerging in recent years. These attacks usually resort to ransomware such as WannaCry and ClearEnergy.

On November 28, 2016, San Francisco MUNI's rapid transit system was hit by ransomware. As a result, all ticketing machines displayed the following message: "You Hacked, ALL Data Encrypted." The attacker asked for 100 bitcoins which is equivalent to 70,000 dollars according to the exchange rate then.

On May 13, 2017, Renault announce to suspend production at factories in Sandouville in France and Romania to prevent the propagation of this ransomware in the system. Besides, NISSAN's manufacturing plant in Sunderland in the UK was also affected.

In March 2018, Atlanta suffered a ransomware attack which left its urban services paralyzed for several days. In response to this attack, Atlanta spent nearly 5 million, dollars to access emergency IT services which cover incident response services, crisis public relations, support personnel addition, and expert consulting services around certain topics.

On August 3, 2018, TSMC's 12-inch wafer factory and operational headquarters in Hsinchu Science Park encountered an attack launched by a variant of the ransomware WannaCry which suspended the assembly line, incurring an economic loss of 170 million dollars. This incident in the separated network of the assembly line was the result of misoperation. As machines scan for viruses only after going live, new machines that were unpatched were infected with this virus and finally all machines got infected.

As targeted machines were not networked, they did not pop up a ransomware window after being infected, but stopped running. This incident, though occurring within ICSs, was caused by an ordinary virus in essence, which demonstrates that even an ordinary virus can lead to a production incident.

From all above, we can see that ransomware is setting its sights on ICSs. Some incidents, though not causing production incidents or personal accident, may result in a data restoration cost that is far higher than the ransom asked by the attacker, incurring a great loss and impact to enterprises and the society.

Ransomware viruses and traditional ICS-targeting viruses (like Stuxnet) can all lead to ICSs being unable to operate properly. However, a big difference lies between the two types of viruses. Firstly, ransomware viruses are intended to target ordinary IT systems, while ICS-targeting viruses aim to hit industrial control devices, with explicit attack targets and expected results. Secondly, currently, ransomware viruses are designed to infect general-purpose operating systems like Windows, and therefore they usually run on a human-machine interface of an ICS. Traditional ICS-targeting viruses, however, used to strike specific ICS devices such as PLC and DCS. Lastly, the former viruses are crafted to gain economic benefits, while the latter ones are mainly used to compromise the integrity of ICSs, making them unable to run properly. With the development of ICSs, some research indicates that ransomware viruses targeting industrial control devices like PLC can make a profit while rendering ICSs unable to operate properly.

Besides ransomware, attacks in other forms have occurred to reap illegal profits. For example, a user's illegal unlocks of heavy machinery of SANY Heavy Industry Cooperation Limited led to a sales loss to this company.

All in all, with IT and OT are converging at a rapid pace, ICSs will be exposed to more and more threats.

2.2 ICS-Targeting Malware Analysis

In recent years, more and more malware took ICSs as targets, causing an increasingly great damage. The following sections analyze major ICS-targeting malware.

2.2.1 Electric Energy Malware Industroyer

- **Overview of the Industroyer incident:**

  On June 8, 2017, the security company ESET discovered the ICS-targeting malware Win32/Industroyer. Dragos verified analysis results of ESET and released the hash information and analysis report of Win32/Industroyer on June 12. Those behind Industroyer have a deep knowledge and understanding of ICSs, especially industrial control protocols used in electric power systems. Support for four different industrial control protocols, specified in the standards listed below, has been implemented by the malware authors:

  - IEC 60870-5-101 (aka IEC 101)
  - IEC 60870-5-104 (aka IEC 104)
  - IEC 61850
  - OLE for Process Control Data Access (OPC DA)

  Compared with the malware causing power outage in Ukraine in 2015, Industroyer has a more advanced functional structure and can cause the system to crash, making it deny service to legitimate users. Dragos's analysis and speculation show that Industroyer may be related to Ukraine's power outage incident that occurred in December 2016.

- **Industroyer's attack process is shown as follows:**

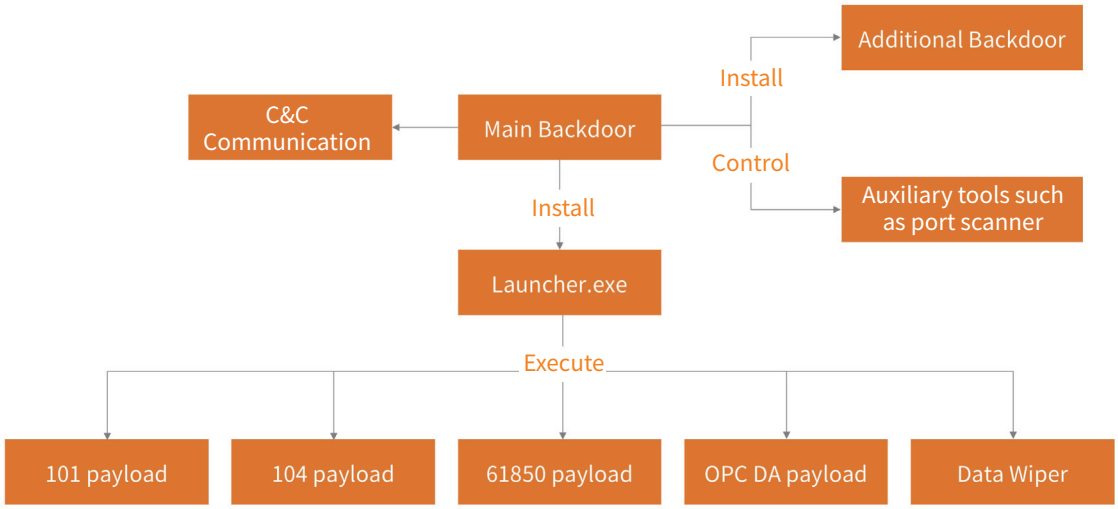


Figure 2.1 Attack process of Industroyer

Functional Modules

This malware consists of the following modules:

- Main Backdoor

  A main backdoor communicates with port 443 on the remote C&C server through port 3128 of the local agent, receiving commands from the server for local execution.

- Launcher

  The Launcher module is responsible for launching payloads. A new thread loads payload.dll, calls the export function called "Crash", and performs attacks against industrial control protocols. Another thread loads the data wiper module haslo.dat, calls the export function called "Crash", and performs the wipe operation.

- Data wiper component

  The data wiper provides the following functions:

  - Traverse registry keys in **SYSTEM\\CurrentControlSet\\Services** to change the value of ImagePath of all services to null. This operation will make system services unavailable and the

system unable to restart.

- Traverse all local and network disk drives assigned disk letters from C to Z. If a file with a related extension is found, create a new thread to overwrite all contents of this file to compromise it.
- Enumerate system processes and terminate related ones, which will cause the system to crash.

- Scanner

  As Industroyer has a port scanner built in, the -ip and -port parameters can be set to an IP address range and a port range for scanning.

- Additional tools: DoS tool

  The DoS tool exploits the vulnerability (CVE-2015-5374) to target a SIPROTEC device from Siemens by sending a crafted 18-byte UDP packet to port 50000. After the attack is completed, the device stops responding to legitimate instructions until the device is manually rebooted.

Sum-up

Win32/Industroyer is a type of malware designed to target ICSs. It supports four industrial control protocols: IEC101, IEC104, IEC61850, and OPC DA. The sample contains multiple modules, with the main backdoor responsible for installing and running other modules, communicating with the C&C server to receive C&C commands, and performing the next-step operation as instructed. Attacks against industrial control protocols are completed by different payloads, causing the ICS to crash and making it deny service to legitimate users.

2.2.2 Dragonfly 2.0 Malware

The Dragonfly organization, also known as Energetic Bear, mainly carries out cyber espionage activities targeting electric power operators, major power generation enterprises, petroleum pipeline operators, and industrial equipment providers in the energy sector. According to a Joint Analysis Report (JAR) released by the Department of Homeland Security (DHS), Dragonfly is a Russian APT

entity sponsored by the Russian government. The information publicly availably reveals that Dragonfly, a hacker organization with a wide range of attack capabilities, can access the target network with stolen credentials of victim hosts and also provide an extensive customized hacking toolset to launch attacks against the target network. From the viewpoint of the evolution from Dragonfly 1.0 to Dragonfly 2.0, this hacker organization is taking more and more countermeasures (such as HTTPS-encrypted communication, real-time download and execution of encrypted shellcode, pre-initialized code hijacking, and template injection) and beginning to use legitimate system management tools like PowerShell, PsExec, and Bitsadmin to launch attacks. To some extent, this makes it more difficult to discover threats. Though the hacker organization has never exploited 0-day vulnerabilities for attacks, it is an organization carrying out highly targeted attacks as it has been collecting intelligence from the energy sector for a long time. Looking at its attack cases, we can see that this organization is motivated by political reasons.

Symantec indicates that it has been tracking this organization from 2011 and has revealed the association between this organization and cyberattacks launched against western enterprises in 2014. The following lists attacks initiated by this organization:

In 2011, it targeted the defense and aviation companies of the USA and Canada.

In a second phase in early 2013, Dragonfly focused its effort on US and European energy firms.

In 2014, it targeted organizations in the USA, Italy, France, Spain, Germany, Turkey, and Poland.

After the report went public in 2014, the Dragonfly group went dark and appeared again in December 2015 when it launched cyber-attacks on Turkish energy companies that were also targeted during 2016.

After being dormant for several years, this organization has become active again recently. Researchers find that Dragonfly has hit energy companies in the USA and Europe (Turkey and Switzerland), aimed at taking control of and even compromising energy facilities.

Like Dragonfly 1.0, Dragonfly 2.0 uses more than one attack method (malicious email, watering-hole attack, and legitimate software binding) to penetrate into the target and plant malicious code. For Dragonfly 1.0, activities were conducted for reconnaissance, while those by Dragonfly 2.0 are carried

out for destructive purposes. Here show what policies are adopted by the hacker.

The attacker employs widely available malware and "living off the land" tools such as administration tools like PowerShell, PsExec, and Bitsadmin.

Dragonfly 2.0 adopts all sorts of attack means, from spear phishing emails to watering-hole attacks.

In the first attacks spotted by Symantec in December 2015, hackers used spear phishing messages disguised as an invitation to a New Year’ s Eve party.

From 2016 to 2017, the attacker usually used spear phishing emails to target the energy sector.

Symantec found that phishing emails were crafted with the Phishery toolkit, attempting to steal victims' credentials through a template injection attack. Also, the attackers resorted to watering-hole attacks to target websites that were likely to be visited by personnel in the energy sector, so as to obtain network credentials. Symantec reported that in at least one case, the watering hole attack was used to deliver the Goodor backdoor via PowerShell 11 days later.

Here, we only give a general introduction to this malware and its organization. For more details about this malware, please see related analysis reports.

2.2.3 New ICS Attack Framework "TRITON"

In the middle of November 2017, the Dragos, Inc. team found malware tailor-made for ICSs and identified it as TRISIS (referred to as TRITON in this document) because it fixed it gaze on Schneider Electric's Triconex safety instrumented system (SIS), enabling the replacement of logic in final control elements.

TRITON is highly targeted and likely does not pose an immediate threat to other Schneider Electric customers, let alone other SIS products. Importantly, the malware leverages no inherent vulnerability in products from Schneider Electric. However, this capability, methodology, and tradecraft in this very specific event may now be replicated by other adversaries and thus represents an addition to threat models of industrial asset owners and operators.

The attacker first gained remote access to an SIS engineering workstation and deployed the TRITON

attack framework to reprogram the SIS controllers. During the incident, some SIS controllers entered a failed safe state, which automatically shut down the industrial process and prompted the asset owner to initiate an investigation. The investigation found that the SIS controllers initiated a safe shutdown when application code between redundant processing units failed a validation check, resulting in an MP diagnostic failure message. Also, TRITON was found in this investigation.

The attacker intended to cause a consequence of physical damage in the long run. Based on such a fact, the attacker initially gained a sound foothold on the DCS and already had the capability of manipulating the process or shutting down the factory. Upon intrusion into the DCS and SIS system, the attacker could do damage to physical devices to the maximum extent possible.

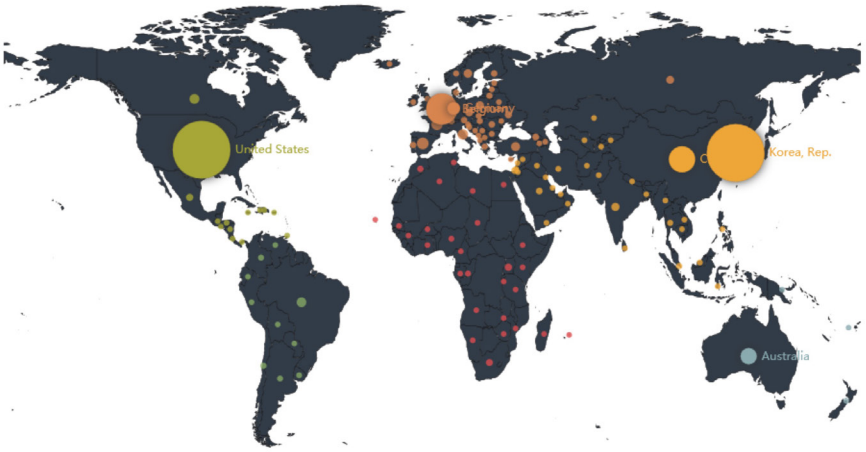
2.3 Vulnerabilities in ICS Assets

Most ICS security mechanisms are short of authentication, encryption, and audits, and therefore such ICS assets are rather vulnerable. When connecting to the Internet, ICSs are susceptible to external probes or identification via special fields included in information returned through public or private communication protocols, web services, telnet, and FTP. In this way, ICS assets can be easily controlled by attackers. In addition, more and more ICS vulnerabilities are identified by researchers, leaving ICS assets exposed on the Internet rather vulnerable.

2.3.1 More ICS Assets Exposed

To minimize the chance of industrial control devices being hit by cyberattacks, ICSs should run in a physically isolated environment. However, this is not the case in the actual production environment. In July 2016, Kaspersky released a report indicating that 188,019 ICS hosts in 170 countries around the world were found connected to the Internet. [1]

The following figures show the exposure of global assets on the Internet detected by NSFOCUS Threat Intelligence (NTI) using multiple protocols. The figures below take Modbus and the Siemens S7 protocol as an example to show the exposure and distribution of industrial control devices around the world (statistics are not collected for a particular year).



A total of 373,612 devices detected

Figure 2.2 Global distribution of industrial control devices using Modbus

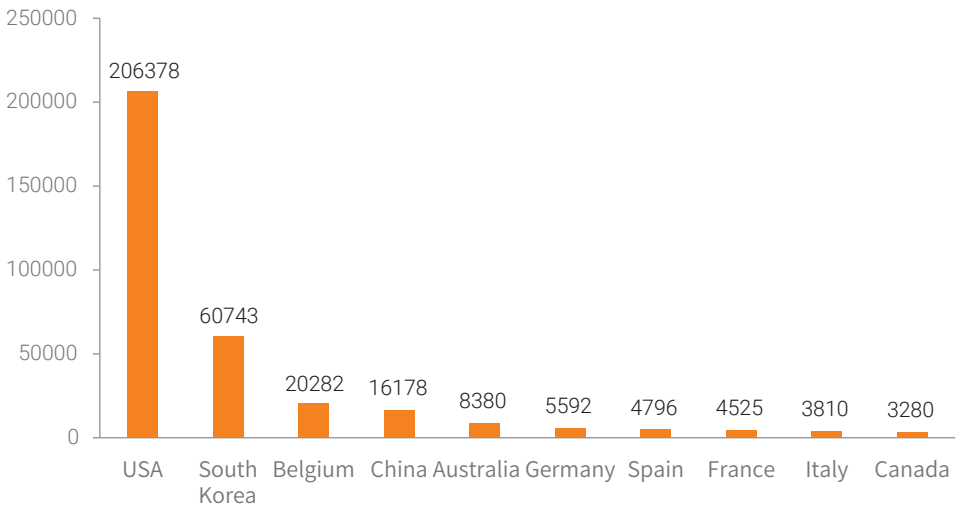


Figure 2.3 Top 10 countries by the number of exposed industrial control devices using Modbus

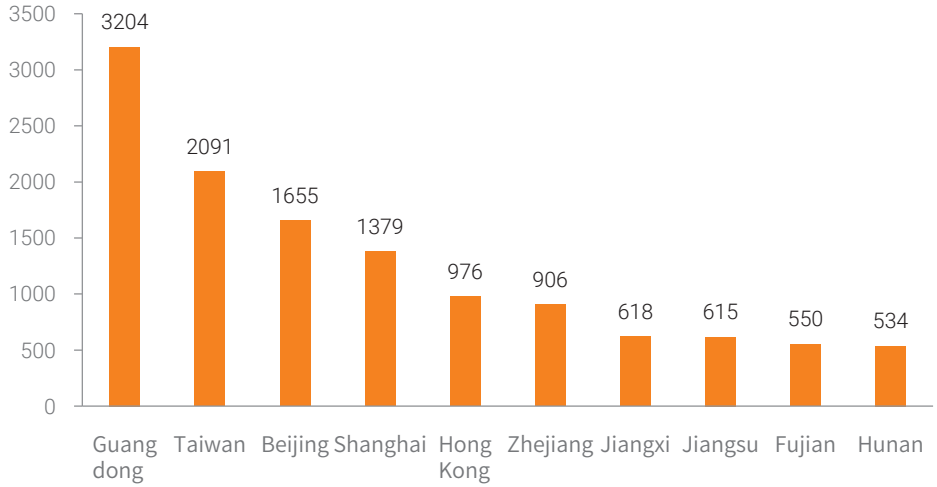
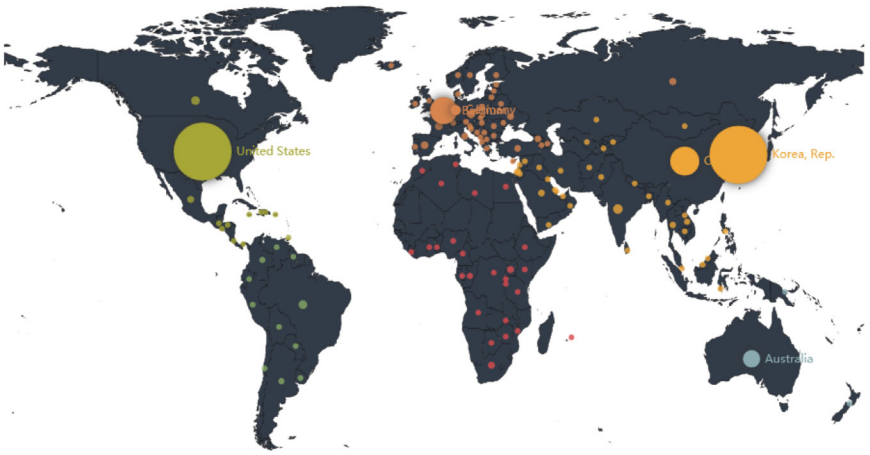


Figure 2.4 Top 10 provinces in China by the number of exposed industrial control devices using Modbus



A total of 375,835 devices detected

Figure 2.5 Global distribution of industrial control devices using S7

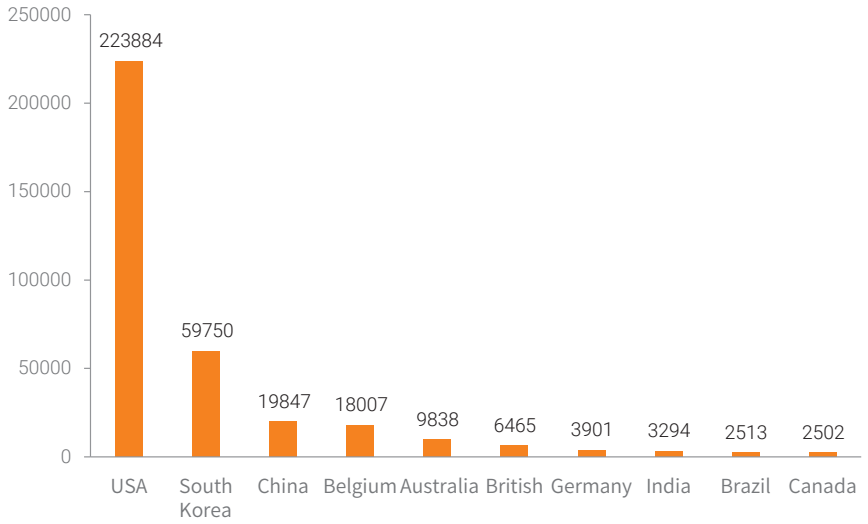


Figure 2.6 Top 10 countries by the number of exposed industrial control devices using S7

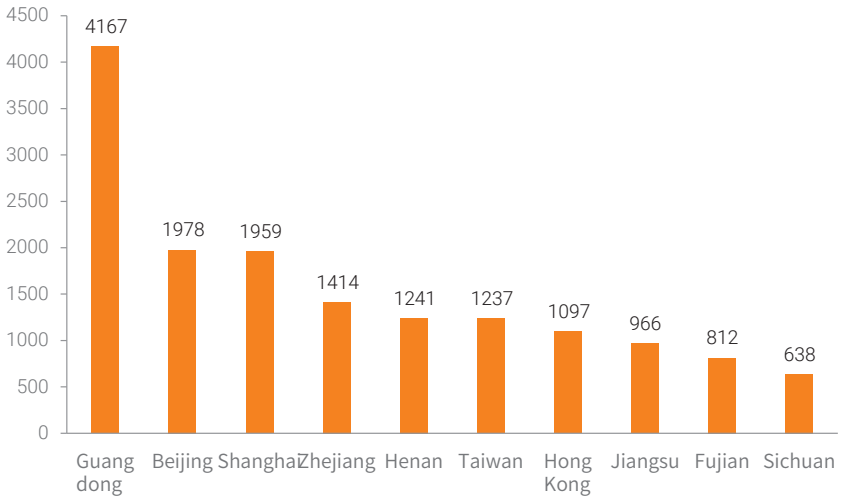
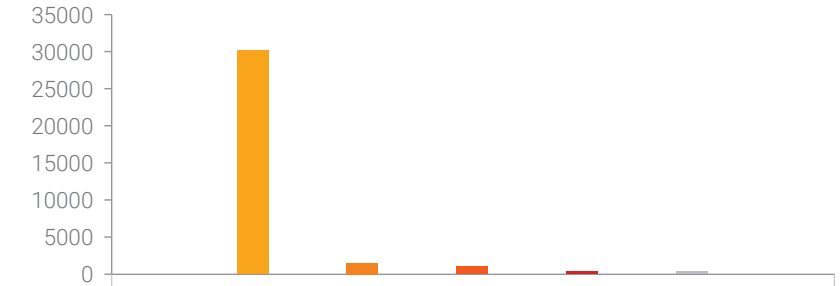


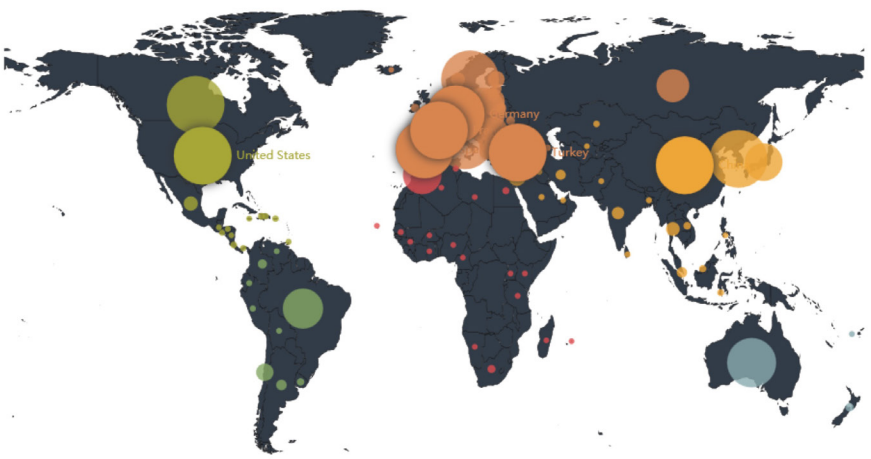
Figure 2.7 Top 10 provinces in China by the number of exposed industrial control devices using S7

The following figure shows the number of industrial control devices using Modbus, S7, DNP3, ENIP, and IEC around the world in 2018.



	Device Count
Modbus	30065
IEC	1451
DNP3	953
S7	243
ENIP	232

Figure 2.8 Statistics of global industrial control devices using different protocols



A total of 32,944 devices detected

Figure 2.9 Global distribution of industrial control devices using the five protocols

As more and more industrial control systems and devices worldwide are connected to the Internet, they will be exposed to more security risks. According to statistics from Kaspersky, in 2017 H1, 20.6% of threats against ICS computers were sourced from the Internet and this figure was increased to 27.3% in 2018 H1.[2]

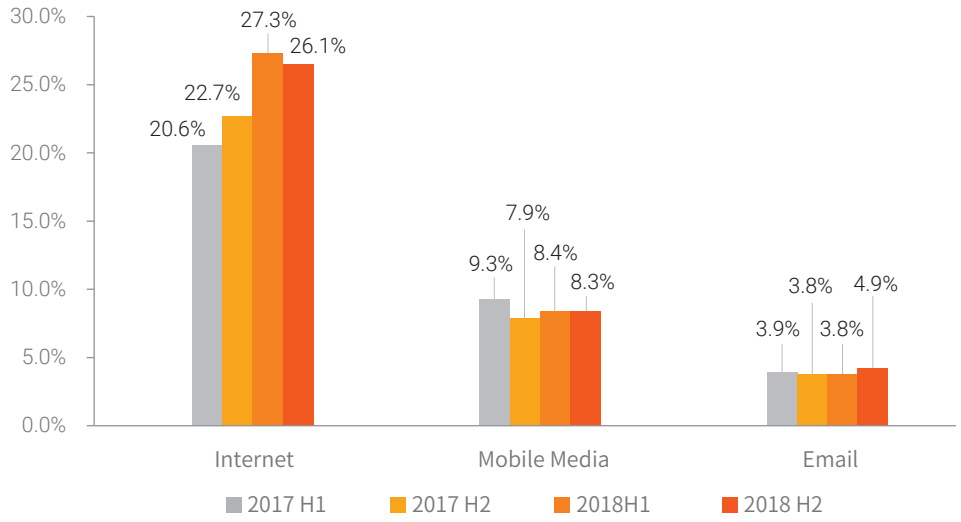


Figure 2.10 Distribution of threats against ICS computers[3]

It seems to attackers that these industrial control devices exposed on the Internet make it possible for them to infect industrial control networks. If certain industrial control devices contain unpatched vulnerabilities and certain vulnerabilities within ICS software and hardware are shared and made publicly available, vulnerabilities in these devices will become attackers' most likely point of entry into the industrial control networks.

In addition, we have worked out the distribution of industrial control device vendors serving different sectors, as shown in the following figures. As HMIs, DCSs, and PLCs need to run operating systems and software, vulnerabilities tend to occur in the three types of devices. Therefore, we mainly focus on these types of devices here.

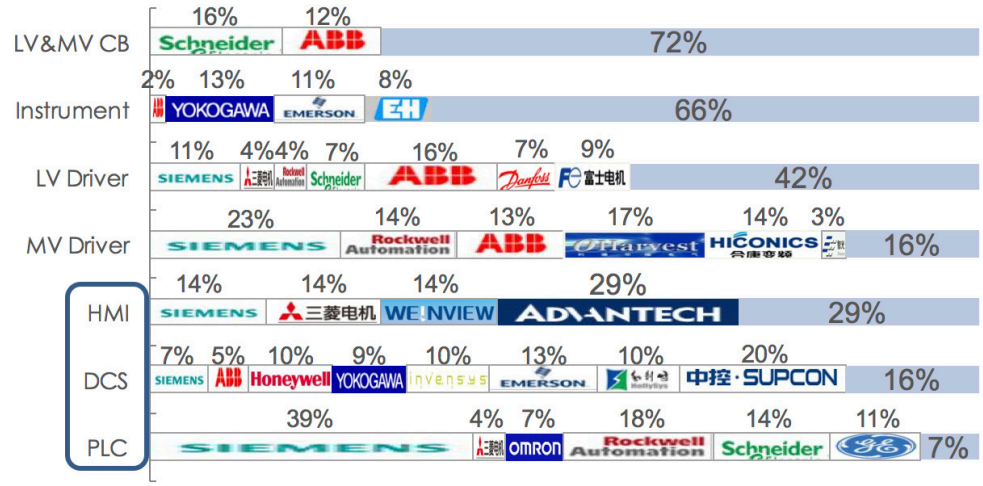


Figure 2.11 Distribution of ICS vendors serving the water supply and treatment sector

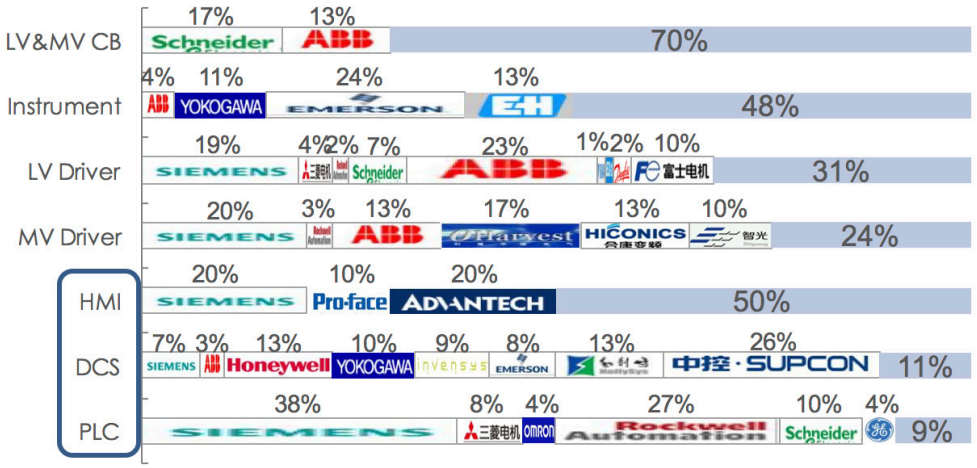


Figure 2.12 Distribution of industrial control device vendors serving the chemical sector

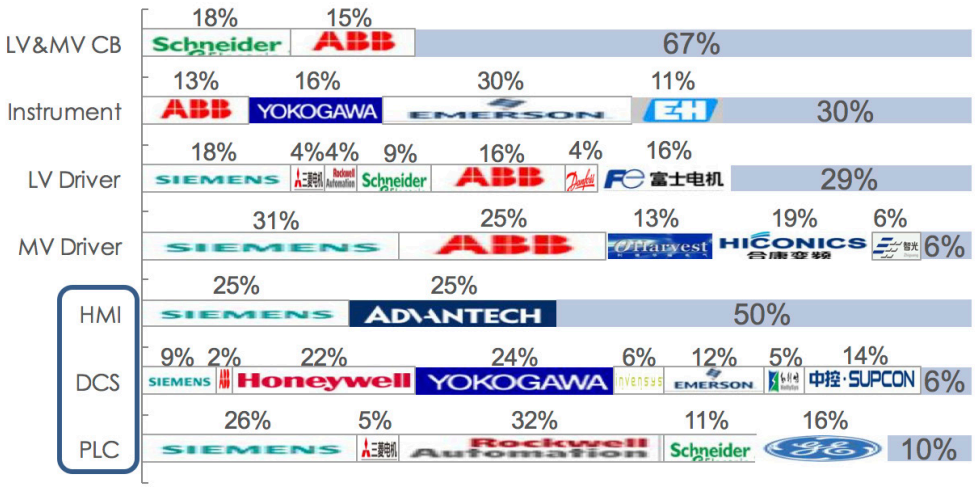


Figure 2.13 Distribution of industrial control device vendors serving the petrochemical sector

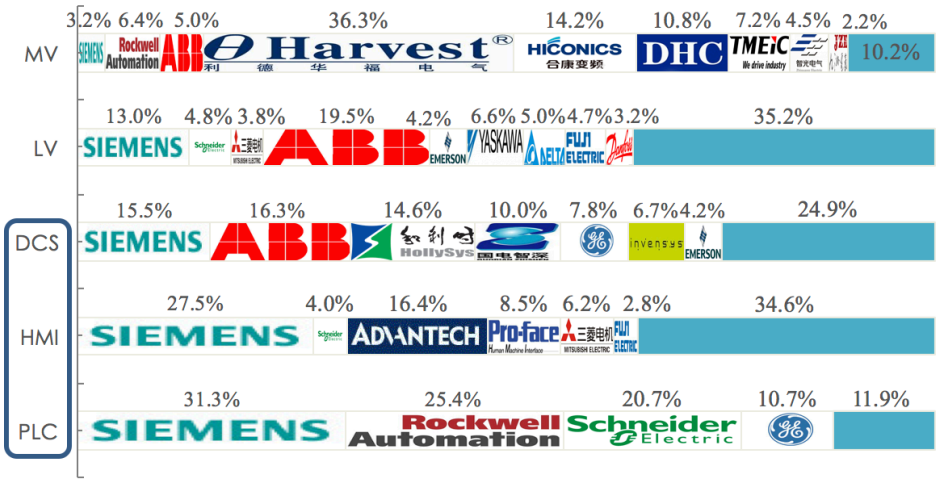


Figure 2.14 Distribution of industrial control device vendors serving the electric power sector

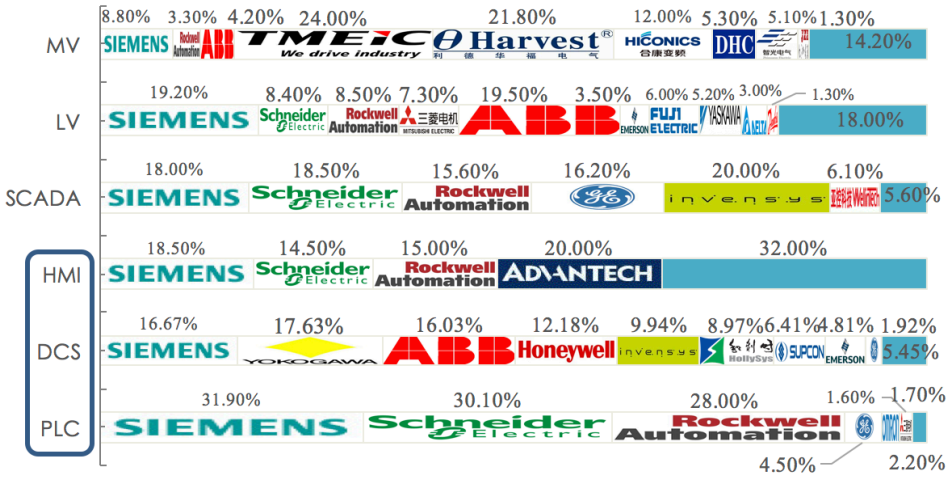


Figure 2.15 Distribution of industrial control device vendors serving the metallurgy sector

2.3.2 ICS Vulnerability Trend

As industrial control has been delving deeper in recent years, more and more ICS vulnerabilities are discovered by researchers. As vulnerabilities publicly available are only a small portion of those hidden in ICSs, the possibility of ICS vulnerabilities being stashed as potential cyber weapons cannot be ruled out. The following sections analyze the trend of ICS vulnerabilities by reference to data publicly available.

2.3.2.1 Statistics Based on Data from ICS-CERT

The USA's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) is responsible for coordinating ICS security response and promoting information sharing. By December 13, 2018, ICS-CERT had released a total of 1046 security advisories on its official website.[4]

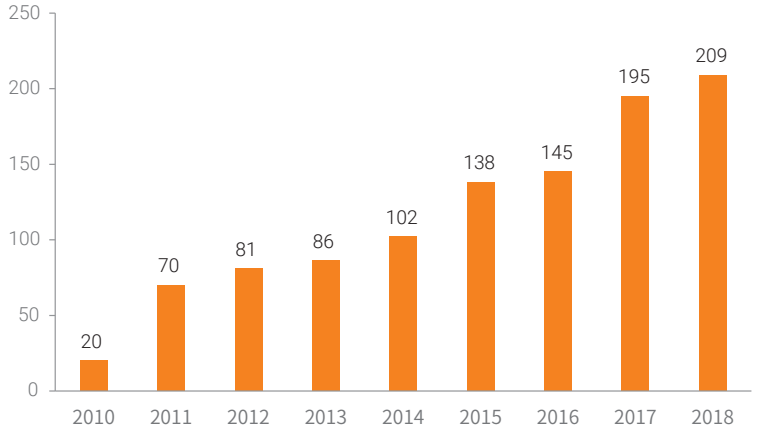


Figure 2.16 Distribution of ICS advisories by year

An annual report released by ICS-CERT[5]shows the distribution of vulnerabilities reported from 2010 to 2018:

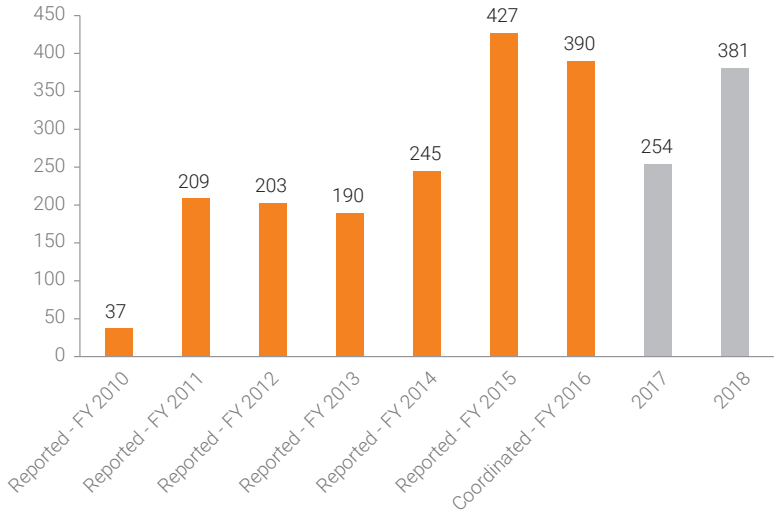


Figure 2.17 Distribution of ICS vulnerabilities by year

Notes:

1. FY refers to fiscal year starting on January 1 and ending on December 31.
2. Statistics in 2010 and 2016 are sourced from the annual report released by ICS-CERT [6], with those

in 2010 through 2015 focused on vulnerabilities received by ICS-CERT. We can see there are 390 vulnerabilities in 2016, each of which is validated and assigned a CVSS score. This is a result of 2282, the total number of vulnerabilities received by ICS-CERT in 2016, minus the number of those that are rejected or proved invalid by vendors.

3. Currently, ICS vulnerability statistics in 2017 and 2018 are not released by ICS-CERT. Statistics presented here only CVE vulnerabilities whose sources include ICS-CERT. As CVE IDs for some ICS vulnerabilities are marked as reserved, please use these statistics with caution.

According to statistics by ICE-CERT, we can see that ICS vulnerabilities are increasing year by year, with a leap in 2015 which is more likely an unusual peak. An average of 5% increase estimated based on previous years' data is more probably a future trend.

2.3.2.2 Statistics of Vulnerabilities Assigned CVE IDs

Some ICS vulnerabilities are given CVE IDs. In the light of the influence of CVE, we collect statistics on ICS vulnerabilities assigned CVE IDs.

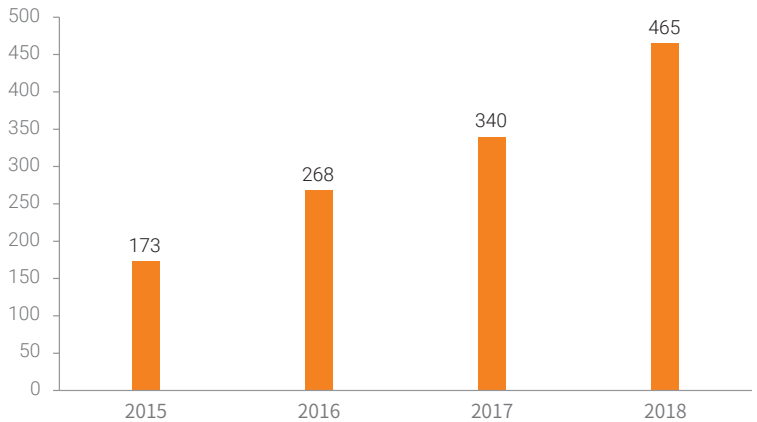


Figure 2.18 Distribution of ICS vulnerabilities assigned CVE IDs in 2015 through 2018

Note: It takes a long time to fix ICS vulnerabilities (most ICS vulnerabilities are not addressed until six months later and a few remain unfixed within one year). By December 13, 2018, some of ICS vulnerabilities discovered in 2017 and 2018 were still not solved. Those unpatched vulnerabilities are

not covered in statistics.

Since the occurrence of the Stuxnet incident, ICS security has begun to draw attention of more and more countries. Many companies and institutions are discovering ICS vulnerabilities, more and more ICS vulnerabilities are detected year by year.

We divide vulnerable devices into HMIs and devices and show their proportions in the following figure.

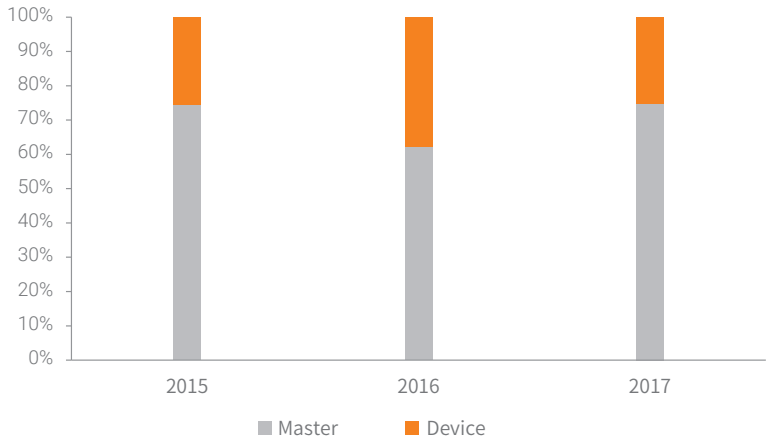


Figure 2.19 Statistics of devices with ICS vulnerabilities

According to statistics, a large portion of ICS vulnerabilities stem from HMIs which usually use web systems and database systems that are susceptible to security issues. ICS vulnerabilities related to application software running on PCs can be easily identified by traditional security companies. By contrast, discovering vulnerabilities in industrial control devices entails greater difficulties because ICSs tend to be embedded systems and industrial control software and hardware are highly customized and tailored. In addition, ICS vendors seldom make firmware updates publicly downloadable, and so only a smaller number of vulnerabilities are spotted on industrial control devices. However, as security vendors are setting about to go deep into industrial control device security, more and more vulnerabilities will be revealed.

The following figure shows the distribution of ICS vulnerability by vendor:

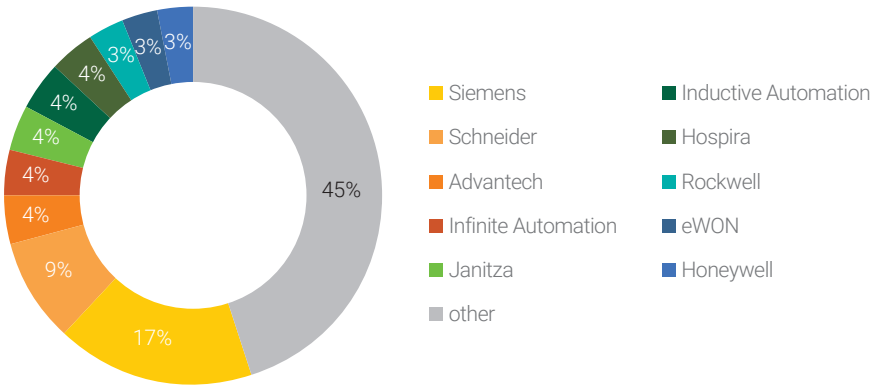


Figure 2.20 Distribution of ICS vulnerabilities by vendor in 2015

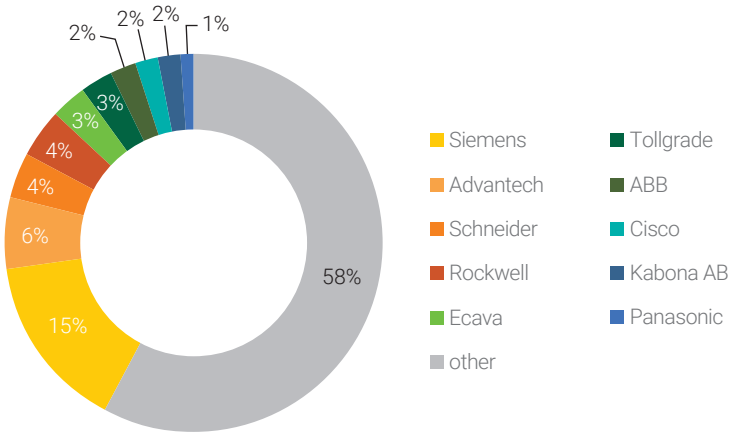


Figure 2.21 Distribution of ICS vulnerabilities by vendor in 2016

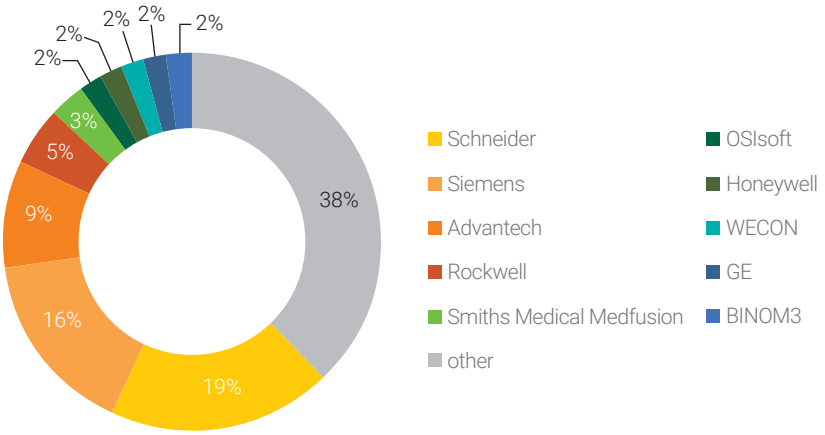


Figure 2.22 Distribution of ICS vulnerabilities by vendor in 2017

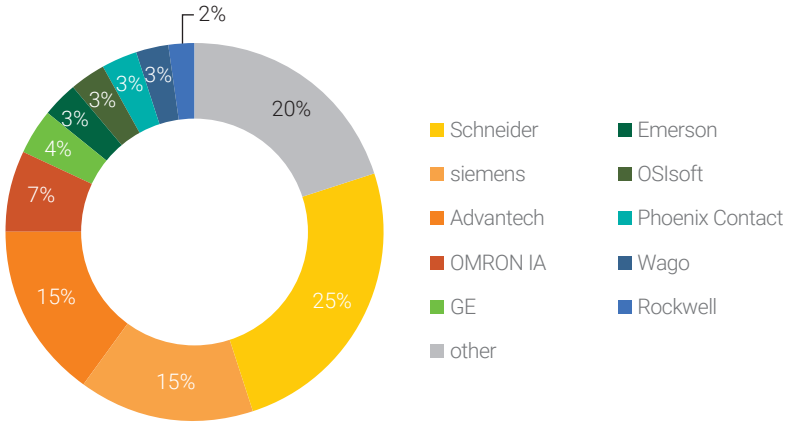


Figure 2.23 Distribution of ICS vulnerabilities by vendor in 2018

After aggregating the ICS vulnerability data in the last four years, we work out the top 10 vendors and their proportions.

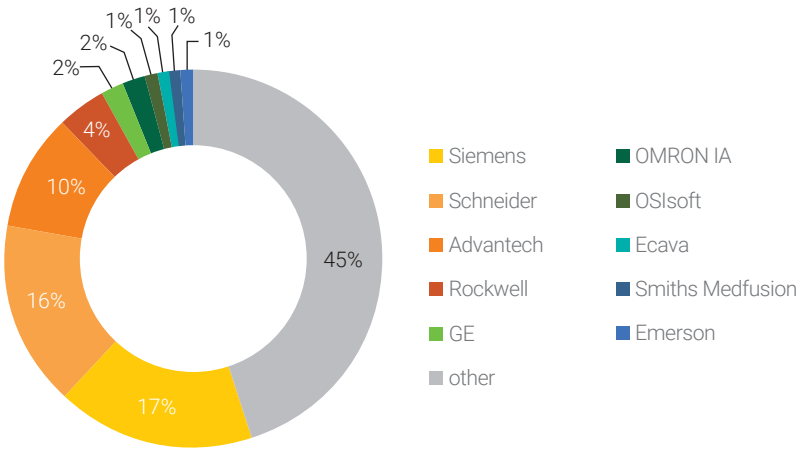


Figure 2.24 Distribution of top 10 vendors with the highest ICS vulnerability ratios in 2015 through 2018

As far as ICS vulnerabilities are concerned, Siemens, Schneider, Advantech, Rockwell, and Omron are all top vendors. However, it should be noted that devices with more vulnerabilities revealed to the public are not necessarily less secure. They seem to contain more vulnerabilities only because they are widely used and receive more attention. Take the PLC market in China as an example. Siemens, Mitsubishi, Omron, Rockwell, and Schneider have a combined market share of 80% in the PLC field in China. Thus, it is not difficult to understand why security researchers and attackers focus their attention on PLCs from these vendors.

2.3.2.3 Security Risks Brought by ICS Vulnerabilities

More and more vulnerabilities are exposed each year. So, how do those vulnerabilities affect the ICS industry? Now, we will explain the impact by reference to the data sourced from Mandiant ICS Healthchecks of FireEye. [7]Mandiant ICS Healthchecks have assessed network security risks facing organizations in multiple sectors to determine the risk level of vulnerabilities by identifying the exploitability and the impact of a given issue, and cross-referencing the results. Our statistics show that at least 33% of security issues discovered in ICS organizations are rated high-risk or critical.

This means that attackers are highly likely to exploit these issues to gain control of the target system and compromise other systems and networks, cause disruption of services, disclose unauthorized information, or result in other significant negative consequences.

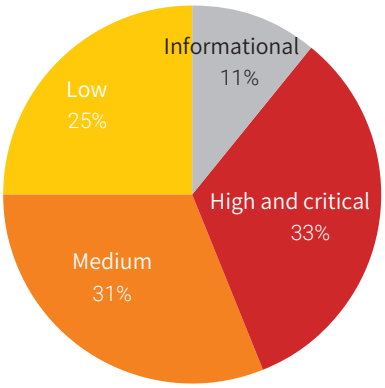


Figure 2.25 Distribution of security issues by risk level

Of the high-risk and critical security issues (33%), most of them are related to vulnerabilities.

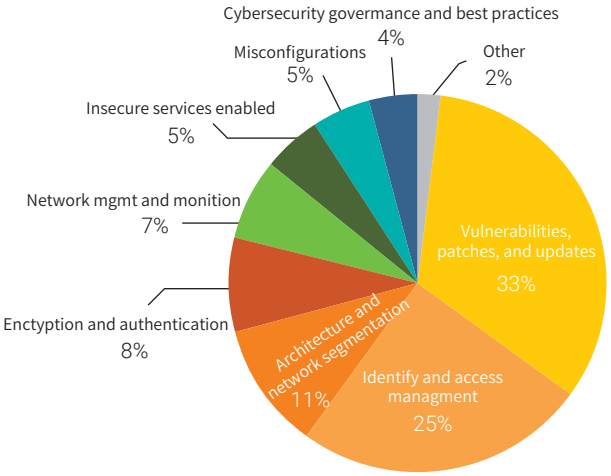


Figure 2.26 Sources of high-risk and critical threats

The preceding statistical results match the statistics of numerous ICS incidents that have occurred in recent years. That highlights the fact that a core section in security incidents is exploiting ICS

vulnerabilities to compromise the entire ICS system.

Here, we take the Stuxnet virus first discovered in June 2010 as an example. Stuxnet is a virus specially made to target infrastructure (in the energy sector) in the real world by exploiting four 0-day vulnerabilities, i.e., shortcut file parsing vulnerability (MS10-046), print spooler service vulnerability (MS10-061), kernel-mode driver vulnerability (MS10-073), and Task Scheduler vulnerability (MS10-092).

At the end of 2014, the refined BlackEnergy malware exploited a recently patched flaw in SIMATIC WinCC (sub-process monitoring system from Siemens) to attack the SCADA HMI system.

In 2017, the TRISIS (also known as TRITON) was found to exploit the 0-day vulnerability in Schneider Electric's Triconex safety instrumented system (SIS) to initiate a cyberattack against an oil and gas factory in the Middle East, causing machines in this factory to cease to function. As the first kind of malware against SISs, TRISIS can cause factories to close down or result in personal injuries, and no doubt, a big threat.

The Threat Landscape Report for Q2 2018 released by Fortinet suggests that the most prevalent exploit attempt in the quarter involved backdoor access in Schneider's Quantum Ethernet Module. As the default account uses a hard-coded password, a remote attacker could gain access to the device with this account through FTP access. A buffer overflow vulnerability in Siemens Automation License Manager came in second, followed by another overflow vulnerability in Advantech WebAccess. The two overflow vulnerabilities are caused by improper input sanitization and can allow arbitrary code execution.

Security vulnerabilities in industrial control networks can lead to a wide range of consequences from factory shutdown to nuclear plant explosion and nationwide power outage. Therefore, discovering and fixing vulnerabilities in ICSs to improve these systems before hackers successfully target ICSs is an important means to ensure secure operating of ICSs and increase security robustness of enterprises.

2.3.2.4 Analysis of Threats Against the Industrial Control Sectors

In preceding sections, we present the distribution of industrial control devices by vendor and the distribution of ICS vulnerabilities by vendor. Based on these statistical results, we make an overall

analysis of security threats facing different industrial control sectors in this section.

ICS vulnerabilities mainly reside in HMIs, PLCs, and DCSs. Here, we first calculate the average proportion of vendors of the three types of devices, and then calculate the threat index by using this proportion and the proportion of ICS vulnerabilities by vendor.

Sector-specific average proportion of controller vendors = (HMI proportion + PLC proportion + DCS proportion)/3

Sector-specific threat index in a certain year = Σ Sector-specific average proportion of controller vendors x Proportion of vendor-specific controller vulnerabilities

The following figures show the threat index from 2015 through 2018.

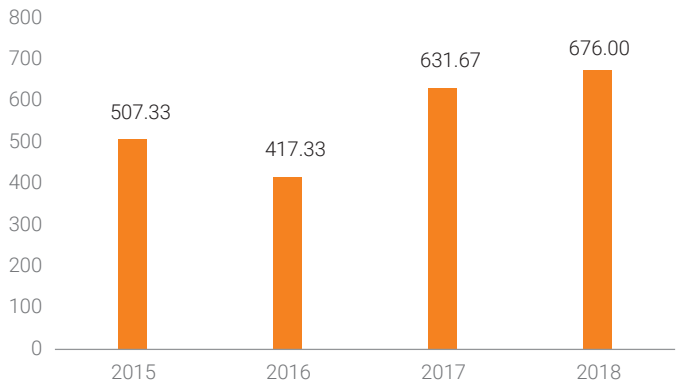


Figure 2.27 Threat trend of the water supply and treatment sector

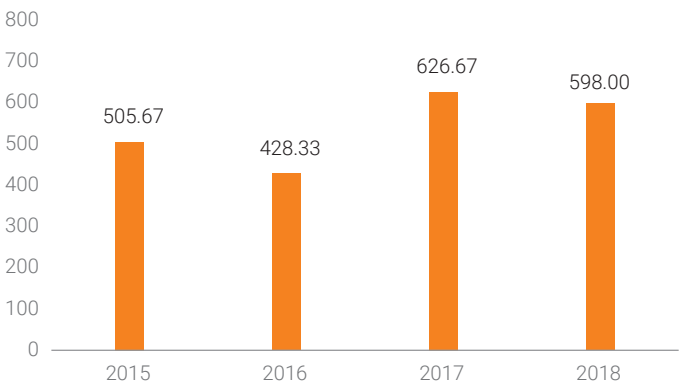


Figure 2.28 Threat trend of the chemical sector

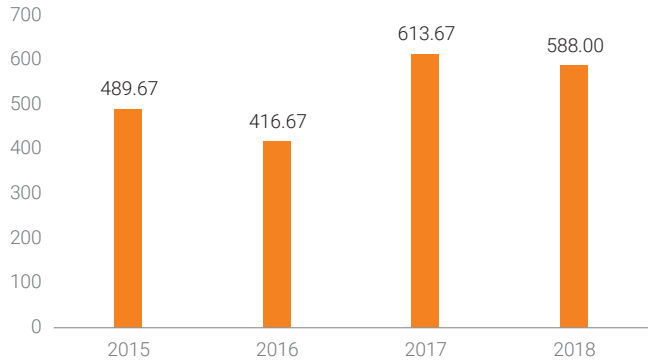


Figure 2.29 Threat trend of the petrochemical sector

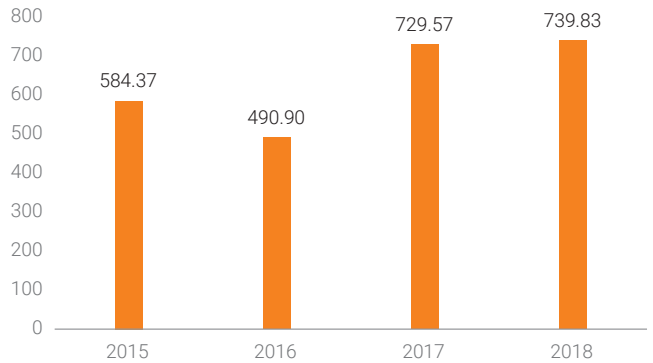


Figure 2.30 Threat trend of the electrical power sector

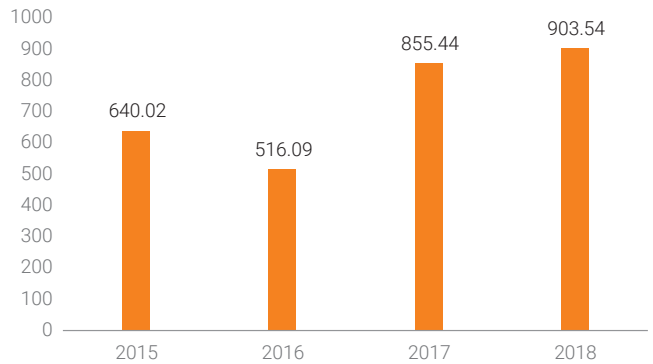


Figure 2.31 Threat trend of the metallurgical sector

According to the preceding statistical results, ICSs were exposed to more threats in 2017 and 2018 than

in 2015 and 2016. Though 2016 saw a relatively low threat index, this does not mean that ICSs were more secure in this year, but only a small portion of vulnerabilities were discovered in industrial control devices in these typical industrial scenarios. As the research on industrial control devices from major vendors goes further, more and more vulnerabilities will be spotted, leaving ICSs vulnerable to much more serious threats.

2.4 ICS Security Trend

All in all, with IT and OT converging at a rapid pace, ICSs will be exposed to more threats that are evolving faster and faster. The threat evolution is reflected in the following aspects:

- ICSs, which were previously deployed on the isolated intranet, are gradually connected to the external network. This is a response to the need of the industrial control industry as well as a must of social progress. However, most ICS security mechanisms are short of authentication, encryption, and audits.
- Also, people, when designing ICSs, fail to realize that they would have the chance to access the Internet. Therefore, ICSs, once connected to the Internet, will be exposed to new security risks.
- Cyberattacks, which originally affect virtual assets, have evolved to do damage to the physical world, that is, beginning to target embedded systems installed on computers.
- Technical changes, including generalization, software and hardware combination, and interoperability, directly contribute to attack surface expansion. Penetrating into ICSs through the Internet has become an important attack approach, making any ICS a potential target.
- Traditional viruses and ICS viruses are interwoven, as demonstrated by the Stuxnet virus.
- Attacks using computers as a springboard may evolve into direct attacks against ICSs in the future.
- The extremely difficult attacks that exploit unrevealed vulnerabilities will develop into attacks which can even bypass the underlying knowledge barrier of ICSs, by combining common attack means.
- It is difficult to discover and alert attacks: It is difficult to acquire hardware (expensive or difficult

to buy) and debug (embedded) them. There is a wide variety of devices which use all sorts of proprietary protocols. Besides, little information is made publicly available regarding ICS software.

- Industrial control devices are facing increasingly severe 0-day issues. Owing to the long cycle of maintenance and testing, industrial control device vendors tend not to fix vulnerabilities in time. Sometimes, they release patches even a year after vulnerabilities are revealed. Even though related patches are released by vendors, these patches usually are not installed in time to address vulnerabilities in devices in industrial control fields due to the continuous operation of devices as well as reasons in the management and technology aspects.
- More and more ransomware viruses will target ICSs. Currently, ransomware viruses such as WannaCry mainly attack IT systems in ICSs, like master devices and ERP systems. In the future, ransomware viruses will arise against OT systems such as PLCs and DCSs.
- Denial-of-service vulnerabilities in ICSs are getting more and more dangerous and possibly responsible for significant security incidents.

In conclusion, as ICSs are facing increasingly serious security threats, ICS security is a long-term process that never ceases changing.

3

ICS Information Security Assurance Framework

3.1 ICS Security Assurance Principles

In response to related compliance requirements put forward by the industry and the country, the ICS information security assurance framework will be developed to combine both technology and management, taking full account of the enterprise's business requirements and ICS operating characteristics. By switching ICS protection from deployment of security policies to that of security capabilities, such a framework aims to enable an all-around improvement in security technology and management capabilities for the purpose of integrating management, control, and defense. With this framework, enterprises' security capabilities will gradually cover system go-live, operating, O&M, and inspection, achieving closed-loop security control and management for ICSs.

3.2 Working Principle of the ICS Information Security Assurance Framework

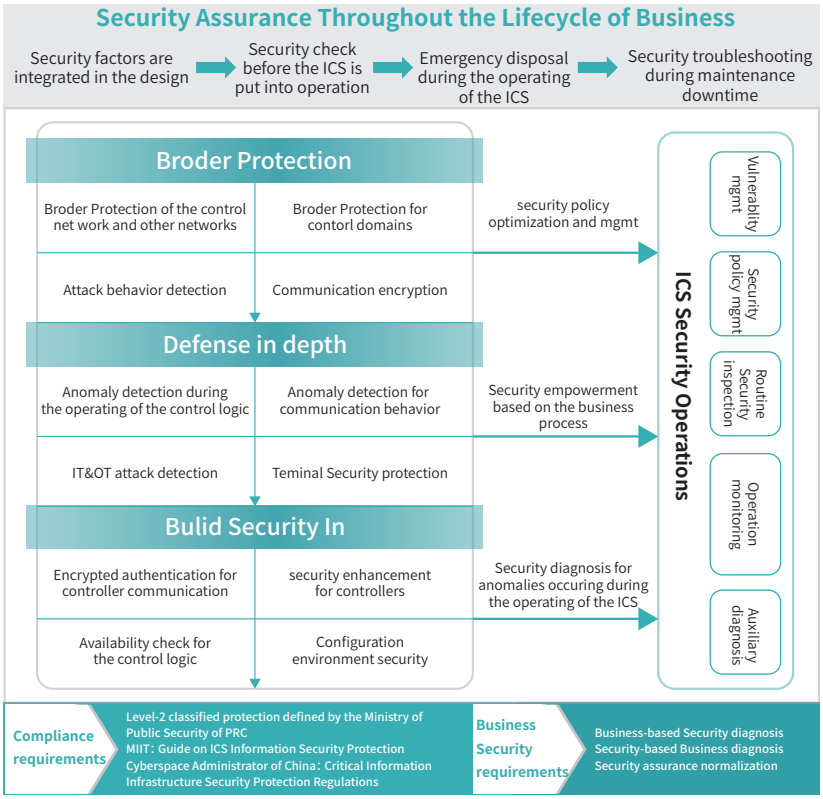


Figure 3.1 ICS security assurance framework

ICS security development should be conducted in line with compliance requirements while addressing business security requirements. For this reason, ICS security should run through the entire business lifecycle, including incorporating security requirements into system development, conducting security inspection before the system goes live, responding to incidents during system operation, and performing security troubleshooting during maintenance downtime. As industrial environment security is an objective existence, an efficient ICS security protection system needs to be built to provide robust security support.

Building an efficient ICS protection system covers three aspects: border protection, defense in depth, and Build Security In. Border protection requires security isolation between different zones. For instance, borders between OT and IT can be isolated using a security device like an industrial firewall or a GAP. Defense in depth should take full account of effective protection for connections between controllers in the controller connection domain to make sure that the communication process is controllable. Sound security monitoring and protection measures should be deployed within the ICS to make it **controllable** and **manageable** and **its monitoring results visual to users**. The control logic needs to match the business profile. Efficiently perceiving behavior in the communication process, the deployed security measures can promptly discover and deal with known attack behavior and perceive what system anomaly is caused by unknown attack behavior, thus providing data support for system failure locating. Security technologies such as industrial invasion detection, industrial anomaly monitoring, and sandboxing should be employed for effective monitoring of communication traffic and files in the system, as well as various terminals such as industrial hosts, industrial databases, and OPC servers. Build Security In should place emphasis on security reinforcements of firmware in controllers, including encrypting the firmware, checking the availability of control instructions, taking account of the self-correction of configuration software during the configuration process, so as to increase the security level of ICSs.

When it comes to security operations, this framework needs to meet the following requirements: reducing security risks for production enterprises while helping them increase the operation efficiency of production systems; addressing business security requirements to ensure that business is done in a compliant and continuous way; improving enterprises' comprehensive business security capabilities on the basis of compliance assurance; incorporating security throughout the lifecycle of business.

3.2.1 Border Security Protection

3.2.1.1 Guidance on Border Protection

Guidance on ICS Border Protection Provided by a Guide from MIIT

As the *Guide on ICS Information Security Protection* is released by MIIT, ICS security is raised to a new height. This guide indicates that industrial enterprises should do a good job in ICS security protection from 11 aspects. This guide expounds on border protection, a key section of ICS security control, as the third aspect, noting that borders between the industrial control network and the enterprise network or Internet should be protected by ICS network border protection devices, for instance, deploying an industrial firewall or GAP to logically isolate security zones of the industrial control network. So, to speak, this guide provides constructive suggestions on ICS border protection from an industry perspective.

Guidance on Border Protection of the Electrical Power Sector

The National Development and Reform Commission (NDRC) released the *Provisions on the Security Protection of the Electric Power Monitoring Systems* as early as in 2014 to normalize security protection of ICS systems of electrical power enterprises, making this industry a pioneer in ICS security. In early 2015, the National Energy Administration issued a document (NEA No. 36) to further set forth ICS security compliance requirements of electric power enterprises, putting forward security protection solutions and security assessment specifications for provincial electricity distribution, prefectural electricity distribution, power distribution networks, power generation plants, and substations. Both No. 34 and No. 36 documents push forward ICS security protection of electrical power enterprises. Revolving around security zone division, dedicated network building, horizontal isolation, and vertical encryption, the two documents put emphasis on border security. The subsection for security of borders between the control zone (security zone 1) and non-control zone (security zone II) specifies that a network device that provides the access control function, a secure and reliable firewall hardware device, or a security device that provides similar functions can be deployed at the border of both zones to implement logical isolation, packet filtering, and access control. The inter-system security protection subsection specifies that logical access control measures of a certain strength should

be taken between different systems in either security zone 1 or security zone 2. In these security protection scenarios, industrial firewalls, isolation devices, or VLAN technology can be deployed to meet compliance requirements while ensuring business continuity, delivering satisfactory border security protection for ICSs of electrical power systems.

Guidance on Border Protection of the Petrochemical Industry

In the petroleum and petrochemical industry, Chinese National Petroleum Corporation and Sino Petroleum Corporation have released the Outline of the Thirteenth Five-Year Plan to clarify the importance of ICS security. For instance, an ICS system network on an oil field, which covers the wellhead, stations, pipelines, and related facilities on the oil production field, is used for real-time production data collection, remote control, and automatic control. This network is susceptible to external attacks as it has a wide coverage, including many devices that are deployed in the wild and use multiple networking methods such as cable and wireless. Ensuring that the ICS can operate in a secure way is a fundamental purpose for protecting security of the industrial control network on an oil field. For the industrial control network of an oil field, a key issue to solve is how to prevent theft, corruption, or tampering of business information, especially instructions, in a bid to stop hackers or malware from using a remote device or an internal LAN terminal to attack devices deployed on the industrial control network in the oil field. Security risks in these information infrastructures can be resolved by deploying an industrial firewall or GAP, thus ensuring that the industrial control network on the oil field can operate in a secure and stable way.

3.2.1.2 Technical Framework for Border Protection

Access Control and Security Protection Between Security Zones

Firewalls are deployed between different layers of network to control cross-layer access and implement deep sanitization of inter-layer data exchanges, preventing attackers from penetrating into or attacking a lower-layer network from an upper-layer one.

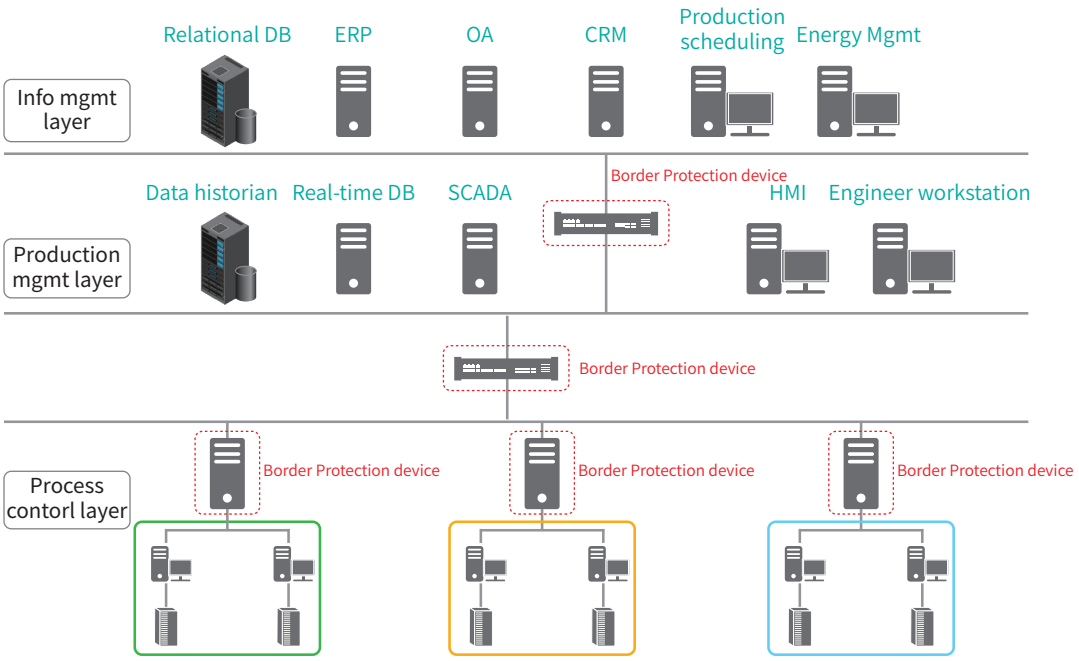


Figure 3.2 Access control and security protection between security zones

Firewalls are deployed between factories, processes, and business subsystems at the same layer to divide them into different security zones. Between these security zones, access is controlled and data exchanges are thoroughly sanitized to reduce the spreading of security issues across security zones as well as lower the impact of these issues.

Security Protection for Major Devices

Firewalls are deployed in front of major devices to restrict access only to certain IP addresses, block access to non-business ports, filter out illegal operation instructions, record all access and operations, and implement all-round security protection and auditing for these operations.

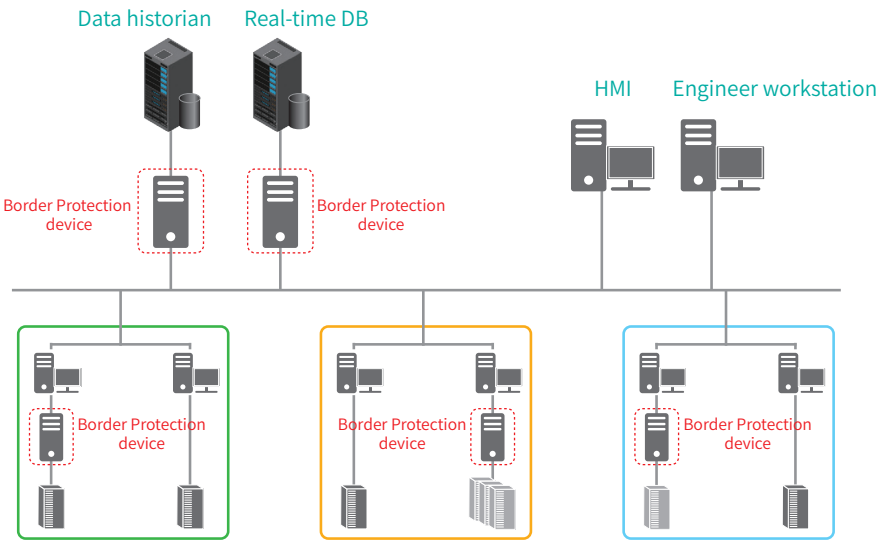


Figure 3.3 Security protection for major devices

Security Interaction Between Industrial Networks in Different Areas

Implement security protection for industrial networks in different operation areas to prevent attacks originated from the public network and ensure border security protection of those networks.

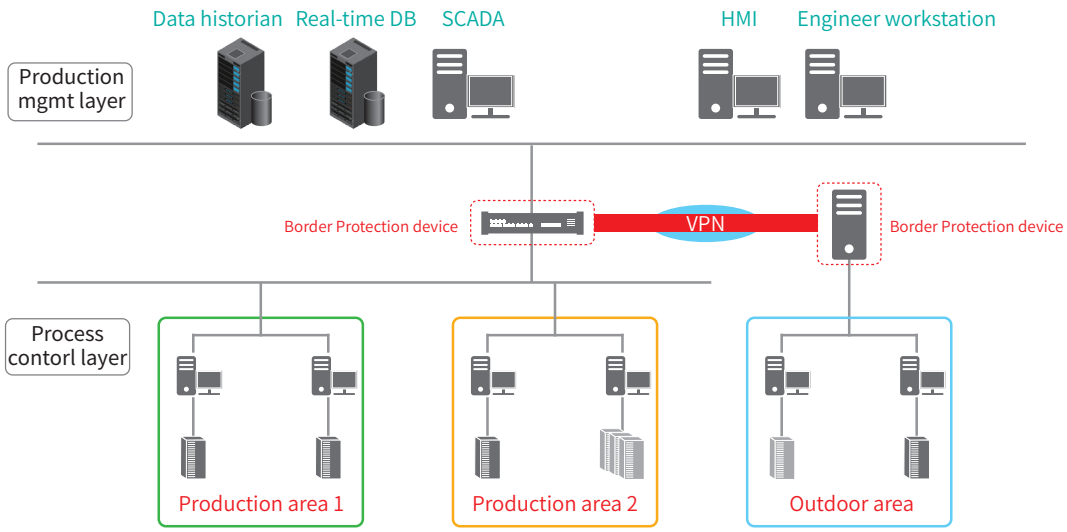


Figure 3.4 Security interactions between dispersed industrial networks

Use a VPN to encrypt and protect the data transmitted between the operation area and the scheduling center and set up secure data exchange channels to ensure secure data transmission.

Security-Aware Remote O&M Management

Deploy a firewall at the border between the industrial network and the public network and enable the VPN function on the firewall to use it as a bastion device for remote maintenance. Remote maintenance personnel connect to the firewall through the VPN to perform identity authentication and implement encrypted protection for remote maintenance operations performed through the public network, thus achieving secure remote maintenance.

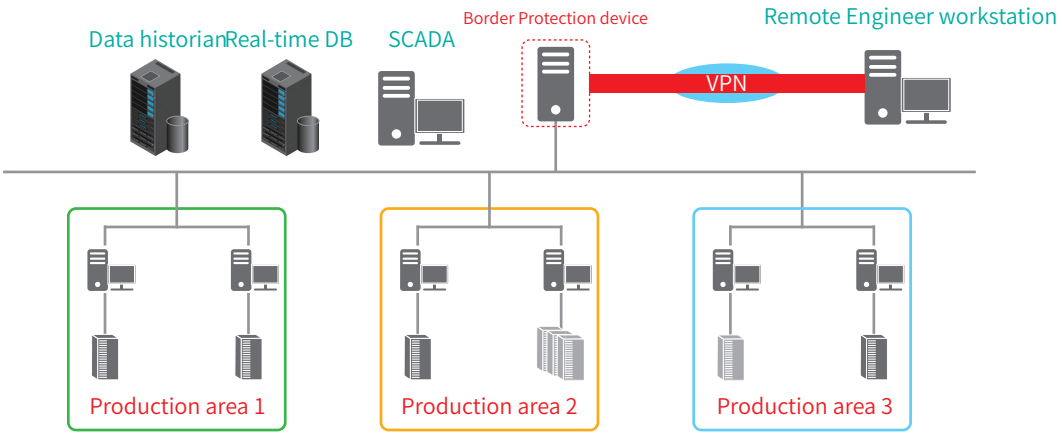


Figure 3.5 Secure remote maintenance

3.2.2 Defense in Depth

3.2.2.1 Defense-in-Depth Framework for Industrial Control Networks

Defense-in-depth measures need to be introduced for automated ICSs, according to characteristics and security requirements of ICSs. Defense-in-depth measures refer to multilayered security protection measures that target different aspects to protect the security of critical ICSs and applications. The major advantage of such measures is that the attacker has to penetrate into or bypass multilayered security mechanisms, increasing the difficulty of launching a successful attack. Once measures at one layer are problematic, other measures at other layers can fill the gap, thus avoiding such a dangerous

situation in which breaking through one of the defense lines may render the entire defense system ineffective.

To build a defense-in-depth system for automated ICSs, we should first analyze actual ICS security requirements and work out an appropriate security plan. Also, we should assess risks facing ICSs to identify sources of threats and risks of those ICSs. On this basis, we should build and deploy a hierarchical security protection system to provide professional industrial security services, by reference to the product security operation guide.

Currently, the industrial information security concept derived from defense in depth covers automated ICSs of all levels, and thus defense in depth is a practical solution to meet key requirements of the industrial information security field. Standard security control measures include establishing security policies and processes, deploying a firewall for security isolation and protection of different security units (security zones), using a VPN to protect communications between units, reinforcing the system, and taking other access control measures such as deployment account management, as well as patch management and malware detection and protection.

3.2.2.2 Policies for Building the Defense-in-Depth System for Industrial Control Networks

For the sake of ICS security protection, we can build a defense-in-depth system by implementing the following policies:

- Application whitelisting (AWL)
- Proper configuration and patch management
- Attack surface reduction
- Defensive environment setup
- Authentication management
- Secure remote access
- Monitoring and response

Though the seven policies can block more than 90% of attacks, ongoing continuous monitoring is

required to identify certain attack means. In addition, some security administrators may overlook alerts concerning anomalies of a relative low severity which are highly likely to be APT attacks initiated by hackers to target ICSs. Making a correlative analysis against the anomaly information to identify potential security issues can not only reduce the pressure of the administrator, but also better protect ICS security.

The security monitoring and response policy refers to security monitoring of the communication process of control devices at the field control layer and workstations at the process monitoring layer. The ICS security monitoring and alerting system can be set up by using three steps:

1. Deploy security devices applicable to protect ICSs, for example, using industrial control firewalls or IDSs for border protection and employing abnormal behavior monitoring systems or asset identification systems within the industrial control network. Deploying these underlying security systems in the industrial control environment can greatly improve the security of ICSs.
2. Above all these underlying security systems, use a monitoring audit and analysis system to aggregate, extract, and make a correlative analysis of alert records and logs generated by underlying devices and dig hidden information out of these records to have a grasp of the overall security trend of ICSs.
3. Forecast the future security posture. If necessary, provide necessary security measures and adopt more friendly visualization technologies.

Currently, the industrial control network security monitoring and alerting solution is still in its infancy of implementation. According to security requirements and vulnerabilities in industrial control device, we should develop security products tailor-made for ICSs to provide the preceding seven policies to protect the industrial control environment by focusing on various threat points.

3.2.3 Build Security In

Information technology (IT) touches upon many fields. Generally, it can be classified as hardware device, software application, and information data. As hardware device control and information data operation

handling need to be implemented by software, software is the "soul" of the system and program code is a specific form of manifestation of software. Arguably, code is a core element of informatization construction as well as a key priority of security protection of information systems and infrastructure.

Trends towards globalization of IT procurement encourage countries or enterprises to purchase information system products from a greater diversity of sources, further complicating the IT supply chain. This is true for software. In many cases, software systems are essentially a combination of the self-developed, purchased, open-source, and outsourced code. VeraCode's statistics show that 30% to 70% of homegrown software contains third-party code that take on the form of open-source components and commercial or outsourced shared libraries or components. This makes software development more efficient, but undoubtedly poses a great challenge to software security and controllability. In particular, in recent years, high-risk vulnerabilities have been frequently revealed in prevailing underlying open-source components such as Struts 2 and OpenSSL, and Stuxnet hit Iran and BlackEnergy targeted Ukraine, which are two malicious programs exploiting vulnerabilities in underlying software to arbitrarily compromise ICSs. In view of all these, countries and enterprises have gradually focused more attention on the security of the software supply chain, open-source software, and software installed on critical infrastructure, having enacted related national security regulations and strategies.

For software security assurance, we should discover and fix vulnerabilities in software systems as early and quickly as possible. As the original form of software, source code has a rich set of semantics. Ensuring that secure source code is written is in line with the Build Security In (BSI) principle, enabling us to discover all sorts of issues in the software as soon as possible. This is the case for ICSs. For ICSs, BSI should focus on the source code security of industrial application software, slave devices, and other intelligent devices, as well as the security of communication protocols:

- Hackers should have a good knowledge of the embedded operating system so as to successfully plant and execute a virus in it. This is also true for a slave device. The operating environment and point of entry are key to solving this issue: Without support from the operating system, the virus has no place to play its game; if the firmware is encrypted, hackers who cannot decrypt the firmware will

be unable to understand the underlying mechanism; if protocols or interfaces are made proprietary or restricted to a given scope of addresses, there is no way for hackers to access them. For this reason, industrial control equipment providers should develop protocol stacks, control algorithms, hardware platforms, BIOS, and deterministic microkernel independently, and encrypt the firmware, raising the threshold for hackers intruding into the systems.

Multilayer data communication encryption and protection technologies should be deployed to ensure data integrity and confidentiality. That is to say, these technologies should run through the operation layer, network layer, control layer, filed bus layer, and wireless layer; data should be transmitted in non-cleartext to prevent data listening and tampering.

4

ICS Security Solutions for Typical Industrial Scenarios

4.1 Electric Power Sector

4.1.1 Thermal Power

4.1.1.1 System Introduction

Based on computers, communication devices, and test control units, the electric power monitoring system provides a basic platform for real-time data collection, switch status monitoring, and remote control of thermal power plants. It can work with detection and controls devices to form an arbitrarily complex monitoring system. It plays a vital role in the monitoring of thermal power plants by helping enterprises eliminate information silos, reduce operating costs, improve production efficiency, and accelerate the speed of responding to anomalies in the process of power transformation and distribution.

The electric power monitoring system of a thermal power plant consists of the distributed control system (DCS) of the thermal power unit, auxiliary control system of the thermal power unit, plant-level supervisory information system (SIS) of the thermal power plant, governor system and automatic generation control (AGC) function, excitation system and automatic voltage control (AVC) function, network control system, the phasor measurement unit (PMU), five-prevention system, telecontrol system, relay protection and fault information substation, and power acquisition unit. The governor system and AGC function, excitation system and AVC function, network control system, relay protection and fault information substation, telecontrol system, and power acquisition unit are power monitoring systems related to the control center; DCS of the thermal power unit, auxiliary control system of the thermal power unit, plant-level SIS of the thermal power plant, and five-prevention system are internal monitoring systems of the power plant; the PMU, relay protection and fault information substation, and power acquisition unit are factory devices of the control center monitoring system. Figure 4.1 shows the architecture of the electric power monitoring system of a thermal power plant.

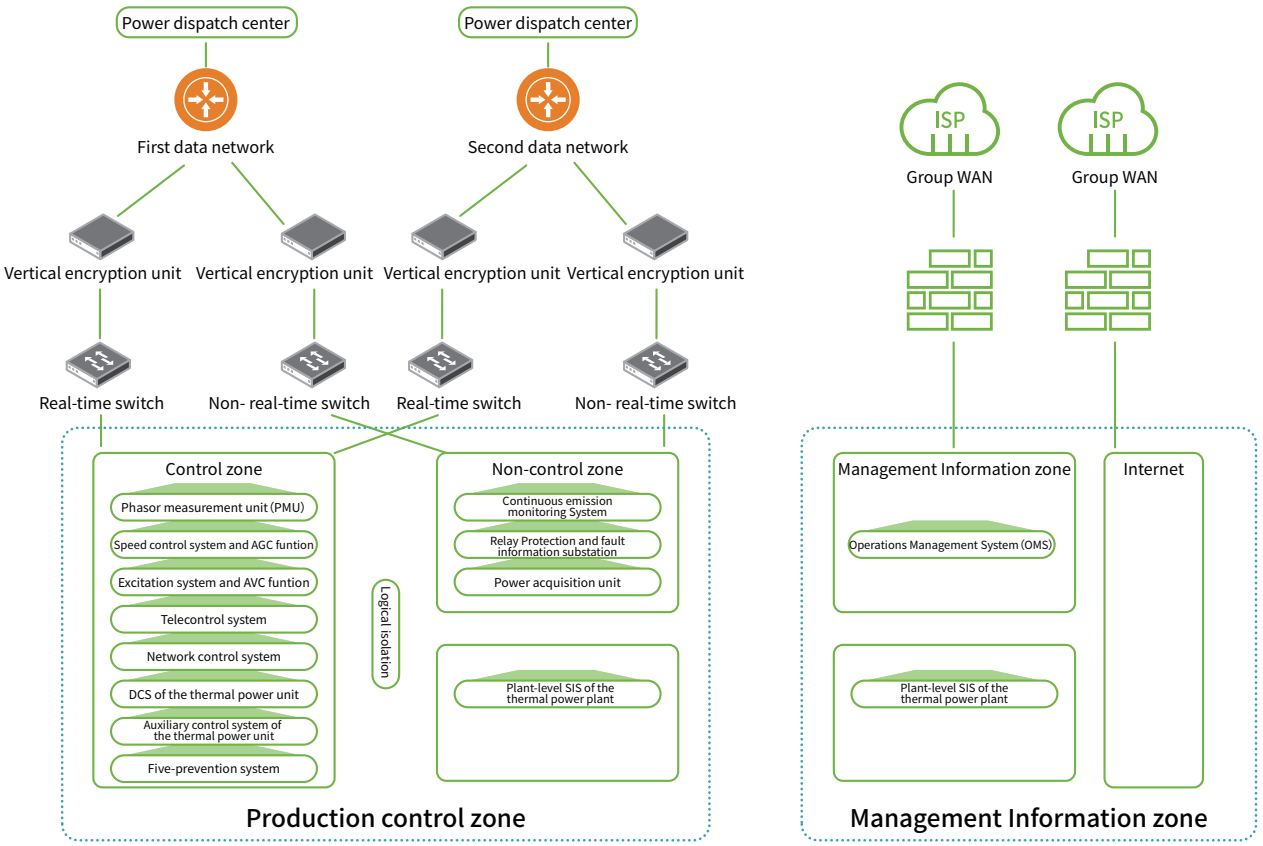


Figure 4.1 Architecture of the electric power monitoring system of a thermal power plant

The electric power monitoring system vertically connects to the provincial control center and network control center and is built with the first and second data networks, forming a redundant structure.

4.1.1.2 System Protection Solutions

Border Protection Solution

- Horizontal border protection
- Horizontal border protection for the production control zone and management information zone

According to actual data interaction requirements of the thermal power plant, forward and backward isolating devices are deployed at the borders of security zone II of the production control zone and the

management information zone. Such deployment is to protect the security of forward and backward data flows between the production control zone and management information zone.

Control Zone (Security Zone I) and Non-control Zone (Security Zone II) Border Protection

Hardware firewalls are respectively deployed at the network border of the control zone and that of the non-control zone, so as to prevent unauthorized access of systems of a lower security level to systems of a higher security level and provide security guarantee for data flows from security zone II to security zone I.

For cross-zone connections with SIS interface message processors via a serial cable, no firewall can be deployed for logical isolation. In this case, associated SIS interface message processors can be deployed in the control zone (security zone I). If no firewall is deployed between servers and SIS interfaces, industrial control firewalls should be deployed.

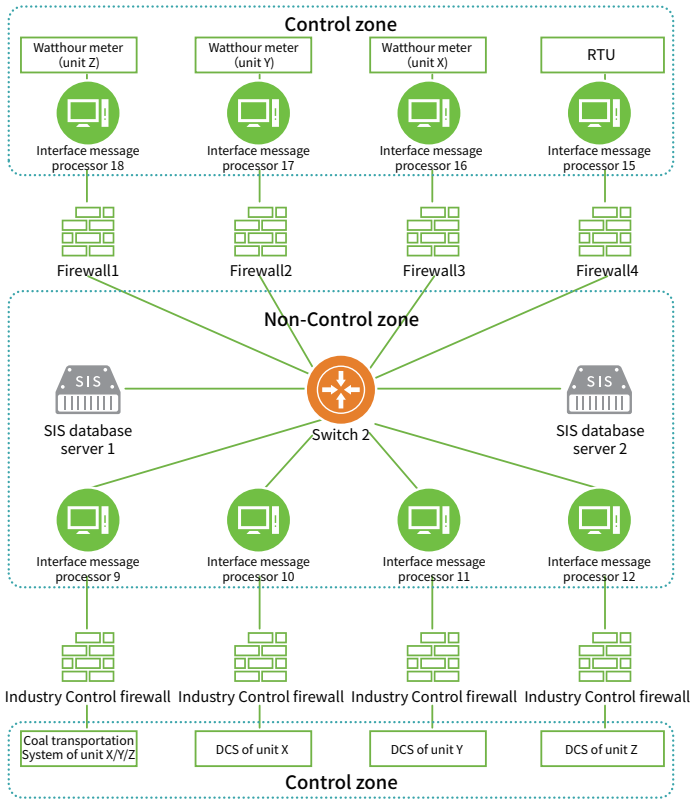


Figure 4.2 Horizontal border protection of the SIS system of units X, Y, and Z

As shown in Figure 4.2, the SIS interface message processors, which connect to watthour meters of units X, Y, and Z, and the RTU respectively, are logically isolated from the switch by four traditional firewalls, while the SIS interface message processors, which connect to the DCSs of units X/Y/Z, X, Y, and Z, are logically isolated from the switch by industrial control firewalls.

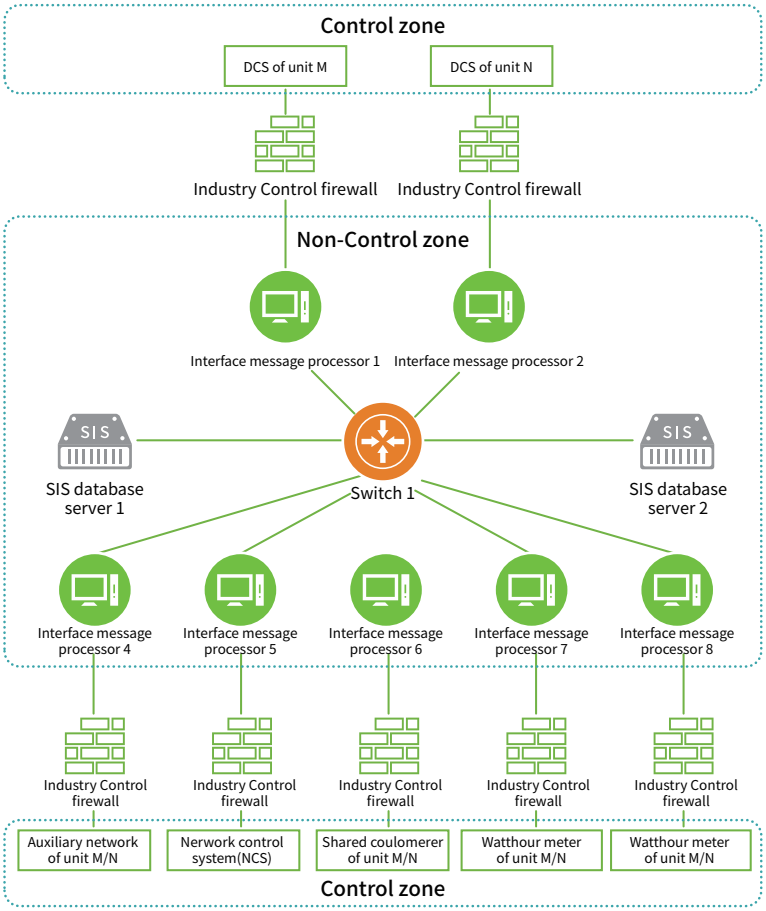


Figure 4.3 Horizontal border protection of the SIS system of unit M/N

As shown in Figure 4.3, the SIS interface message processors, which connect to the DCS of unit M, DCS of unit N, auxiliary network of unit M/N, network control system (NCS), are logically isolated by industrial control firewalls.

- Security protection between systems

According to No.14 Decree of the National Reform and Development Commission (NRDC), all subsystems of the electric power monitoring system should directly adopt the logical isolation technology, such as the VLAN or firewall technology. Each subsystem is logically isolated from other subsystems by using the VLAN technology, so as to meet the requirements for relatively independent connections between subsystems and system availability.

- Vertical border protection

Two sets of communication devices, which back up each other, are deployed respectively for the communication between the thermal power plant and the provincial power dispatch center. In addition, two independent vertical encryption devices are deployed between the access switch in security zone I and the egress router of the power dispatch center.

A vertical encryption authentication device is deployed between the thermal power plant and the centralized control center, so as to establish an encrypted tunnel between the plant and the centralized control center. The communication between the centralized control center and plant adopts the double gateway redundancy mode. Both the master fiber channel and backup channel of each communication gateway are equipped with a vertical encryption authentication device.

- Third-party protection

For thermal power enterprises with a third-party border (for example, they may need to communicate with departments of environmental protection), dedicated isolation devices for the power should be deployed for security protection of the same level.

4.1.1.3 Comprehensive Security Protection Solution

- Intrusion detection

According to NRDC's No. 14 Decree, a unified network intrusion detection system should be deployed in the production control zone. Appropriate rules should be configured for detecting intrusion behaviors hidden in normal information flows and analyzing potential threats.

The deployment of an intrusion detection system in the production control zone can not only meet

compliance requirements proposed in NRDC's No.14 Decree and National Energy Administration [2015] No. 36, but also be used to detect intrusion behaviors in the management zone and production zone boarders. APT attacks against industrial control networks are so destructive that they can even sweep from the management network to the production network by penetrating horizontal isolation devices. At the same time, the attacks spreading to the management zone from control systems in the production control zone should not be ignored. Therefore, industrial control network intrusion detection systems should be able to conduct bidirectional intrusion detection. In addition, since the switch of the SIS system does not support port mirroring, you can use a switch that supports port mirroring or use an externally connected switch that supports port mirroring for traffic mirroring.

- Reinforcing the host and network devices

According to NRDC's No.14 Decree, master servers of critical application systems (such as the plant-level information monitoring system of the power plant), communication gateways at network perimeters, and web servers should use secure and reinforced operation systems. Reinforcement methods include security configuration, security patches, using special software to enhance the access control capability of operating systems, and configuring secure applications. Configuration changes and patch installation should be tested first.

In the power monitoring system of a thermal power plant, industrial control terminals should be deployed on key hosts (such as the operator station, engineering station, historian, OPC server, communication machine, OPC interface message processor, and database server) and whitelist-based security policies should be used for security configuration. The deployed industrial control terminal security management and control system should be implemented together with the DCS system.

- Storage device and peripheral management

According to NRDC's No.14 Decree, the thermal power plant should strictly manage the use of peripheral devices (such as storage devices and printers) to prevent malicious code from entering the power monitoring system via such devices. Printers should be strictly managed by configuring the computer printer authentication function, so as to prevent unauthorized use. An O&M management and control system is deployed on the engineering station, operator station, and historian of important

control systems (such as the master DCS system) in the production control zone of the thermal power plant, in a bid to identify USB interface-based external devices (such as the USB flash drive, keyboard, and mouse). This system can be used to encrypt data, perform virus detection, and record switch messages and data, and supports query and traceback, thereby strictly controlling the use of external storage devices. The deployed O&M management and control system should not affect the running of systems in the production control zone.

- Security audit

According to NRDC's No.14 Decree, the thermal power plant can deploy an industrial control security alert platform (namely, the security audit probe) in independent subsystems of the electric power monitoring system for collecting network running log, running logs of the operating system, database access logs, running logs of business application systems, and running logs of security facilities. The plant should also deploy an industrial control security alert platform in the management information zone to receive audit data sent by the security audit probe for automatic analysis and early warning. The deployed industrial control security alert platform can be used as the man-machine interface of the protection technology for the electric power monitoring system to manage, analyze, alarm, and audit all information security products deployed within the industrial control network. The industrial control security alert platform is connected to the industrial control network as an independent workstation. Via the industrial control environment, centralized management and monitoring can be performed on this platform, together with the industrial firewall, industrial configuration software, industrial switch, system workstation (such as engineering station and operator station), industrial controllers (PLC, RTU, and DPU), and other industrial control devices, visualizing assets, behavior, traffic, and protocols in the industrial control network environment.

- Data backup

According to NRDC's No.14 Decree, critical business data should be backed up regularly and archived data should be stored remotely. The thermal power plant should use a storage device (such as a tape drive) to back up critical service data regularly and then put the storage media (such as a tape) for storing the archived data in a different place (such as a subordinate unit).

- Malicious code protection

According to NRDC's No.14 Decree, organizations should update signatures and view virus detection and removal records in time. The malicious code update file should be tested before installation. For the system workstation on which malicious code protection software has been installed, sharing a malicious code management server between the production control zone and the management information zone should be strictly prohibited. For the system workstations on which malicious code protection software has not been installed, the distributed control system (DCS) implemented by the vendor can be used for security protection.

4.1.2 Wind Power

4.1.2.1 System Introduction

Based on computers, communication devices, and test control units, the wind power monitoring system provides a basic platform for real-time data collection, switch status monitoring, and remote control of wind power plants. It can work with detection and controls devices to form an arbitrarily complex monitoring system. It plays a vital role in the monitoring of wind power plants by helping enterprises eliminate information silos, reduce operating costs, improve production efficiency, and accelerate the speed of responding to anomalies in the process of power transformation and distribution. Figure 4.4 shows its system architecture

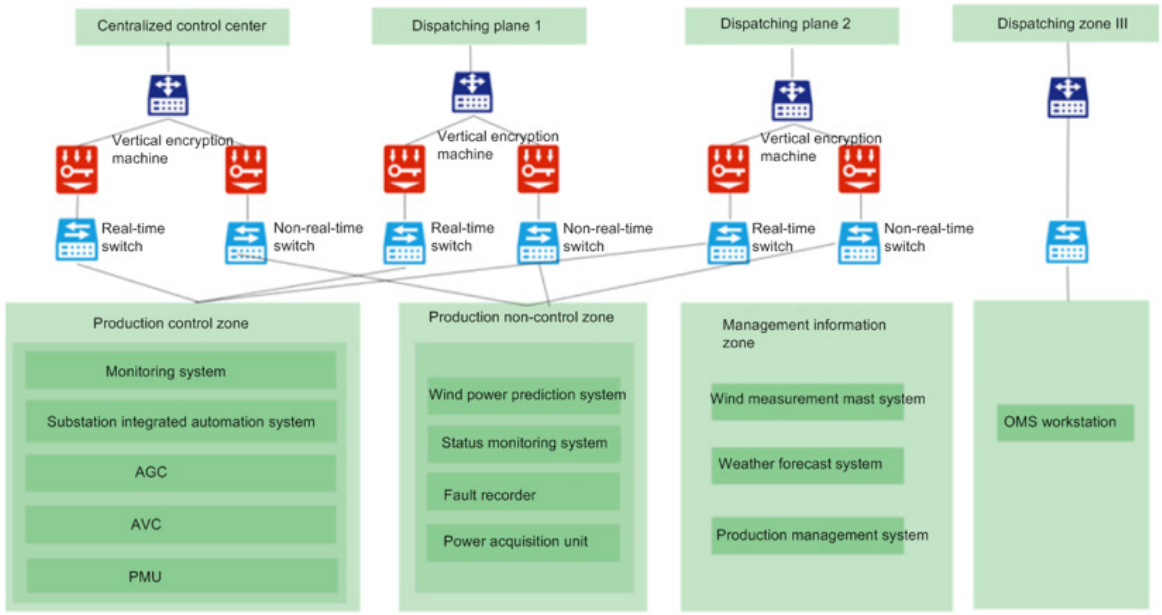


Figure 4.4 Logical architecture of the monitoring system of the wind power plant

Currently, the electric power monitoring system is vertically connected to dispatching planes 1 and 2 and the centralized control center of the wind power plant.

Security zones of the wind power plant are divided according to NRDC's No.14 Decree. The power station network is divided into the production control zone and management information zone. The production zone is subdivided into control zone (security zone I) and non-control zone (security zone II), depending on whether the control is real-time. The production control zone and dispatching planes 1 and 2 use a vertical encryption and authentication device for vertical authentication and encryption. The control and non-control zones are logically isolated and respectively connect to the first data network (plane 1) and second data network (plane 2).

According to NRDC's No.14 Decree, in the wind power plant, the monitoring system, substation integrated automation system, AGC, AVC, and PMU are put in the control zone; the wind power prediction system, status monitoring system, fault recorder, power acquisition unit are put in the non-control zone; separated networks are built for the management information zone and OMS workstation.

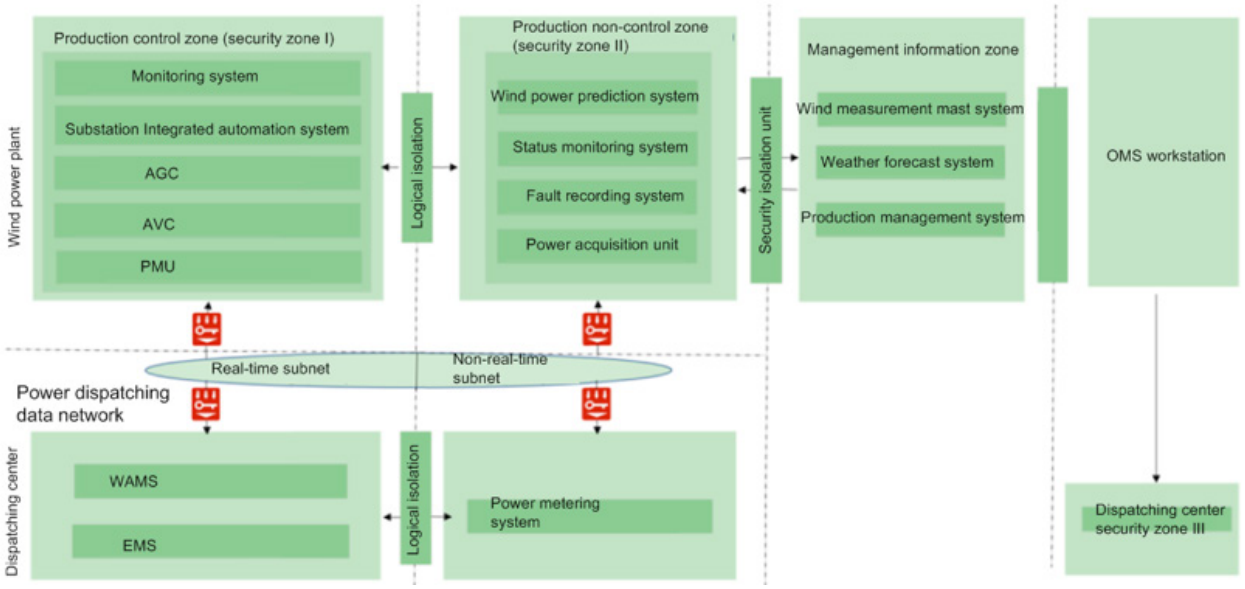


Figure 4.5 Security zones of the monitoring system of the wind power plant

4.1.2.2 System Protection Solutions

Border Protection Solution

- orizontal border protection

According to NRDC's No.14 Decree, a dedicated horizontal electric security isolation device is deployed between the production control zone and the management information zone of the wind power plant. Network devices and firewalls should be deployed for access control between the control zone (security zone I) and non-control zone (security zone II), so as to achieve logical isolation, packet filtering, and access control. According to the data access direction, a forward or backward security isolation device should be deployed between the production control zone and the management information zone. All subsystems of the electric power monitoring system should adopt the logical isolation technology, such as the VLAN or firewall technology.

- Vertical border protection

According to NRDC's No.14 Decree, a vertical encryption authentication device should be deployed for

the wind power monitoring system for remote communication, so as to realize bidirectional identity authentication, data encryption, and access control.

- Third-party border protection

According to NRDC's No.14 Decree, a firewall should be deployed between the monitoring system management zone and external network, ensuring the border security and data transmission security. A security gateway (firewall) should be deployed between the information management zone and external network perimeter and between the OMS workstation and the dispatching zone III.

Comprehensive solution

- Intrusion detection

According to NRDC's No.14 Decree, intrusion detection systems should be deployed respectively for the production control zone (security zone I), non-control zone (security zone II), and OMS workstation aggregation switch. Proper rules should be configured for detecting intrusion behaviors hidden in normal information flows, analyzing potential threats, and security audit. Intrusion detection systems are deployed in out-of-path mode. They only receive and analyze the data mirrored by the switch, but do not forward data.

- Reinforcing the host and network device

According to NRDC's No.14 Decree, master servers of critical application systems (such as the plant-level information monitoring system of the wind power plant), communication gateways at network perimeters, and web servers should use secure and reinforced operation systems. Reinforcement methods include security configuration, security patches, using special software to enhance the access control capability of operating systems, and configuring secure applications. Configuration changes and patch installation should be tested first. The host security reinforcement software is adopted in the process of reinforcing the monitoring system of the wind power plant. Reinforcement software should be available in Windows and Linux editions.

- Storage device and peripheral management

According to NRDC's No.14 Decree, the wind power plant should strictly manage the use of peripheral

devices (such as storage devices and printers), so as to prevent malware from entering the power monitoring system via such devices. The host security reinforcement software can be deployed to identify USB interface-based external devices (such as the USB flash drive, keyboard, and mouse).

- Security audit

According to NRDC's No.14 Decree, the monitoring system in the production control zone should have the security audit function, so as to record and analyze important operations on operating systems, databases, and service applications, thereby discovering violations, viruses, and hackers' attack behaviors. After a user logs in to the system, his/her operation behaviors should be strictly audited. Network running log, running logs of the operating system, database access logs, running logs of business application systems, and running logs of security facilities should be collected in a centralized mode and automatically analyzed.

- Data backup

According to NRDC's No.14 Decree, critical service data should be backed up regularly and archived data should be stored remotely. Key applications, software, configuration files should be backed up regularly.

- Malicious code protection

According to NRDC's No.14 Decree, organizations should update signatures and view virus detection and removal records in time. The malicious code update file should be tested before installation. Sharing a malicious code management server between the production control zone and the management information zone should be strictly prohibited. An antivirus management server should be deployed in the production control zone and antivirus software should be deployed on Linux and Windows hosts in the production control zone. The antivirus management server can be used to manage and upgrade antivirus software in a centralized mode.

4.1.3 Hydropower

4.1.3.1 System Introduction

The computer monitoring system of the hydropower plant adopts a hierarchical distributed open system structure totally controlled by the computer, which consists of the main control layer of functions and the local control unit (LCU) layer of objects. The main control layer consists of the operator station, data server station, external communication station, internal communication station, engineering station, voice alert station, GPS time synchronization system, UPS power supply, and network devices.

The main control layer collects all types of data reflecting the running status and parameters of main devices from the LCU layer in real time (such as communication value, analog value, impulse value, AC volume, polling data, and interrupt signals), monitors and manages main plant devices in a centralized mode (including device adjustment and control, working condition conversion, parameter setting, and maloperation-proof output lockout, alert records, historical query, event sequence record, accident recall, temperature trend alert and analysis, voice event alert, picture soft copy, statistical production report generation, and system database management), so as to enable advanced applications such as AGC and AVC.

As the underlying control device of the monitoring system, LCU mainly completes the collection and pre-processing of all types of data, sends the collected data and alert information to the main control server, and checks the validity of the data and then executes them as directed by the main control server. When the main control server fails or exits, LCU still runs properly and performs basic monitoring functions on devices, such as data collection, processing and device running monitoring, device adjustment and control, working condition conversion, and parameter setting, event sequence record, hardware self-diagnosis, and online diagnosis and alert.

4.1.3.2 Risk Analysis

1. Network security risk

① Insufficient protection of network borders. Although there is no direct physical network connection between the production control zone and the management information zone of the hydropower plant, protection measures for the border between the real-time and non-real-time systems in the production control zone are insufficient. Such measures do not support industrial protocols and

protection against industrial viruses.

② No protection for the access zone. In the production industrial control system of the hydropower plant, wireless communication via microwave is adopted between the backend and the front-end test control station of the hydrological system in the non-real-time zone. There is no security protection device at the receiving end for protecting wireless data inputs.

③ No intrusion detection protection management mechanism. The lack of intrusion detection devices at key network nodes in the production management zone, real-time zone, and non-real-time zone of the hydropower plant makes it impossible to effectively detect attacks, prevent or restrict internal and external network attack behaviors, or analyze network behaviors.

2. Host security risk

Lack of malicious code/virus protection mechanism. The host in the power monitoring system has no malicious code prevention platform or other compensation mechanisms to control and manage malicious code.

3. Application security risk

Lack of account management and authentication. At present, the hydropower plant has set up corresponding privileged accounts for each system according to positions and levels. However, no necessary application security control policies are available for performing authentication, access control, and security audit for user logins, system resources access, and other operations.

4. System O&M security risk

① Lack of security management and control for mobile media. No management and control platform is deployed for USB interfaces of the devices in the electric power monitoring system.

② Lack of monitoring audit of the information system. At present, the hydropower plant can monitor the electric power monitoring system, but it cannot monitor and audit upper computers, servers, operating systems, and databases and is unable to monitor security devices in the electric power monitoring system.

③ Lack of protection for important control devices. At present, the hydropower plant has not deployed

protection devices with the function of industrial protocol-based in-depth packet detection on the frontend PLC of each control system to prevent unauthorized operations on and intrusion against the controller.

4.1.3.3 Security Protection Solution

1. Replace the existing traditional firewalls with industrial firewalls, deploy intelligent protection devices between the LCU switch and the core switch of the monitoring system, deploy a unidirectional isolation device on the link for receiving telemetry data of the hydrological system, and deploy intrusion prevention and vulnerability scanning devices before the egresses of the management information zone and the Internet.
2. Strengthen the host in the industrial control system; deploy industrial control terminal protection software on the upper computer of the monitoring system, upper computer of the hydrological system, upper computer of the gate monitoring system, industrial television workstation, and power metering sub-station; use the terminal management and control platform for unified management; deploy USB protection devices on the upper computer of the engineering station in the monitoring system, hydrological system, and gate monitoring system.
3. Deploy a monitoring and audit device and build an online monitoring and audit platform dedicated for hydropower plants. The monitoring and audit device is deployed in out-of-path mode on one side of the core switch at the monitoring layer in the production control zone, so as to audit and monitor production control operations and threat traffic. It has the following functions:

   Provide the overall running status of the entire control network, automatically identify network devices, display the current status of network devices, and conduct comprehensive analysis of network performance;

   Monitor all packets passing through important network nodes or zones of the industrial control system; conduct in-depth analysis of packets and analyze whether there is an external intrusion or maloperation in the case of any abnormal or illegal packets;

   Remind onsite operators by generating an alert in the case of any anomalies.

4.1.4 Nuclear Power

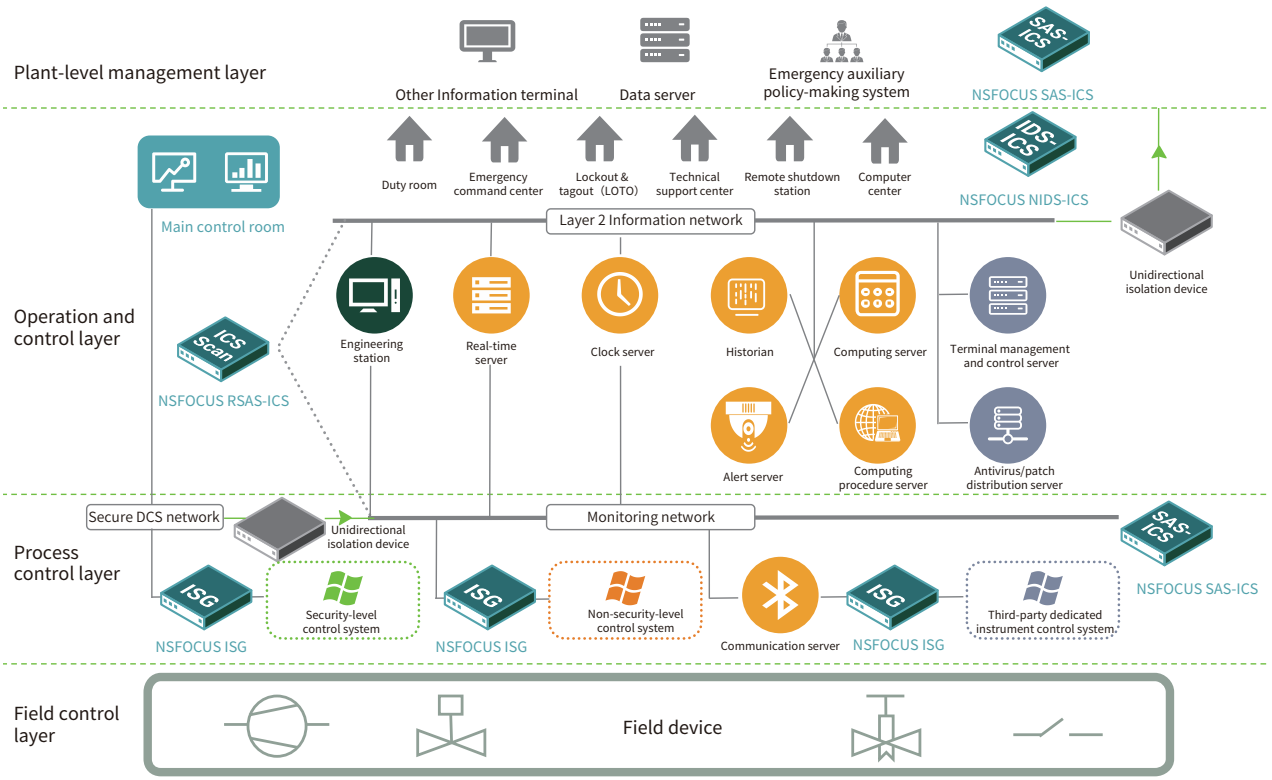


Figure 4.6 Security protection of a nuclear power plant

The security scenario of the nuclear power plant is similar to that of the thermal power platform. For details, sees section 4.1.1. Generally, it contains the following contents:

Security threat detection: An industrial control vulnerability scanning system is deployed to scan vulnerabilities in the operating system and applications in the SCADA/HMI.

Network border protection: unidirectional Isolation devices are deployed between the layer 2 information network and the plant-level management layer and between the security-level control system and non-security-level control system for unidirectional data transmission. Industrial security gateways are deployed between the monitoring network and the field control layer and between the monitoring network and third-party dedicated instrument control system, so as to block virus

propagation and hacker attacks from the monitoring network, prevent unauthorized operations, and avoid impact on the control network and damage to the production process.

Internal network monitoring: An industrial control intrusion detection system is deployed on the layer 2 information network and an abnormal behavior audit system is deployed on the monitoring network. Both systems are deployed in out-of-path mode, in a bid to accurately detect abnormal network traffic, discover potential network attacks and abnormal behaviors by means of in-depth analysis of industrial control protocols, and then generate alerts immediately.

Host security reinforcement: The host security should be reinforced by configuring security settings, such as account privilege, password policy, system service, patch update, and log management. According to nuclear service requirements and related information security standards, baselines should be configured for various host assets, and an industrial control benchmark verification system should be deployed to conduct regular security configuration audits.

Comprehensive terminal management and control: An industrial control terminal management and control system should be deployed on the host terminal to implement strict control access, status monitoring, process monitoring, virus protection, patch upgrade, malicious code monitoring, operation behavior audits, and whitelist-based application management and control.

4.2 Manufacturing Sector

4.2.1 Tobacco Industry

4.2.1.1 System Introduction

4.2.1.1.1 Network Architecture of a Cigarette Factory

The network architecture of a cigarette factory consists of the production network and management network, as shown in Figure 4.7.

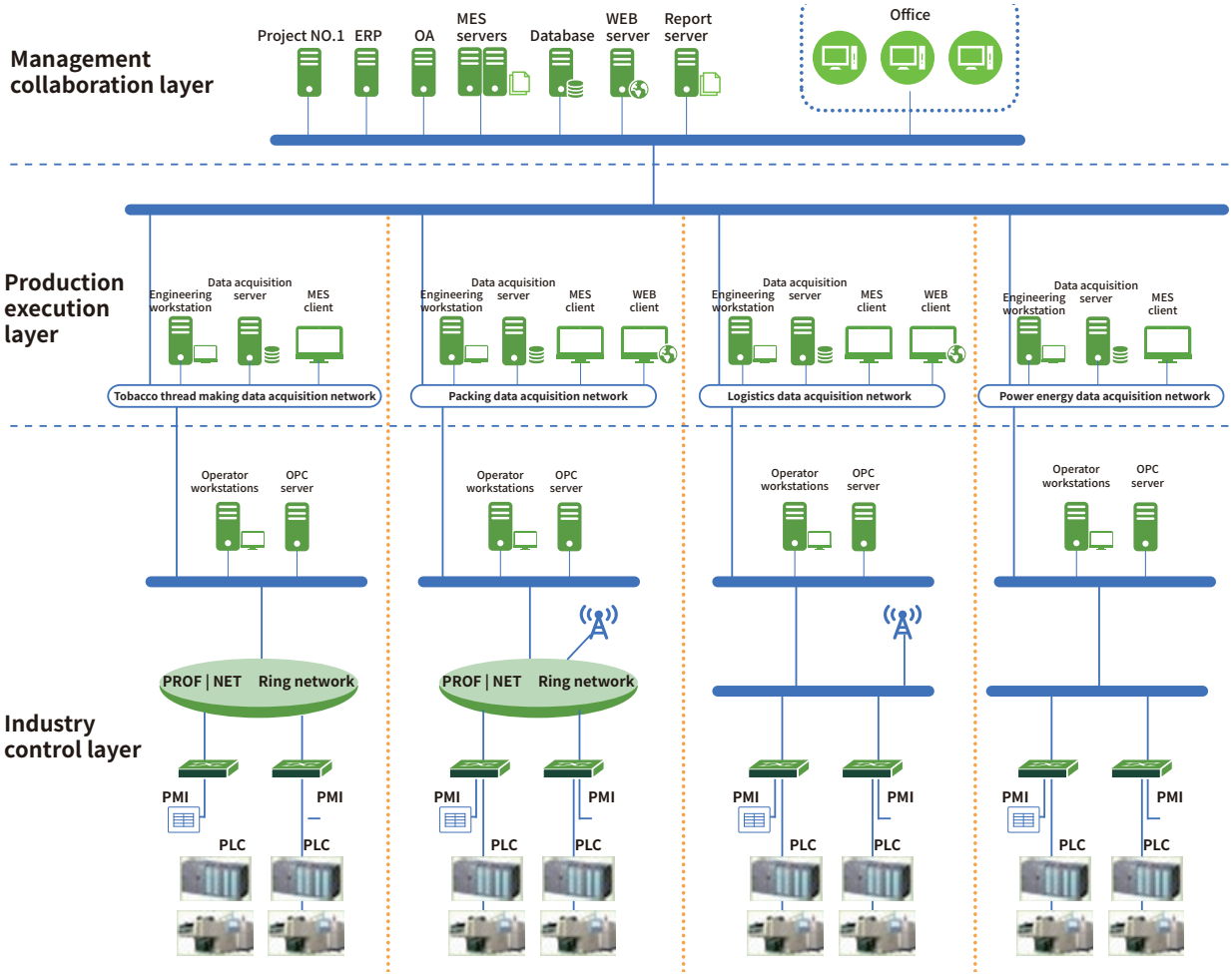


Figure 4.7 Network architecture of a cigarette factory

At the top level, the management collaboration layer information system is responsible for the enterprise's internal operation and management and control, facilitating business collaboration between an industrial enterprise and its upstream and downstream enterprises. Its key application system is the enterprise resource planning (ERP) system that integrates the enterprise logistics, information flows, and capital flows to facilitate the enterprise's operations, planning, controls, and performance appraisals. This system ensures smooth communication and facilitates effective collaboration between the cigarette production management department and the production execution department forming

an organic whole. This helps realize integrated management of production management information and production control information, integrated management of operation information and production information, integrated management of device resources and human resources, and achieve effective control and governance of enterprise production and operation management. Other application systems of the management collaboration layer include many subsystems, such as production management, financial management, quality management, workshop management, energy management, sales management, personnel management, equipment management, technology management, and integrated management subsystems. The management information system provides information service and decision support.

At the product execution layer, the manufacturing execution system (MES) is between the management coordination layer and the industrial control layer. In the production process of tobacco enterprises, the MES is an important bridge between production automation and IT-based management. It is mainly responsible for management execution for the upper production planning and scheduling for the lower protection control system, playing a key role in the two-way channels between the management collaboration layer and the industrial control layer. The data of the MES comes directly from the production process control system (PCS). The real-time data collected by the monitoring system and data acquisition system is processed to generate production process information for the MES's use. The MES is responsible for production planning and scheduling, resource (personnel and equipment) optimization and scheduling, material management, production quality control, process control, energy supply control, and production process monitoring as well as data integration and application like necessary data and information conversions.

Directly oriented to cigarette machines, the industrial control layer is responsible for collecting real-time production data generated by the automatic control system of various cigarette production devices and receiving control instructions (such as production operations) issued by the MES. The production control system of the tobacco industry refers to such production systems as the tobacco treatment line, rolling and packaging, power energy center, and logistics center of the production workshop. It is mainly responsible for processing, test and manipulation, and operation management.

4.2.1.1.2 Security Issues Facing the Cigarette Factory

Security issues facing the cigarette factory are mainly from the network and communication layer, and the controller, host and application layer.

- Security issues of the network and communication layer:

1. The security isolation mechanism between the production network and the management network are improper.

Currently, security isolation mechanisms between the production network and the management network include the following:

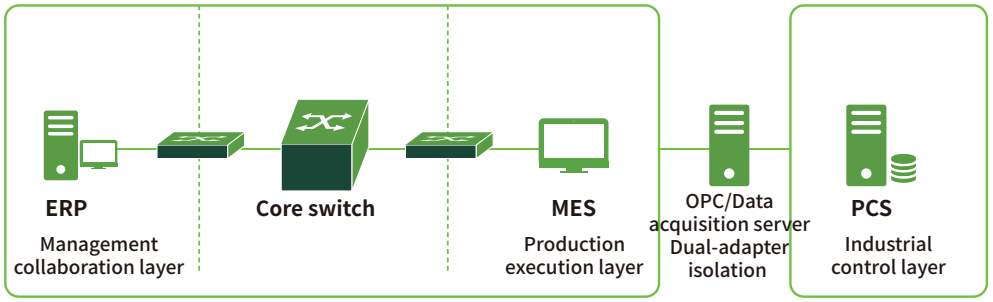


Figure 4.8 Dual-adapter isolation of the data acquisition server or OPC server

As shown in Figure 4.8, the access control mechanism features double adapters installed on the data acquisition server or OPC server. One adapter communicates with the management network and the other with the production network. These two adapters are on different network segments. Access control policies are configured on the server (and front-end switching device at the production execution layer) to isolate the management network and production network.

Since the data acquisition server or OPC server is in both the production network and management network at the same time, the dual-adapter isolation method has a risk of unauthorized access and data transmission between the production network and the management network.

In addition, the data acquisition server or OPC server in the dual-adapter mechanism has been exposed to the management network (which is possibly connected to the Internet), and therefore it is at the risk

of being scanned and attacked. Furthermore, the server is interoperable with the internal production network. If the server is infected by a virus in the management network, the virus will spread to the industrial control system of the production network, directly affecting the production.

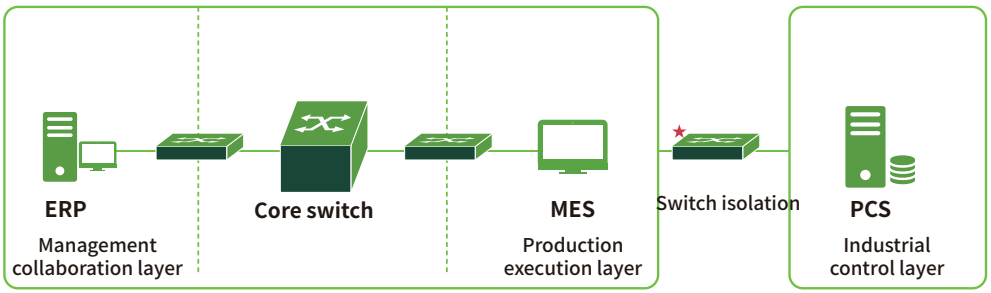


Figure 4.9 Switch isolation

This access control mechanism is implemented only via a switch device connecting the management network and production network and by configuring an ACL policy specifying who are allowed to directly access production network devices. Generally, only specified network administrators can directly access these devices.

Although some switch devices also have control filtering functions (such as an access control list on the firewall), they cannot defend against network attacks like professional firewalls and do not have the dynamic packet filtering function. Therefore, if a switch device is used as a substitute of professional security isolation devices (such as firewalls), the attack and intrusion risk remain quite high.

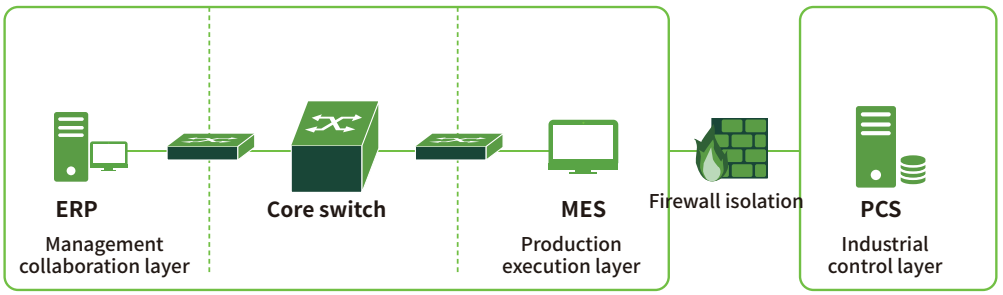


Figure 4.10 Firewall isolation

So far, some cigarette manufacturers with proper good network structure planning have built a security isolation mechanism between the management network and the production network, most of which use

professional firewalls for access control and attack defense. However, due to inconsistent standards and specifications for firewall security policies, some traditional firewalls only support access control and packet filtering but not support security audits or malicious behavior identification. Such firewalls even cannot identify industrial Ethernet control protocol-based (such as OPC, ProfiNet/ProfiBus, and ModBus) packets. Therefore, this isolation method has limitations.

2. Control command data is transmitted in plaintext.

The transmitted data mainly includes communication data within the management network and industrial control commands (such as ProfiNet/ProfiBus, ModBus, and DNP3).

3. The management and control mechanism for the wireless network in the production network is absent or incomplete.

For example, the Automated Guided Vehicle (AVG). It consists of the wireless access point (AP), configuration software of the master device, and in-vehicle PLC. Wi-Fi is adopted for communication between the controller and the in-vehicle PLC.

4.The configuration of network device security is incomplete.

Most network devices on the production network are managed by the workshop system administrator (not security administrator) who leaves the configuration at default values. Therefore, these devices are at a high risk of unauthorized access or attack.

5.The industrial control security audit mechanism is absent.

As there is no audit management of O&M personnel's daily operation and maintenance of the industrial control network, it is impossible to trace human factors for abnormal events in the cigarette production business and find the root cause. As a result, no qualitative analysis can be carried out.

- Security issues of the host and application player:

1.The ICS contains a lot of vulnerabilities.

Currently, the mainstream brands of ICSs in the tobacco industry are Siemens S7 series PLC, Rockwell AB PLC, and GE PLC. These devices are usually prone to such vulnerabilities as the denial-of-

service vulnerability, buffer overflow vulnerability, information disclosure vulnerability, remote control vulnerability, and privilege escalation vulnerability. Exploitation of these vulnerabilities could cause service interruption, sensitive information (such as the production plan and process of cigarette manufacturing enterprises) theft, and control of an ICS, thereby disturbing and damaging the normal production or operation activities of the cigarette factory.

2. The HMI identity authentication mechanism for key production devices is incomplete.

The login identity authentication mechanism for the touch screen HMI of the front-end onsite operation in the PLC of some cigarette manufacturing enterprises is incomplete. Weak passwords or no authentication, together with the absence of supervision and monitoring mechanism, lead to the possibility of unauthorized operations on associated production devices.

3.There is no security reinforcement mechanism for the engineering workstation, operator workstation, and monitoring terminal.

Generally, the engineering workstation, operator workstation, and monitoring terminal of cigarette manufacturing enterprises use Windows systems, which have been running for many years without being patched. Since computers at the operator workstation can directly send production instructions to the ICS and monitor the production device status, vulnerabilities existing in the system increase the risk of ICSs being attacked (for example, after obtaining privileges, an attacker can dispatch arbitrary control commands).

4.Remote O&M operations on the key production device components, engineering workstation, operator workstation, and monitoring terminal.

The O&M and troubleshooting of key ICS PLCs are mainly locally performed. But the security isolation mechanism of some manufacturing enterprises is not incomplete, which makes it possible for remote access operations. For example, capabilities that enable maintenance engineers and vendors to remotely access the system should be under security control, so as to prevent unauthorized individuals from remotely accessing the production network.

In addition, local access operations on the engineering workstation, operator workstation, and

monitoring terminal should be done in the central control room, and remote O&M management should be prohibited. However, port 3389 on most terminals for remote desktop is not disabled and remote login operations are allowed for the convenience of daily O&M, which allows attackers to obtain the highest system privileges, send arbitrary commands to the controller (PLC), and launch a malicious attack against production devices.

5.There is no malicious code detection mechanism for the engineering workstation, operator workstation, and production network business system server.

In some cigarette manufacturing enterprises, due to the compatibility issue between the industrial control application software on the engineering workstation, operation workstation, and monitoring terminal, and antivirus software, antivirus software is not installed, which leaves room for the infection and spreading of viruses and malicious code. In order not to affect the production availability, antivirus software is not installed for data acquisition servers and web servers. Even if antivirus software is installed, the virus library has probably not been updated for years.

6.The identity authentication mechanism for the engineering workstation, operator workstation, and monitoring terminal system is incomplete.

For the convenience of daily O&M, some cigarette manufacturers use a public account (even default account) for the operator workstation and monitoring terminal in the central control room and the system operating interface is always open, with no idle lockout function. As a result, all personnel entering the central control room can perform operations, making it possible for unauthorized operations. This is to say, arbitrary operations on the workshop PLC are allowed and it is impossible to find out who is responsible for a security event.

7.The division of IP address segments in the production network is improper.

In some cigarette manufacturing enterprises, office computers and business servers on the production network are planned in the same IP network segment, which may lead to conflicts between the IP addresses of third-party computers on the production network and those of business servers on the production network, and lead to the security risk of system interruption.

8. Management and control measures for mobile devices in the production network are incomplete.

Some cigarette manufacturers do not physically disable USB interfaces of production devices on the industrial control network or strictly control USB-based mobile storage media of production network employees, bringing a risk of exposing the production network to virus infection.

In addition, the unauthorized connection of insecure mobile devices (such as laptops) also facilitates the spreading of malicious code (such as trojans and viruses) in the production.

9. Permissions of the business system and database account are improperly configured.

For the MES, a core business system of cigarette manufacturer, login accounts are granted privileges based on roles. However, the process of applying for privileges in most cigarette manufacturers is not well executed. For example, a workshop employee can apply to the system administrator from the information management department via telephone and then the system administrator contacts the onsite O&M personnel from the vendor to change account rights, with no approval record. A workshop employee can also directly apply to O&M personnel of the vendor via telephone. Permissions will be immediately assigned without any confirmation or approval. For workshop data acquisition servers, some enterprises do not differentiate account privileges or simply use the default user name and password without setting a password protection policy. Attackers could obtain the database privileges, and corrupt and tamper with the production database at will.

10. No backup is available for configuration files of key devices.

There is no storage and backup mechanism for configuration files of key devices on the production network, making it impossible to respond to accidents, such as employees' maloperation or attackers' changing configuration files, thereby causing service interruption or production data loss.

4.2.1.2 System Security Protection Solutions

4.2.1.2.1 Border Security Protection Solution

The production network is the core security zone of cigarette manufacturers, mainly including the business system and devices used for cigarette production. According to the workshop scale, the

production network can be subdivided into four sub-zones, namely, the energy access zone, packaging access zone, logistics access zone, and power energy access zone. The production network is hierarchically built and divided into different security zones. Its security isolation mechanisms for security domains is as follows:

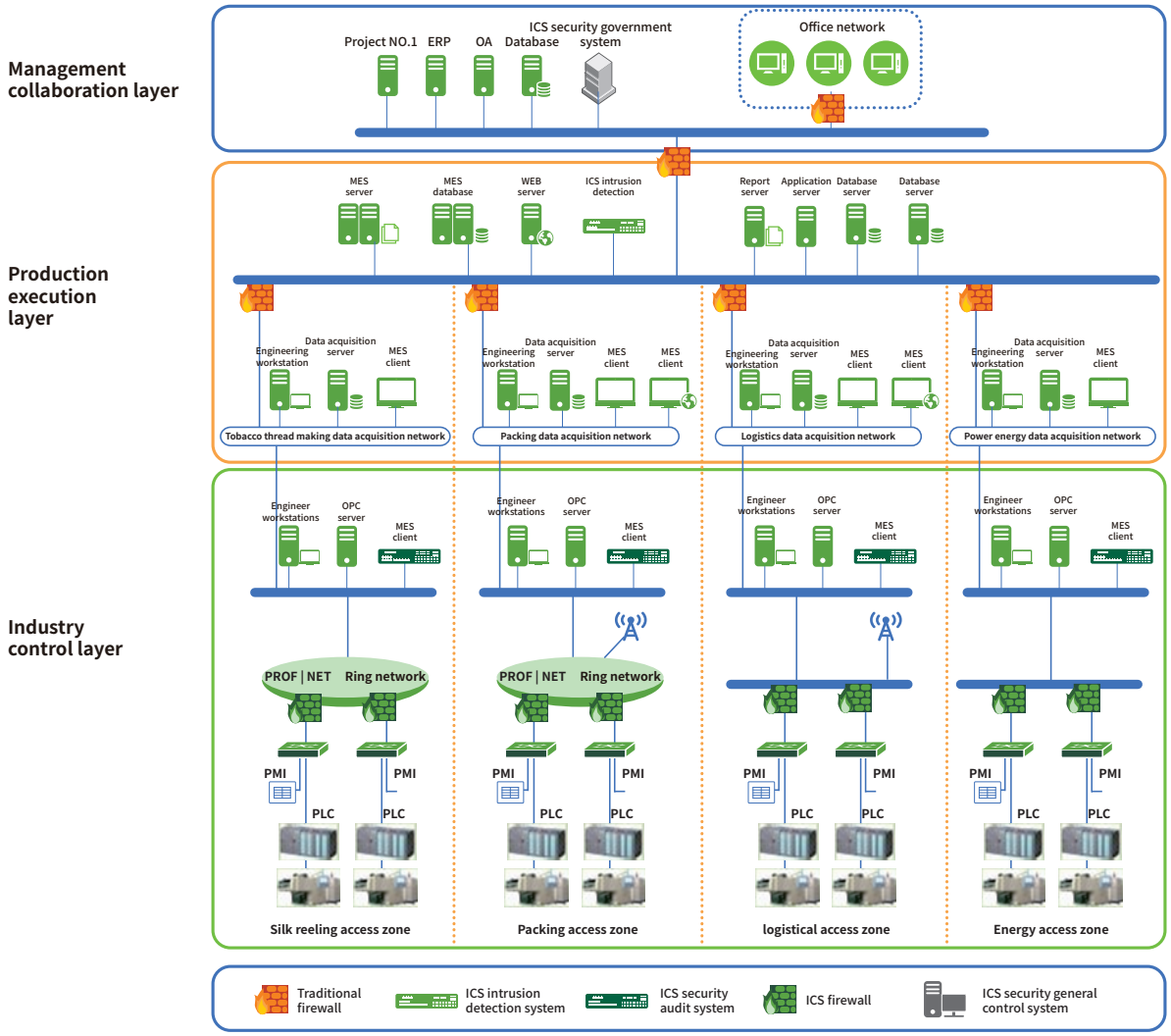


Figure 4.11 Security protection of a cigarette factory

At the management collaboration layer outside the production network, the access control among the production execution layer is provided by traditional firewalls, including access control, address translation, application proxy, event audit, and alert functions. However, within the industrial control layer of each cigarette manufacturer, in the ring network and at cigarette device nodes of the bus network, professional industrial control firewalls dedicated for industrial control network environments are required. The reason is that, in this scenario, we need to identify industrial control protocol-based packets, and parse and check the content of industrial network protocols and application data. In addition to the basic access control function of traditional firewalls, industrial control firewalls can conduct fine-grained check and in-depth filtering for common industrial protocols-based (such as Modbus and OPC) packets, so as to block the spreading of viruses and hacker attacks from the management network, thereby preventing any impact exerted on the production network and production services.

4.2.1.2.2 Comprehensive Security Protection Solution

- Security audit

By effectively identifying the operation instructions based on IEC 60870-5-101, 102 and 104 protocols, IEC 61850, MODBUSRTU, and PROFINET protocols, the ICS security audit system can effectively audit the instruction information transmitted between the central control room and dispatching center of the cigarette factory, with the purpose of checking whether operation instructions conform to the preconfigured audit rules. If any malicious operations or maloperation instructions are found, the audit device will generate an alert promptly. In addition, in the traceback process, the audit device can be used for after-event inspection by rebuilding event and system conditions and generating a report, which provides an effective basis for after-event analysis.

- ICS security general control platform

The unified and centralized control of security is the direction of information security construction during the Thirteenth Five-Year Plan specified in the blueprint of "CT-155" industry information architecture. The building of ICS security-based unified management and control platform will be a

trend. Centralized management and control measures in the production network are mainly to monitor log information of industrial equipment and upload such data to the integrated management and control platform of the industrial control security. Through the comprehensive evaluation of the system security risk situation, these measures can be used to monitor all types of log alert information on ICS devices on the production network and generate alert information. The workshop system O&M personnel can monitor, analyze, and diagnose threats by setting, screening, and analyzing monitoring alerts. At the same time, the platform can collect statistics on, analyze and evaluate alarm events according to the requirements proposed by the workshop system O&M personnel, and display statistical results and development trends of various events.

- System security assessment before going live

At present, in cigarette factories, there is no management mechanism for PLC networking and going-live. This is an important stage in security lifecycle of the entire ICS and provides the best opportunity for the system owner and operator to learn about the security risk level. Therefore, the top priority of security assessment before system going-live is to analyze the security of the ICS and detect potential vulnerabilities existing in the system based on the system going-live process and overall acceptance requirements. Then, it is to contact the providers of the corresponding industrial equipment and system to obtain related mitigations for the detected vulnerabilities. Vulnerability detection mainly includes scanning of known vulnerabilities and active vulnerability discovery (FUZZ technology).

4.2.2 Automobile Manufacturing

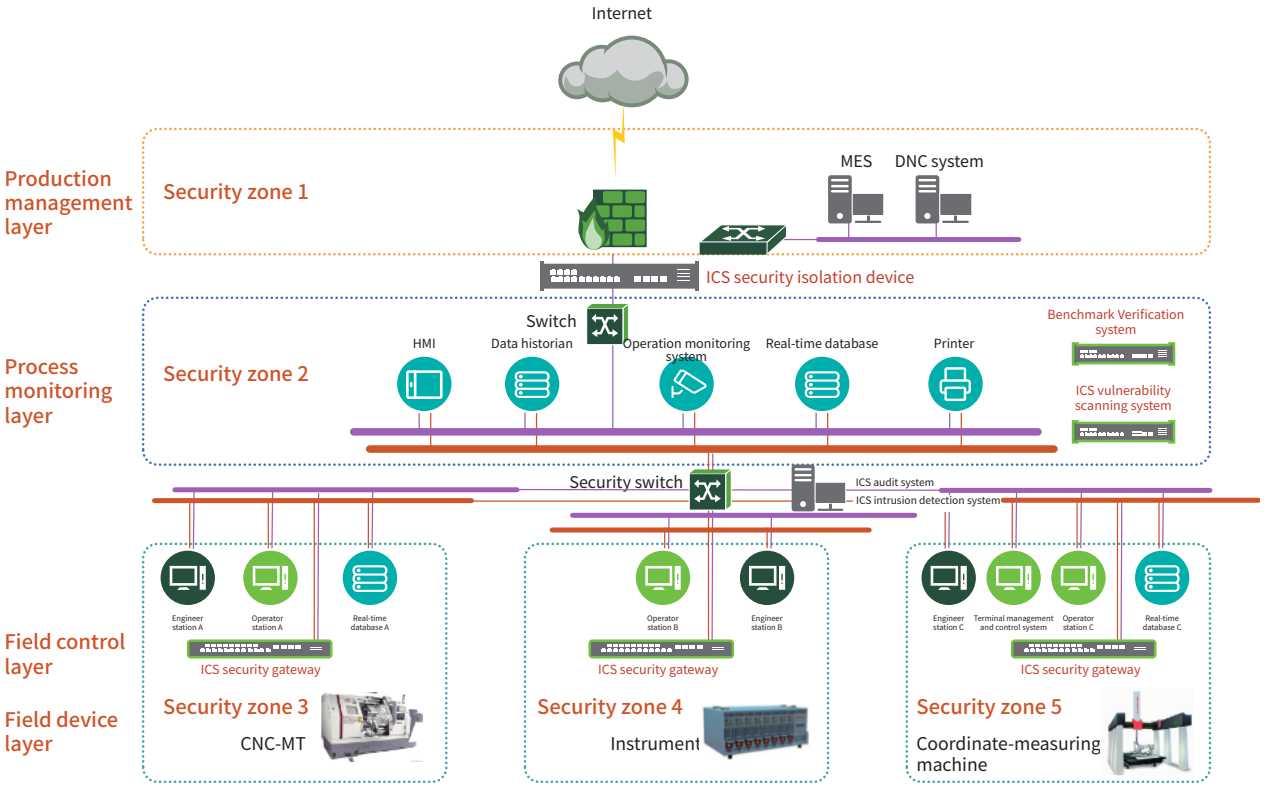


Figure 4.12 Security protection of an automobile factory

- External border isolation and monitoring. The external border refers to the border between the ICS area and the IT area, that is, security zones 1 and 2 shown in the preceding figure. An ICS security gateway can be deployed at the external border as the first line of protection for preventing external threats from entering the ICS environment.
- An industrial control security gateway can be deployed at the boundary of each security zone in the industrial environment, forming a defense-in-depth structure to strictly control communication. ICS gateways are respectively deployed at borders between security zones 3 security zones 4 and 2, and security zones 5 and 2.
- An ICS audit system is deployed in security zone 2 for auditing traffic and operations and monitoring

the running status and logs of all distributed industrial devices in the industrial control environment in a centralized mode.

- An ICS vulnerability scanning system and ICS benchmark verification system are deployed in security zone 2 to assist vulnerability management in the O&M process.
- A terminal management and control system is deployed for all IT servers and PCs in the industrial control environment for peripheral management and control, process management and control, and malicious code prevention.
- If the vendor's remote O&M of automatic devices is required, a VPN or CA authentication system needs to be deployed to identify remote O&M personnel, thereby improving the credibility authentication of remote access to the industrial network.

4.3 Government Affairs

4.3.1 Water Affairs

4.3.1.1 SCADA System Architecture Used in Water Affairs

The SCADA system used in water affairs mainly consists of the operator workstation, engineering workstation, SCADA system of the water intake pump room, SCADA system of the drug dosing room, SCADA system of the backwashing system, SCADA system of the water supply pump room, and SCADA system of the dewatering pump room. Figure 4.13 shows the architecture.

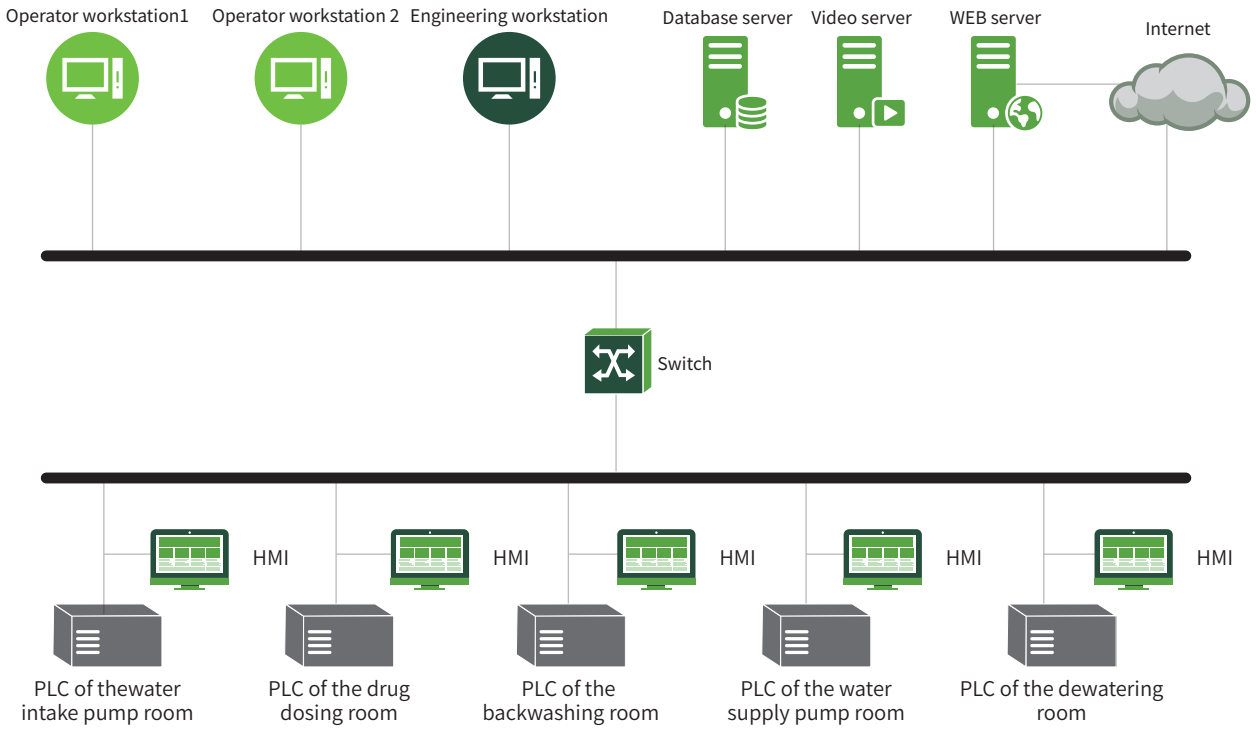


Figure 4.13 Architecture of a water factory

4.3.1.2 Security Requirement Analysis

1. Portal website security analysis

Since the portal website of water affairs can be directly visited via the Internet, it has different kinds of visitors from both within and outside of China and can easily draw hackers' attention. Main security threats are:

① By launching an SQL injection or cross-site scripting (XSS) attack, a hacker can easily obtain administrative privileges of the portal website and then further tamper with its web page code. The hacker can replace the portal website with a phishing website or pornographic website, or publish sensitive remarks on the web page, causing an extremely reverse impact to the enterprise.

② After successfully obtaining control privileges of the web server, the attacker can use the server as a

springboard to penetrate and scan the intranet or even launch an attack against the intranet, posing threats to the enterprise's sensitive data. According to the security assessment result of the current host, after a hacker enters the intranet, he/she can easily comprise other servers.

Traditional border protection devices such as firewalls and intrusion prevention systems, though taken as indispensable modules to implement overall security policies, are unable to provide satisfactory protection against web application attacks due to their own product positioning and protection depth. Therefore, it is necessary to adopt a professional web protection system to effectively prevent various attacks and reduce website security risks.

2.Network border security analysis

The computer network itself is so vulnerable that it may suffer different attacks and damage at any time, some of which are even destructive. Main factors that damage network security are as follows:

① Network protocols are, by nature, insecure. The network is an open information system, which can connect to the Internet and communicate with any computers on the network. The network is at risk due to the vulnerability of the TCP/IP protocol.

② Virus worms spread rapidly. Once the intranet of water affairs is infected with viruses or worms, it will degrade the processing performances of the network and system, seriously threaten sensitive data, and even congest the network and cause service interruption.

③ Weaknesses of current firewall solutions. In such a situation where network applications and new threats spring up like mushrooms, either traditional firewalls or unified threat management (UTM) devices, or next-generation firewalls (NF) can no longer meet users' requirements for network security protection. Specifically, traditional firewalls cannot effectively identify and control network applications and users, and current IP address-based access control is not reliable any more.

3.Business system security analysis

The security analysis of the business system evolves with the development of network environments. The work such as order management and file distribution in the system of water affairs is now done by computers and information storage and provision are performed in a digital way. Main factors that damage the security of business systems are as follows:

① System vulnerabilities impose serious threats to the business system. Malicious attackers could exploit system vulnerabilities to enter the system background by conducting malicious scanning or launching remote overflow attacks, so as to obtain, tamper with, and even destroy sensitive data, influencing the proper running of the entire network.

② Network security auditing is an especially serious issue. Traditional network security means, such as firewalls and intrusion detection systems, can manage and monitor abnormal network behaviors (such as controlling the validity of network connection and access and monitoring network attack events), but they cannot monitor network content access and authorized internal network access. Therefore, they are unable to detect information disclosure events and network resource abuse caused via legitimate network access (such as instant messaging, forums, online videos, P2P downloads, and online games). Also, it is difficult to effectively monitor and manage content and behavior and trace the source of security events. Therefore, a new security method is urgently needed to address the preceding issues. Audit forensics are essential in any security systems.

③ Human errors and service privilege management problems, for example, weak passwords, incorrect sharing, misuse of application systems, internal personnel's unauthorized access to business application systems, unauthorized operations, or the operator's incorrect inputs that lead to system breakdown.

4.3.1.3 Security Solutions

1. Portal website protection

Use a web application protection system to ensure the security of web application systems. The web application protection system is an overall solution that features pre-event prevention, in-process protection, and post-event remediation. As a middleman between the web client and the server, the web application protection system can protect the web server from being directly exposed on the Internet, monitor bidirectional HTTP/HTTPS traffic, and detect and protect bidirectional data at the network layer and web server/application layer, thereby reducing the security risk of websites and preventing all kinds of bandwidth consumption and resource consumption DoS attacks.

2. Network border protection

Use a network intrusion prevention system to ensure the security of network borders. The security protection system of network borders can intelligently identify and analyze protocols, detect protocol anomalies, and detect abnormal traffic, and therefore can effectively discover various trojans and backdoors bound to any ports, detect unknown overflow attacks, zero-day attacks, and DoS attacks, and effectively defend against DDoS attacks, unknown worms, and rogue traffic attacks.

3. Network security audit

A security audit device should be deployed in the system of water affairs to fulfill the following functions:

① Content audit. It has in-depth content audit functions, so as to provide comprehensive content detection and information restoration for website access, mail receiving and sending, remote terminal access, database access, data transmission, and file sharing. It can also customize the keyword database for fine-grained audit tracking.

② Behavior audit. It has the comprehensive network behavior audit function. According to the configured behavior audit policy, it monitors network application behaviors (such as website access, mail receiving and receiving, database access, remote terminal access, file upload and download, instant messaging, forum, mobile application, online video, P2P download, and network game) and generates alerts and records events matching the policy in real time.

③ Traffic audit. It analyzes traffic based on protocol identification, collects statistics of various packet traffic in the network in real time, and comprehensively analyzes the traffic, so as to provide reliable support for making traffic management policies.

4.3.2 City Gas System

4.3.2.1 Overview

The SCADA system of the city gas system mainly consists of the dispatch control center, city gate, distribution station, unattended gas station, and important user monitoring points. The SCADA

system mainly consists of the dispatch control center, station control system, and data transmission communication system. The dispatch control center cooperates with substations. Figure 4.14 shows the architecture.

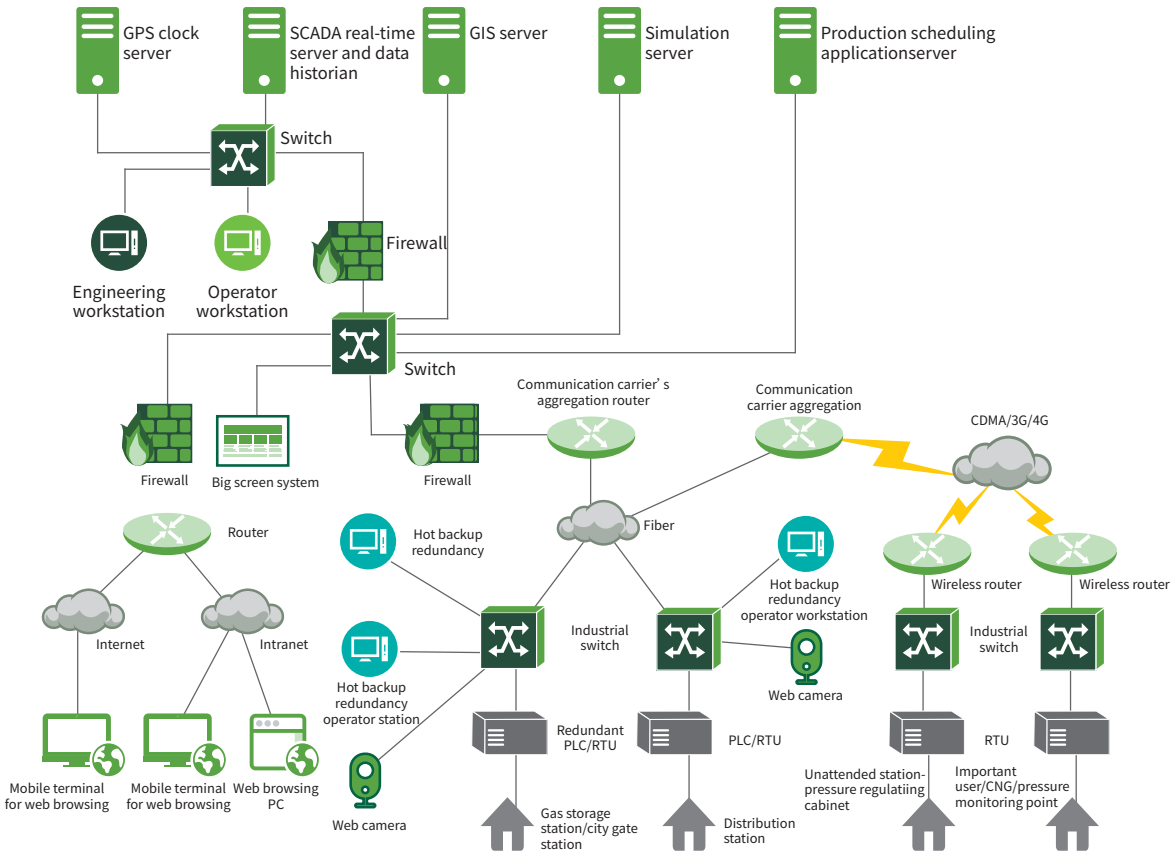


Figure 4.14 Security protection of the city gas system

Dispatch control center: According to the size of the SCADA system, dispatch control centers can be divided into the general dispatch control center, standby dispatch control center, and regional dispatch control center. They monitor important stations and remote control shut-off valve rooms of urban high- and medium-pressure gas pipeline networks, and monitor the monitoring points of medium-pressure pipeline networks, so as to optimize pipeline network running, make transportation plans, and conduct metering management.

Station control system: According to the distribution of pipeline networks and stations, station control systems of different sizes can be deployed at the city gate station, distribution station, pressure regulating station, and press monitoring points. Station control systems are remote monitoring stations of the SCADA system. They execute the commands dispatched by the primary dispatch control center to implement station data collecting and analyzing, interlocking protection, continuous control, monitoring of the device running status, and upload of all kinds of data and information collected to the primary dispatch control center.

4.3.2.2 Security Protection Solution

4.3.2.2.1 Border Security Protection Solution

An ICS security gateway can be deployed between each station control system PLC/RTU and the industrial switch, in a bid to prevent malicious traffic or attacks from entering field stations through a city gate station.

Before the SCADA server, engineering workstation, and operator workstation, an industrial firewall can be deployed to conduct in-depth analysis of all data destined for the server, protecting this server from unauthorized operations, malicious control of illegitimate commands, and virus attacks.

4.3.2.2.2 Comprehensive Security Protection Solution

- Divide security zones. The entire gas network system is divided into different security zones, with the purpose of conducting permission control for mutual access between the service system zone, accessing users, Internet egress, and core switch zone. The SCADA industrial control system zone is also divided. Improve the reliability of network security protection. Design a redundant architecture of key node devices in the core switch zone, mobile user access zone, and sensitive data access zone to form a hot backup, thereby ensuring the high reliability of the whole security protection system devices.
- Deploy a database audit system and clearly define data access permissions. By deploying a database audit system in the sensitive data zone, we can audit users' database operations in real time, including the creation, deletion, and modification of tables.

- Strengthen data protection. Deploy a data disclosure prevention system to ensure that confidential data will not be leaked in the production, transmission, and storage links, and that even if the data is duplicated, it cannot be accessed.
- Deploy a unified security management zone. After security protection measures are taken for the entire network system, effective management and O&M should follow. We can deploy the threat analysis system, vulnerability scanning system, and operation security management system (OSMS), which are effective for unified security management, and deploy ICS vulnerability scanning system, ICS security audit system, and ICS intrusion detection system in the central SCADA zone for security management of the entire SCADA industrial control system.

4.4 Petroleum and Petrochemical Industry

4.4.1 Oil and Gas Production

4.4.1.1 Overview

- System introduction

Oil field exploitation is field work featuring strong fluidity, large quantities of scattered points, and a long distance. In the process of oil field exploitation, out of management requirements, the oil and gas management center connects to the gathering and transportation control center, gas processing plant control center, gas transmission initial station, and field control layer through an industrial network. Therefore, the system needs a large number of wired and wireless networks for data transmission and remote system management.

- Overall network situation of oil and gas branches

The core network of the production network of oil and gas branch companies usually connects to their secondary units in different regions through a self-built optical cable. In terms of network redundant connections, each secondary unit deploys two routers as mutual backups, which respectively connect to the core of GMC and core of BGMC. The network communication is implemented via the OSPF protocol. Therefore, the entire production network forms a reliable architecture with high redundancy.

From the perspective of network links, GMC and BGMC of oil and gas branches connect their secondary units in different regions through a dedicated oil link, and the core router is used as a backup link of secondary units by satellite. Currently, for those geographically remote central stations or field stations without cables, satellites, wireless bridges, and 3G/4G are used for data transmission.

4.4.1.2 Protection Solutions for Industrial Control Network Security

4.4.1.2.1 Border Protection Solution

On the premise of ensuring the system availability, it is necessary to protect the industrial control system of the production network by "vertical layering and horizontal zoning".

- Division of security zones

"Vertical layering and horizontal zoning" is to vertically divide industrial control systems into four layers, namely, the field device layer, field control layer, supervisory control layer, and production management layer, and horizontally separate networks of each industrial control system, making them belong to different security zones.

- Vertical layering

According to the idea of information security protection of industrial control systems, each industrial control system should be in a separate zone. Detailed division is as follows:

① The office network and production network of the branch are two separate security zones, which are isolated via GAP.

② The security zone of the branch production network is subdivided into the branch GMC security zone, gas transmission DCC security zone (branch BGMC security zone), DCC security zone in region A, DCC security zone in region B, DCC security zone in region C, DCC security zone in region D, and DCC security zone in region E.

③ According to the preceding division, the branch production network is vertically divided into security zones by administrative level.

- Horizontal zoning

The branch company is divided into five layers by administrative level, with each layer containing multiple units. Horizontally, units of the same level are divided into different zones. A secondary unit is divided into seven horizontal zones, namely, five mines, one division, and one factory. Hydrologic institutes are isolated by dividing zones.

According to the idea of information security protection based on security zones, an industrial control system is divided into five zones at one layer, namely, the data server zone, security support zone, core switch zone, user access zone, and branch access zone. Hydrologic stations and lower-level units can select security zones as required.

The data server zone is mainly used to plan and deploy servers related to the industrial control production at this layer. Threats in this zone mainly come from internal personnel's overstepping and abusing power, internal personnel's maloperations, software and hardware failures, internal personnel's tampering with data, internal personnel's repudiation. Main protection methods include application and service development and maintenance security, application-based audits, identity authentication, and behavior audits. Auxiliary protection methods include anomaly detection and access control.

The security support zone is used to plan and deploy security O&M, security detection, and security management devices related to industrial control production at this layer. Threats in this zone mainly come from network transmission leakage, unauthorized access and abuse, internal personnel's repudiation. Protection methods include out-of-band management and network encryption, identity authentication and access control, and audits and tests.

The core switch zone is mainly used to plan and deploy core switch devices related to industrial control production at this layer. Threats in this zone mainly come from network device failures, network leakage, and physical environment threats. Protection methods include the availability (backup and redundancy), confidentiality (network transmission encryption), and integrity (network-based authentication) of the basic network.

The user access zone is mainly used to plan and deploy user terminals related to industrial control production at this layer. Threats in this zone come from internal personnel's malicious behavior and internal information disclosure. Main protection methods include terminal behavior control and access

control.

The branch access zone is mainly used to plan and deploy outreach devices related to industrial control production at this layer. Threats in this zone come from hacker attacks (external intrusion), malicious code (viruses and worms), and unauthorized access. Protection methods include access control (industrial control firewall), intrusion detection (IDS), and malicious code protection (antivirus).

4.4.1.2.2 Border Protection

In-depth protection security policies should be provided for branch industrial networks. Among these policies, border security protection is the most important link. It can not only ensure a strict control of access between networks, but also cut off the transmission paths of various viruses and malicious code, thereby guaranteeing the border security at all levels.

ICS firewalls are deployed at branch companies, gas transmission stations, secondary units, and between secondary units and hydrological stations. By deploying special firewalls applicable to industrial environments, configuring industrial protocol-based access control policies, combing the existing security policies of traditional firewalls in the network, and improving the granularity of packet filtering policies, we can combine industrial security protocol-based protection methods with traditional security policies and divide security zones according to security levels, so as to improve the capability of protecting borders, regions, and terminals, and effectively reduce the risk of network intrusion and security threat migration and spreading.

In the aspect of the overall network service structure, we can configure ACLs on core network devices, establish point-to-point, point-to-multipoint, and multipoint-to-point service access relationships, and forcibly regulate business data flow paths, thereby strengthening business process management and reducing security risks on business data flow paths.

4.4.1.2.3 Comprehensive Security Protection Solution

Security audit

- Enhancing current devices

Enable the built-in system logging and security logging functions to record information about the device running status, network traffic, user behaviors, event dates, users, and event types, so as to help administrators to fully understand the device running status and make security events traceable.

- O&M personnel audit (industrial control O&M OSMS)

Currently, some O&M management regulations have been developed in branch companies and their subordinate units, but these regulations cannot completely eliminate risks. This is partly due to the fact that these regulations are not perfectly carried out. Another main reason is that most station attendants are professionals in the field of automation who have little knowledge about information security, databases, and related software and therefore are unable to audit O&M personnel's operations. In addition, in traditional security and industrial security cases, a large number of security events are caused by illegal operations of O&M personnel or internal personnel. Therefore, professional and industrial environment-based O&M audit devices are needed for audits.

Mobile O&M audit systems are deployed at branch hydrologic stations and central stations for onsite maintenance of PLCs, DCSs, industrial switches, HMIs, operator workstations, engineering workstations, data historian, and real-time databases in industrial control systems.

- Intrusion detection

The following attacks should be monitored at network edges: port scanning, brute force attack, trojan backdoor, DoS, and IP fragment attack. When an attack is detected, the source IP address and attack type should be recorded. In the case of a critical intrusion event, alerts should be promptly generated and such intrusion should be immediately blocked.

Unlike traditional network application protocols, control protocols used in industrial control systems are often proprietary protocols. Intrusion detection systems based on traditional seven-layer network protocols cannot effectively monitor the security of industrial control systems. It is necessary to understand special industrial control protocols used in industrial control systems and configure specific industrial control network detection policies, so as to effectively detect intrusions in industrial control network systems. An ICS anomaly detection system is deployed on core networks of branch companies, secondary units, hydrological stations, and stations. Meanwhile, a comprehensive signature

database and efficient signature matching algorithms applicable to industrial control networks are employed to effectively detect malicious code and viruses.

Security management

- Industrial control vulnerability discovery system

In order to effectively detect and investigate security risks hazards in industrial control systems, it is necessary to deploy the vulnerability scanning system of industrial control systems to detect potential security defects or vulnerabilities in industrial control systems. Based on the signatures of known vulnerabilities (such as SCADA/HMI software vulnerabilities, vulnerabilities in embedded software like PLC and DCS controllers, vulnerabilities in mainstream fieldbus protocols such as Modbus and Profibus, and SCADA/HMI software vulnerabilities) in industrial control systems, the system scans and identifies control devices, operation workstations, engineering workstations, servers, databases, and middleware in industrial control systems such as SCADA, DCS and PLC, so as to provide perfect vulnerability analysis and detection capabilities for industrial control systems.

For unknown vulnerabilities in industrial control systems, with a fuzzing test tool for vulnerability discovery, we can detect vulnerabilities existing in the tested object by sending crafted attack test data to the SCADA/HMI software, DCS system, and PLCs and then checking the returned results.

5

What to Expect for ICS Security in the Coming Years

With the policy guidance of various ministries and commissions under the State Council, related financial support, and the increased emphasis on ICS security by ICS enterprises, the ICS information security will get on the fast track of development. With the advancement of "one network, one database, and three platforms" proposed by the Ministry of Industry and Information Technology (MIIT), the introduction of *Classified Protection of Information System Security 2.0*, and the introduction of *Critical Information Infrastructure Security Protection Regulations*, industrial security will see a very good opportunity for development.

Industrial enterprises have experienced the following three stages in developing industrial control security:

1. Security assessment stage driven by compliance and security events;
2. Pilot construction and lessons learned stage to find solutions and methods;
3. Stage of large-scale application upon promotion with a mature model.

At the current stage, with further regulatory requirements, the application of industrial security in various industries has begun to scale up from sporadic pilots and demonstrative applications. In some industries such as the electric power industry, especially the power generation industry and rail transportation industry, regional large-scale deployment and application have emerged. From the perspective of the industrial control security development, large-scale deployment and application is still a long time effort. Currently, stimulating industrial security with pilots is a big trend of industrial security.

At present, the core technology of industrial control security has not been effectively addressed. The technical development has entered a bottleneck period, witnessing serious product homogeneity. Technical bottlenecks lead to small product function differences. Therefore, vendors are facing an intense competition in a narrow space with few market yields. The industrial control security technology still needs a new round of innovations. Whether incorporating techniques of IT information security or constructing the technology of its own characteristics, industrial control security needs to reflect characteristics of industrial control systems. How to effectively integrate the unified security technical methods of IT+OT into industrial control security capabilities should also be taken into consideration. Technically, the association between lightweight, undisturbed, business data collection and security

data collection should be taken into consideration, and so are the differences of application in various industries, extraction of common technologies, and application of heterogeneous technologies.

Controller vendors, another important participant, have also attached more importance to industrial control security. On the one hand, they add relevant security features to their own control systems, forming "inherent security functions". On the other hand, they have enlarged cooperation with security enterprises, in a bid to jointly promote security solutions matching their own business characteristics and attributes.

As for security capability building, integration with the business management platform, integration of security and business data collection, platform-level data exchange and sharing, and comprehensive business fault diagnosis and analysis will be a development trend of industrial control security in the future. In the building process, security data and business data need to be translated and interpreted, forming an effective "exchange mechanism". The bridge and channel between security data content and business data content need to be gradually set up. In this way, business channels will provide effective data for security, which, in turn, provides effective support for business guarantee.

At the same time, in the major trend of industrial information transformation and extensive interconnection, due to the convenience and cost advantages of interconnection, the enclosed model of original industrial systems will be gradually broken and new business application forms will bring new security risks, such as cloud security risks, edge security risks, and plant-level security risks. With an eye to the future, industrial information security is bound to be comprehensive security, covering cloud security, border security, control security, and data security. The value of security should also be reflected in its role of promoting business, which conforms to industrial attributes and characteristics.

6. Abbreviations

Abbreviation	Full Spelling
AGC	Automatic Generation Control
APT	Advanced Persistent Threat
AVC	Automatic Voltage Control
CPS	Cyber Physical System
DCS	Distributed Control System
DOS	Denial of Service
DPU	Distributed Processing Unit
ERP	Enterprise Resource Planning
FCS	Fieldbus Control System
GE	General Electric Company
HMI	Human Machine Interface
ICS	Industrial control system
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
MES	Manufacturing Execution System
OMS	Order Management System
PCS	Process Control System
PLC	Programmable Logic Controller
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SIS	Safety Instrumented System

7. References

[1] https://me-en.kaspersky.com/about/press-releases/2016_91-1--of-vulnerable-industrial-control-systems-likely-belonging-to-large-organizations

[2] https://ics-cert.kaspersky.com/reports/2018/09/06/threat-landscape-for-industrial-automation-systems-h1-2018/#_Toc523849948

[3] https://ics-cert.us-cert.gov/advisories

[4] https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/NCCIC_ICS-CERT_2016_Annual_Vulnerability_Coordination_Report_S508C.pdf

[5] ICS-CERT Annual Vulnerability Coordination Report, https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/NCCIC_ICS-CERT_2016_Annual_Vulnerability_Coordination_Report_S508C.pdf

[6] https://www.fireeye.com/blog/threat-research/2018/10/ics-tactical-security-trends-analysis-of-security-risks-observed-in-field.html

NSFOCUS

SECURITY MADE SMART & SIMPLE

www.nsfocus.com