*Security and Safety*, Vol. 2, 2023001 (2023)
https://doi.org/10.1051/sands/2023001
sands.edpsciences.org

Views OPEN ACCESS

Industrial Control

# Protection architecture of endogenous safety and security for industrial control systems

Yaozhong Xin*

*Alliance of Industrial Control System, Beijing 100070, China*

Received: 26 October 2022 / Revised: 6 December 2022 / Accepted: 7 March 2023 / Published online: 24 April 2023

**Abstract** According to the essential characteristic of industrial control system (ICS), endogenous safety and security (ESS) can be achieved by merging cyber security (CS) into functional safety (FS). In this paper, the basic principles, functional requirements and protection architecture (TEMt) of ESS are proposed, and the successful experience of an electric power control system is introduced.

**Keywords** Industrial control system, Endogenous safety and security, Protection architecture

**Citation** Xin Y. Protection architecture of endogenous safety and security for industrial control systems. Security and Safety 2023; **2**: 2023001. https://doi.org/10.1051/sands/2023001

## 1 Introduction

Important industrial control systems, such as energy and electric power, transportation, municipal facilities, manufacturing and other industrial control systems, are the most critical infrastructures, directly related to national security and social stability [1].

The global industrial control system faces increasingly serious cyber security threats. On October 13, 2000, Sichuan Ertan Hydropower Station received an abnormal instruction from the external network, and all six units were shut down, leading to a large area of power failure and almost the collapse of the independent Sichuan power grid at that time [2]. During the 2008 Beijing Olympic Games, the related power grid was attacked 8939 times from outside cyber, an average of 598 times per day. On December 23, 2015, hackers attacked the power grid control system (SCADA) in several regions of Ukraine, directly shutting down 7 110 kV substations and 2 335 kV substations, leading to a massive power outage. On March 8, 2019, Venezuela suffered a massive power outage that lasted for several days, the local government blamed the United States for the cyber attack. In May 2021, the United States entered a state of emergency due to a ransomware attack on oil pipelines [3]. During the Russia-Ukraine conflict, which began in February 2022, both sides suffered cyber attacks on government websites, military facilities, and infrastructure from the other side. According to the recent security monitoring statistics of the external network border of the State Grid of China [2], it suffers from various malicious network attacks more than 10 000 times every day, with an average of one attack every few seconds. Cyber warfare is already underway, with critical infrastructure being targeted.

Cyber security threats are evolving from software to hardware. The TRITON, Stuxnet [4], Blackenergy, and ransom-ware reported to attack energy control systems in recent years, are all software attacks targeting Windows operating systems. In 2017, it was found that almost all processors have hardware

* Corresponding author (email: 13601038643@163.com)

security problems such as meltdown, spectre. [5], etc. This brings a new major technical challenge to the security of industrial control systems.

The "Ertan incident" in 2000 caused the national competent authorities of China to attach great importance to it and immediately organized and studied the network security protection measures for the power grid control system, three orders were issued [6], and after more than twenty years of continuous effort, the cyber security protection architecture of power grid control system covering the whole industry has been gradually established, it effectively ensures the safety and security of the power system [2].

However, there are two major problems in most industrial control system. The first one is the cyber security measurements were separated from the functional safety of industrial control, another is the protection architecture have not been established for many industries, but any single security measurement could not defense rapidly increasing cyber security threat.

For the first problem, JiangXing Wu created the mimic defense [7, 8], proposed the concept of endogenous safety and security [9, 10], and generalized functional safety [11]. Kavallieratos *et al.* studied the cyber security and safety co-engineering of cyber-physical systems [12]. Steven X. Ding studied the functional safety and cyber security in automatic control systems [13].

In order to solve the two problems, this paper focuses on merging or melting cyber security (CS) into functional safety (FS), to form endogenous safety and security (ESS); the protection architecture of ESS for industrial control is proposed and analyzed; based on the architecture, the higher ESS level with lower cost can be achieved; the successful experience of electric power control system is introduced.

## 2 Abstract model and basic characteristics of ICS

Industrial control systems are generally divided into two categories: one is the process-level industrial control system, such as substation control system, workshop production line control system, etc. The other is system-level industrial control systems, such as power grid dispatching and control systems at all levels, all kinds of pipeline monitoring and control systems, rail transit dispatching and control systems, etc.

The industrial control systems are composed of the following abstract components: sensors (including all kinds of analog input AI and digital input DI), actuators (including all kinds of analog output AO, and digital output DO), field controllers, local control systems, remote control systems, dedicated local area networks, and dedicated wide area networks. The sensor and the actuator are directly connected to the industrial process. The field (or on-site) controller is close to the industrial process, generally using signal cable or network cable (no switcher) to connect the sensor and the actuator, to achieve the nearest fast control. The local control system connects the local sensor, actuators and field controller through the local area network (or signal cable) to realize the local coordinated control. The remote control system connects several local control systems through a dedicated wide area network to realize the coordinated control of the whole system. As shown in Figure 1.

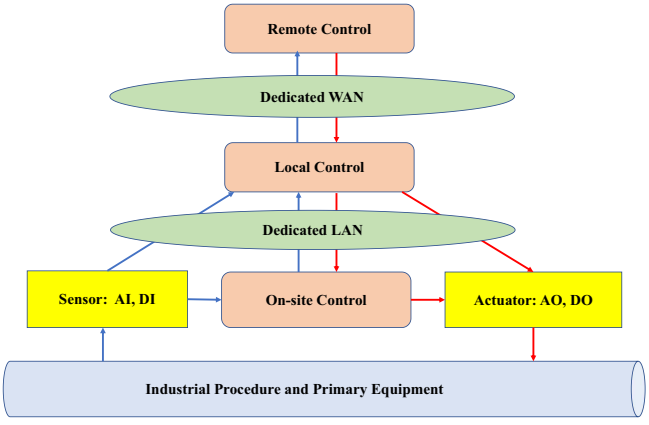


**Figure 1.** Abstract model of industrial control system

The industrial control system has three major typical characteristics. The first is high reliability, the second is strong real-time, and the third is high safety which includes functional safety and cyber security. If the industrial control system lost reliability and real-time, it could not complete the industrial control function, which is equivalent to self-attacking.

For industrial control systems, functional safety is more basic and important than cyber security. Cyber security serves functional safety, and the goal of cyber security is to ensure functional safety. Therefore, only by merging cyber security into functional safety, and forming the endogenous safety and security (ESS) mechanism, then, the overall safety of the industrial control system can be guaranteed.

## 3 Basic principles of ESS for ICS

This paper summarizes the experience and lessons in the field of industrial control of many industries in the past 30 years in the world, and puts forward six basic principles of endogenous safety and security (ESS) for industrial control system, as follows.

(1) Facing industrial production, focusing on industrial control.

The core goal of industrial control systems in various fields is to make industrial control businesses more safer and more reliable, more economic and efficient, more green and environmental protection, and more practical, and friendly. The design and development, engineering construction, operation and maintenance of the industrial control systems should focus on the core business objectives to meet the practical needs of the business. If the business requirements, functional and technical specifications, the use of the main body is not clear, but if the project construction carried out blindly, it will cause unnecessary waste.

(2) Hierarchical partition control and global collaborative optimization.

According to the control theory and the internal characteristics of industrial control business, a large industrial control system adopts a hierarchical control mode. For example, the power grid control can be divided into national, regional, provincial, district, county, substations and power plant levels, each level has objects of direct control within its scope of responsibility and accepts the superior dispatching command and coordination control. Multilevel control systems need to be tightly coupled to achieve the global sharing of business models, real-time data, graphical interfaces, and alarm information. Global cooperative control based on security mechanisms such as identity authentication can be achieved. The "big centralization" mode for non-real-time management business is not suitable for industrial control systems.

(3) Nearby distributed processing, timely response to events.

The real-time data collected by the industrial control system include second level, millisecond level, microsecond level, etc. the total amount of data is very large. According to the requirements of the control logic, specific actions must be completed within a specific time. Therefore, edge computing and distribution processing can only be adopted, and the nearby distribution processing can be used to transmit the "ripe data" to the upper control center, and the "big data" will naturally become "small data", which is convenient for subsequent analysis, processing, and decision making. If all the original data is directly transferred to the control center for centralized processing, it will lead to a "big data disaster", which will seriously affect the system performance and control function. An Industrial control system requires a timely response to system events, there is no need to pursue high enough real-time, the higher real-time, the higher cost.

The response time ($t$) of the industrial control system is proportional to the action distance ($r$), the faster the response time of the control function, the shorter the control action distance, this can be expressed as Equation (1).

$$r(t) = vt + b, \tag{1}$$

Here, $v$ is the velocity of the control loop which can be determined by the physical characteristics of sensor speed, communication speed, and control performance; b is a constant that is related to the industrial system, as shown in Figure 2.

In a logarithmic space-time coordinate system, all kinds of industrial control functions are located near the line with a slope of 45 degrees, it reflects the intrinsic characteristic of industrial control system.

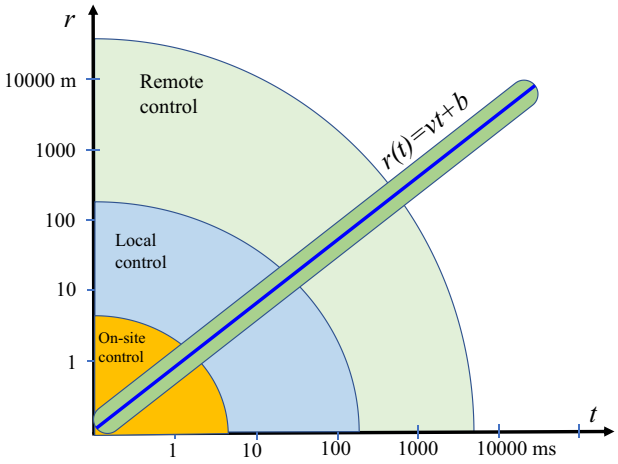


**Figure 2.** ICS functions distributed in space-time

The on-site control functions usually locate in the brown area, the local control functions are usually located in the blue area, and the remote control functions are usually located in the green area.

(4) Parallel redundant mimicry to enhance system resilience.

The main measures to improve the reliability of the industrial control system, one is to improve the reliability of each module itself, and the other is the key module must be redundant to ensure the structural reliability of the system. Generally, dual redundancy is used, and multiple redundancies can be used for important parts. Some important industrial control systems (such as protection relay, etc.) need to use the whole process of mimicry [7] redundancy: different sensors, different communication channels, different controllers, different control logic or principle, different equipment manufacturers, etc. Very important industrial control systems (such as power grid control system, etc.) need to establish redundant backup control centers. Many critical infrastructure facilities are sensitive to major natural disasters, especially the power system. Most of the power facilities are located in the open air, and all kinds of major natural disasters seriously could affect the safety of the power system. Important industrial control systems should have strong resilience and rapid recovery ability to withstand major natural disasters and cyber attacking.

(5) Merge the security mechanism into the industrial control system.

The industrial control system adopts lots of computer and communication technology, not only to ensure the safety of business functions, but also to ensure the security of the network, it is necessary to merge the security mechanism into the industrial control function, to reduce intermediate links, to achieve endogenous safety, to improve the overall safety and reliability. Conventional external security measures (firewalls, etc.) can be used for border protection, but cannot be used inside industrial control processes. All security mechanisms should meet the requirements of reliability, real-time, distribution, and systematic industrial control.

(6) System comprehensive coordination, safety, and economic balance.

Industrial production has always adhered to the principle of "safety first", and worked hard to prevent major personal accidents, major system accidents, and major equipment accidents. However, any safety measures have economic costs, there is no absolute safety. To determine the appropriate safety and security level of the industrial control system, that should be considered comprehensively in its importance, social impact and economic costs and other factors.

For specified functions $f$ and ESS measurements $s$ in the industrial control system, the cost to implement $f$ and $s$ can be expressed as $C(f,s)$, and the productions based on $f$ and $s$ can be expressed as $P(f,s)$. The system safety level, $S(f,s)$, should be proportional to the cost and inversely proportional to the number of functions. The system economic benefit,$E(f,s)$, should be proportional to the productions and inversely proportional to the cost. These can be expressed as Equation (2)

$$\begin{cases} S\,(f,s) = \frac{C(f,s)}{f} \\ E\,(f,s) = \frac{P(f,s)}{C(f,s)}. \end{cases} \tag{2}$$

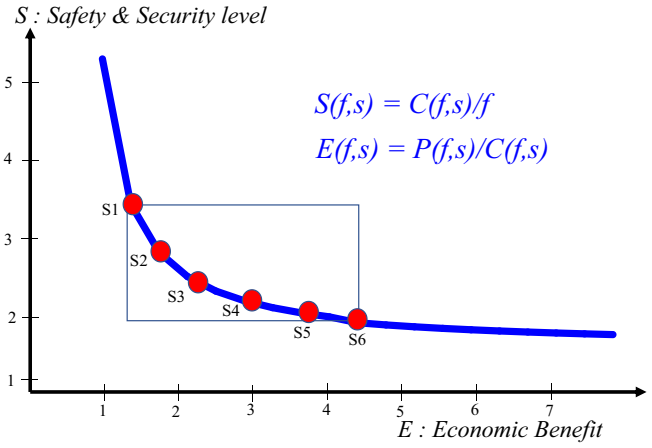


**Figure 3.** Balance of safety and security with economic benefit

Figure 3 shows the relationship between safety and security levels with economic benefits. The red points on the curve from S1 to S6 indicate different levels of safety and security. If the industrial control system is an important infrastructure, a higher level of safety and security should be taken, for example, S1 or S2, but have to pay some higher cost. Otherwise, some lower level could be taken, such as S3 or S4, etc.

At the same time, we must be aware that no matter how comprehensive and balanced a variety of factors, safety is always the lifeline of industrial control, which must always be put in the first place.

## 4 Functional requirements of ESS for ICS

(1) Endogenous safety and security for sensors and actuators

Strengthen the safety and reliability of sensors and actuators. Sensors and actuators are the underlying infrastructure of industrial control systems and the physical interface with industrial processes, which should be able to adapt to strong electromagnetic interference, dust environment, high temperature and humidity, low-temperature freezing, mechanical vibration, wind and sun exposure, fog, frost, rain and snow, lightning disasters and other industrial site environments. Important sensors and actuators should be redundant to ensure their long-term safe and stable operation.

The practical sensing mode should be selected according to the characteristics of industrial business. The industrial control system should select the sensing mode with high safety and reliability, simple and practical, and a small amount of data. For example, electric power control naturally selects electrical sensors, supplemented by non-electrical sensors. Intelligent inspection robots and automatic driving engineering vehicles can choose liDAR, video navigation, short-wave navigation, and other ways. Although video technology has been widely used in public safety, face recognition, plate recognition, product inspection, etc., it is not suitable for closed-loop or open-loop control processes in the industry. For example, conventional DI sensors require only two bits to represent the switching state. However, if video monitoring is used to monitor the switching state, at least a 2 Mb/s communication channel is required for continuous transmission. The data volume is more than a million times larger than that of conventional DI, the reliability and security are greatly reduced, and the cost is greatly increased.

Important smart sensors and smart actuators should support identity authentication and encrypted data transmission. Conventional sensors and actuators have no processing capabilities. Digital sensors have certain processing capability. The new smart sensor and smart actuator have strong processing capability, which should be able to support the encrypted transmission of sensing data and the identity identification of control instructions, so as to prevent Stuxnet and other similar malicious codes from tampering with the original sensing data or control instructions.

The industrial control system cannot solve the problem of the industrial primary equipment itself. The safety and reliability of the primary equipment are the physical cornerstones of the whole industrial control system. Sensors and industrial control systems can find some problems with the primary equipment, but

cannot solve these problems. If we want to solve the problem fundamentally, we can only improve the safety and reliability of the primary equipment itself. Some "intelligent primary equipments" have been equipped with many sensors and monitoring mechanisms, which not only cannot solve the problem of the primary equipment itself, but also affect the safety and stability of the whole system.

(2) Endogenous safety and security for network communication facilities

Choose a secure and practical communication method. The important industrial control system should adopt a dedicated communication network. Local communication can use the dedicated local area network or network cable, and the field short-distance communication can use the shielded signal cable or network cable. Fixed industrial control businesses should prefer fixed special optical communication modes. Due to the metal reflection, the dust environment, and the electromagnetic interference, all have a great impact on wireless communication, generally do not use wireless communication, if necessary, optical fiber + wireless mode can be used. As for mobile industrial control (vehicle-mounted, ship-borne, airborne control system, etc.), it can only use wireless communication for external communication, but its internal communication should also use a fixed dedicated local area network. The industrial control system can select a suitable dedicated network according to the business characteristics. The physical dedicated network is built on the basis a special communication medium (dedicated optical cable, fiber, wavelength, circuit, etc., the isolation intensity decreases in turn), which has high security and high cost. Virtual private network (VPN) adopts logical isolation (VPN, APN, 5G slice, etc.) over the common communication medium, which has low security and low cost.

The dedicated LAN should be layered and segmented. Industrial fiber Ethernet has become the main communication mode of the workshop and plant-level industrial control systems, but the delay and jitter of LAN switch, clock synchronization, packet collision, data storm, cyber security, and other problems need to be considered comprehensively. Important industrial control systems (such as relay protection, etc.) can use Ethernet cables for point-to-point communication, and try to avoid using LAN switchers. The LAN should be layered and segmented according to business requirements. It can be divided into plant layer network, workshop (bay) layer network, process layer network, and so on. Each layer is divided into multiple segments, each of which is configured redundantly. The LAN adopts a tree structure to ensure network segment traffic balance and avoid network storms and cyber security problems.

The topology of dedicated WAN should be a grid structure. The network topology structure can be optimized according to the geographical location of industrial control services to form multiple circuitous routes and improve the reliability of network services. Industrial control networks should not use star or line topology to prevent a single point of failure from affecting the whole network. A large dedicated network should also be divided into a backbone network and an access network.

(3) Endogenous safety and security for the field, local, and remote control systems

Control software should have built-in security mechanisms. The field controller (small PLC, measurement and control unit, other process-level controllers), the local control system (DCS and other shop-level and plant-level control systems), the remote control system (SCADA and other control center systems, which can be deployed at multiple levels) should have built-in security mechanisms such as identity authentication, data encryption, trusted immunity, to ensure the safety and reliability of closed-loop control and open-loop control. Important industrial control software must be tested by professional institutions for functional safety and cyber security certification. Only after passing the test it can be put into operation. After the modification and upgrade of the control software, a comprehensive test and certification shall be conducted again. Field modification of control software source code is not allowed.

Strengthen operating system kernel security. The operating system kernel should support mandatory behavior control, mandatory access control, mandatory ability control, trusted immunity, identity authentication, data encryption, real-time preemptive scheduling, fast interrupt response, and other mechanisms. The traditional macro kernel operating system is complex and huge, it is difficult to adapt to the needs of small industrial control equipment, and many industrial control equipment can be only "naked" (no operating system). It is recommended to adopt a safe and real-time micro-kernel operating system to improve the overall safety and reliability of the industrial control system.

Ensure hardware security of the main board. Important industrial control systems should use a safe and reliable main-board, should support multiple power supplies, reliable grounding, electromagnetic shielding, interface isolation, adapt to high and low temperatures, low power consumption without a fan, be waterproof, and dustproof, remove useless modules, adapt to the harsh environment and safety

requirements of the industrial site. In nodes with large computing processing capacity, multiple nodes can be deployed in parallel redundancy mode to improve system reliability and processing capability.

Critical chips and instructions should be secured. Important industrial control systems should adopt safe and reliable processor chips, which can support security and credible immunity, tightly coupled storage architecture, fast interrupt response, fast thread switching, etc., and should be without chip-level or instruction-level security risks such as "spectre" and "meltdown", and should be able to adapt to the harsh environment of industrial sites.

In 2009, the smart grid dispatching and control system (D5000) was successfully developed, which merged the security technology into every control module, and realized the endogenous safety and security of the core control business of the power grid [14]. The system has been widely used in the power systems of China, which effectively ensures the safe and stable operation of the power grid.

## 5 Protection architecture of ESS for ICS

Industrial control system safety is very complex, involving a variety of technologies, a number of professionals, a variety of facilities, and a number of entities. Any single safety technology is only effective in a certain range, and cannot adapt to all safety problems. Therefore, it is necessary to establish the endogenous safety and security protection architecture of the industrial control system, by integrating safety and security technology, emergency measures, and safety management into an organic whole, to improve the overall safety and security level of the industrial control system.

The endogenous safety and security protection architecture of industrial control system has a four-dimensional spatial and temporal structure, in which the $X$ axis is safety and security technology ($T$), the $Y$ axis is emergency measures ($E$), the $Z$ axis is safety and security management ($M$), and the $T$ axis is the constantly developing time coordinate ($t$), which is called TEMt architecture. The technology dimension ($T$) mainly includes infrastructure, structure, ontology, immunity, and so on. The emergency dimension ($E$) mainly includes redundant reserve, emergency response, multiple lines of defense, etc. The management dimension ($M$) mainly includes the management of all personnel, all devices, and its whole life cycle. The time dimension ($t$) indicates that the system will develop and improve over time. It can be expressed as Equation (3).

$$\mathrm{ESS} = \int (T \times E \times M)\, dt, \tag{3}$$

Here, $T \times E \times M$ represents the cross product of three dimensions, the integration represents the accumulation effect for the time dimension, the diagram can be shown in Figure 4.

The dimension of technology reflects the deepening of technology and is the technical basis of the whole architecture. No technology can guarantee absolute security, and problems can occur at any node, so emergency measures are needed. Emergency measures reflect the concept of safety and reliablity from industrial control. Industrial control system involves a variety of personnel and a variety of equipment, so the need for comprehensive safety management, safety management condenses long-term experience and lessons in the industry. With the development of time, various technologies, emergency measures, and management methods are constantly developing, and the protection architecture must be constantly improved. In short, the four dimensions support each other and together constitute a four-dimensional space-time protection architecture.

The structural safety of the industrial control system is the backbone of the protection architecture. The topology of the protection architecture should be a three-dimensional grid structure, and any single point of failure should not affect the whole system. The important industrial control system should adopt a dedicated communication network. The dedicated network should be interconnected as needed to ensure security and strictly prevent illegal external connections. Large industrial control systems can use dedicated cloud technology to prevent the public cloud from "one cloud cover sky". The industrial control system can use dedicated IoT (internet of things) technology to prevent the public IoTs "Internet of everything".

Industrial control systems and their dedicate networks have clear physical boundaries. Appropriate security isolation and monitoring facilities should be deployed at the boundaries. Border security and structural security are the important basis of other security measures. For control systems that have not realized endogenous safety and security, border security is the main technical measure. Some notions that

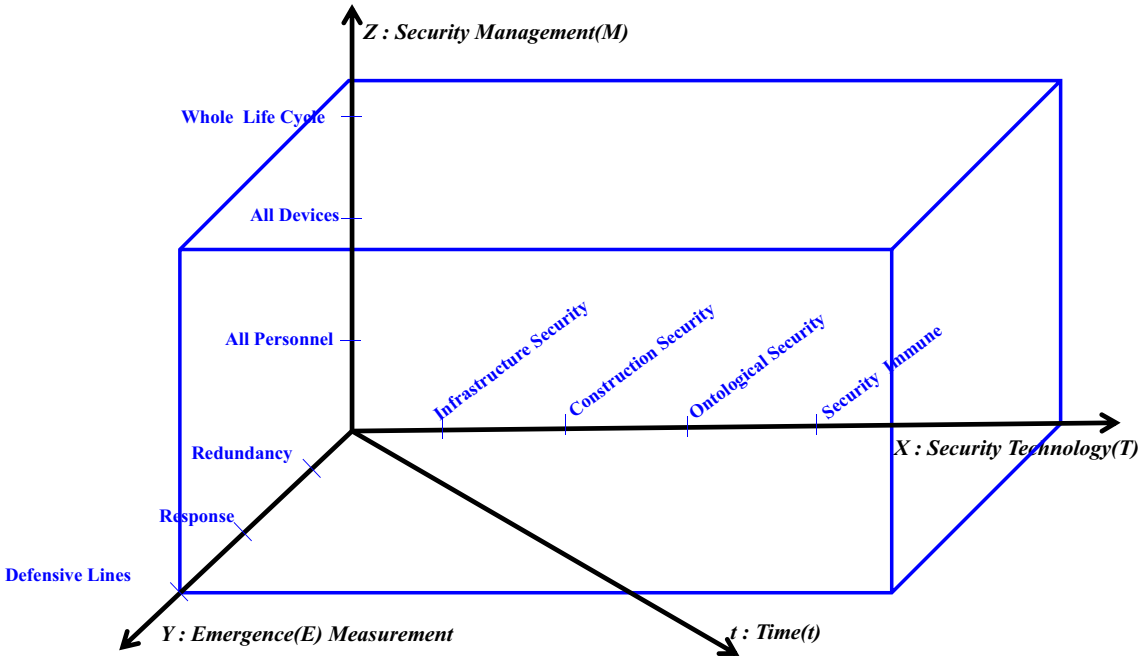


**Figure 4.** Protection architecture (TEMt) of endogenous safety and security

"zero trust" systems no longer require secure borders are false. In fact, the "zero trust" system requires stricter borders and stricter security measures, such as identification, and also within borders.

The cyber security protection architecture of China's electric power control system was built in 2008 and developed continuously [2]. It has covered all levels of power grid control centers, all kinds of substations, and power plants, and withstood years of actual tests and verification, effectively ensuring the safe and stable operation of the power system. The related achievements have formed the national standard GB/T 36572-2018 Guidelines of cyber security protection for electric-power control system [15], and GB/Z 41288-2022 Information security technology – guidelines of cyber security protection for important industrial control system [16]. GB/Z 41288-2022 aims to guide all kinds of industrial control systems to establish their cyber security protection architecture.

The characteristics of global industrial control systems in different industries vary greatly. The energy industry and public utilities mainly use fixed control and fixed communications. The transportation industry is dominated by mobile services. The intelligent production and manufacturing industries are dominated by local control. The different nature of industrial control business will inevitably lead to different protection measures of safety and security, but the protection architecture (TEMt) and protection principles are the same.

The protection architecture of endogenous safety and security could adapt to all kinds of industrial control systems worldwide, which is especially suitable for important infrastructure industrial control systems.

## 6 Conclusion

This paper analyzed the essential characteristics of industrial control systems, achieved endogenous safety and security (ESS) by merging cyber security into functional safety, discussed the basic principles and functional requirements, proposed the protection architecture (TEMt) of ESS, and introduced the successful practice of electric power control system in China. Hope the protection architecture of ESS could improve the safety and security for the all industrial control systems worldwide.

### Conflict of Interest

The author declares no conflict of interest.

### Data Availability

No data are associated with this article.

### Acknowledgements

Thank Jiangxing Wu for helpful comments and suggestions.

### Funding

No funding are associated with this article.

## References

[1] The security protection regulations of critical Information Infrastructure. The State Council of China, 2022.
[2] Xin Y. The cyber security protection architecture of important industrial control system. J Inf Secur Res 2022; **8**: 528–33.
[3] Tsvetanov T and Slaris S. The effect of the Colonial pipeline shutdown on gasoline prices. Econ Lett 2021; **209**: 1–5.
[4] Langner R. Stuxnet: Dessecting a cyber warfare weapon. IEEE Secur Privacy 2011; **9**: 49–51.
[5] Paul K, Jann H and Anders F et al. Spectre attacks: Exploiting speculative execution. In: IEEE Symposium on Security and Privacy (SP) 2019. https://doi.org/10.1109/SP.2019.00002.
[6] The order 14, The cyber security protection regulations of electric power monitoring and control system. The National Development and Reform Commission of China, 2014.
[7] Wu JX. Cyberspace Mimic Defense: General Robust Control and Endogenous Safety & Security. China: Springer, 2019.
[8] Wu JX. Cyberspace Endogenous Safety and Security: Mimic Defense and General Robust Control. China: Science, Press, 2020 (Chinese).
[9] Wu JX. Cyberspace endogenous safety and security. Engineering 2021, in press. https://doi.org/10.1016/j.eng.2021.05.015.
[10] Wu JX. Development paradigms of cyberspace endogenous safety and security. Sci China Inf Sci 2022; **65**: 156301. https://doi.org/10.1007/s11432-021-3379-2.
[11] JiangXing W. Problems and solutions regarding generalized functional safety in cyberspace. Secur Saf 2022; **1**: 2022001. https://doi.org/10.1051/sands/2022001.
[12] Kavallieratos G, Katsikas S and Gkioulos V. Cybersecurity and safety co-engineering of cyber physical systems – A comprehensive survey. Future Internet 2020; **12**: 65.
[13] Steven X. Ding, A note on diagnosis and performance degradation detection in automatic control systems towards functional safety and cyber security. Secur Saf 2022; **1**: 2022004. https://doi.org/10.1051/sands/2022004.
[14] Yaozhong X, Boming Z, Mingyu Z, Qiang L and Huafeng Z. New energy management system in China. IEEE Power Energy 2018; **16**: 37-47.
[15] GB/T 36572-2018 Guidelines of cyber security protection for electric-power control system.
[16] GB/Z 41288-2022 Information security technology - guidelines of cyber security protection for important industrial control system.

**Yaozhong Xin** is currently the chairman of Alliance of Industrial Control System and chief expert of China Electricity Council. His research interests include power system automation, industrial control systems, and cyber security protection.