Journal of Trends in Applied Science and Advanced Technologies
Print ISSN: 3007-6870
Online ISSN: 3007-6889
DOI: https://doi.org/10.61784/asat3021

CYBERSECURITY GOVERNANCE MECHANISM OF INDUSTRIAL CONTROL SYSTEMS UNDER THE BACKGROUND OF INTELLIGENT MANUFACTURING

WenTao Liu
Shenzhen Rongan Networks Technology Co., Ltd., Shenzhen 518000, Guangdong, China.

Abstract: With the advancement of intelligent manufacturing, industrial control systems (ICSs) are transforming towards IT/OT convergence and cloud-edge collaboration, leading to the disintegration of the boundaries of traditional closed industrial control networks and a surge in security risks. The existing governance mechanisms still suffer from such problems as an imperfect system, ambiguous rights and responsibilities, and disconnection between technical and management practices. Based on the risk governance theory and the whole life cycle concept, and in alignment with the IEC 62443 standard and domestic policies on industrial control security protection, this paper constructs an ICS cybersecurity governance mechanism featuring a three-dimensional governance framework, closed-loop full-process operation and multi-stakeholder collaborative linkage. The mechanism clarifies the rights and responsibilities of the government, enterprises, suppliers and other parties, designs a full-process system including risk identification, protection implementation, monitoring and early warning, emergency response, and continuous improvement, and proposes an implementation path of three-dimensional integration of technology, management and operation. It also divides the implementation steps into three phases: basic construction, in-depth construction and optimization and upgrading, with supporting guarantee measures in four aspects: policy, technology, resources and collaboration. This mechanism can effectively reduce the incidence of security incidents and improve the efficiency of emergency response, providing theoretical and practical support for the safe and stable operation of ICSs in intelligent manufacturing scenarios.
Keywords: Intelligent manufacturing; Industrial control system; Cybersecurity; Governance mechanism; IT/OT convergence

1 INTRODUCTION

With the in-depth implementation of *Made in China 2025* and the new industrialization strategy, intelligent manufacturing has become the core direction for the transformation and upgrading of the manufacturing industry. In recent years, security incidents such as frequent industrial control vulnerabilities, ransomware attacks and supply chain intrusions have been common occurrences, which not only threaten the continuity of industrial production, but also bear on the security of critical information infrastructure and the overall development of the industry. Existing research mostly focuses on technical protection of industrial control security or interpretation of a single policy, lacking the systematic construction of governance mechanisms. A complete standard system has taken shape overseas, while domestic research, though developing rapidly, still has shortcomings. Therefore, this paper systematically sorts out the relevant policies, standards and research results of industrial control security governance at home and abroad; adopts a normative analysis method, clarifies the rights and responsibilities of governance subjects and operation processes based on policy requirements and standard frameworks, analyzes emerging security challenges, constructs a collaborative governance mechanism, and designs an implementation path, so as to support the intelligent transformation of the manufacturing industry.

2 EMERGING CYBERSECURITY CHALLENGES FOR INDUSTRIAL CONTROL SYSTEMS UNDER THE BACKGROUND OF INTELLIGENT MANUFACTURING

2.1 Escalating Security Risks Brought by the Application of New Technologies

The iteration of new technologies and industrial models has led to the continuous escalation of security risks of ICSs, with various hidden dangers interweaving and becoming increasingly complex. The deep integration of artificial intelligence (AI) and ICSs, while facilitating intelligent fault diagnosis and autonomous production scheduling and improving the level of intellectualization, harbors dual risks: AI training data is vulnerable to tampering, which may trigger decision-making errors and production accidents; AI system vulnerabilities can also be exploited to launch targeted attacks, and the definition of responsibilities for related accidents is ambiguous with existing legal gaps. At the same time, the industrial Internet of Things (IIoT) features a large number of devices with diverse categories and weak computing power. Most intelligent meters and sensors lack basic security protection, with prominent problems of default and weak passwords, making them easy breakthroughs for attacks. Some old devices cannot undergo firmware upgrades, leaving vulnerabilities unaddressed for a long time and planting persistent hidden dangers. In addition, the global collaborative development of the intelligent manufacturing supply chain has lengthened the security chain.

Industrial control core equipment, components and services are distributed worldwide, and problems such as backdoor vulnerabilities in products and weak protection of third-party service providers can all transmit and trigger security risks [1-3]. China's *Cybersecurity Law* also clearly requires relevant operators to conduct national security reviews and sign confidentiality agreements when purchasing products and services.

2.2 Core Dilemmas Faced by the Governance System

The current industrial control security governance system has multiple shortcomings and is difficult to adapt to the security protection needs in intelligent manufacturing scenarios. On the one hand, the rights and responsibilities of governance subjects are ambiguous, presenting a situation of multiple management and unclear accountability. The responsibilities of multiple government regulatory departments overlap, the division of rights and responsibilities among the security, production and operation and maintenance departments within enterprises is not clear, and the security responsibility chain between suppliers, integrators and users in the upstream and downstream of the supply chain is broken, which is likely to lead to the predicament where no one takes responsibility for accidents and no one leads the rectification. On the other hand, there is a serious disconnection between technology and management. Many enterprises fall into the misunderstanding of focusing on technical investment while neglecting system management. Even if industrial firewalls, intrusion detection systems and other devices are deployed, there is a lack of sound management systems and personnel training mechanisms, making it difficult to exert the effectiveness of the devices. Some enterprises even fail to establish a closed-loop vulnerability management mechanism, leaving high-risk vulnerabilities unaddressed for a long time. In addition, enterprises generally have insufficient emergency response capabilities. Industrial control security incidents spread rapidly, cause great harm and are highly professional, but most enterprises have non-targeted emergency plans and formalistic emergency drills, and lack a multi-stakeholder collaborative linkage mechanism, resulting in extremely low efficiency of emergency response and inability to effectively deal with sudden security accidents[4-6].

3 CONSTRUCTION OF THE CYBERSECURITY GOVERNANCE MECHANISM FOR INDUSTRIAL CONTROL SYSTEMS

3.1 Construction Principles

Combined with the development characteristics of intelligent manufacturing and the core security protection needs of industrial control, the governance mechanism constructed in this paper follows five core principles: taking risk assessment as the foundation and implementing the risk-oriented principle, conducting differentiated control for different risk levels and giving priority to protecting critical information infrastructure and core production links; closely adhering to the whole life cycle principle, covering the entire process of ICS planning, construction, operation and maintenance to decommissioning, and ensuring that security protection is planned, constructed and used simultaneously; upholding the multi-stakeholder collaboration principle, clarifying the rights and responsibilities of the government, enterprises, suppliers and other parties, and building a governance pattern of government supervision, enterprise main responsibility and social collaboration; adhering to the integration principle of technology and management, coordinating technical protection and management systems to realize their complementary and synergistic effects; following the continuous improvement principle, relying on normalized evaluation and optimization, and dynamically adjusting governance measures in response to changes in technology, policies and risks.

3.2 Overall Framework of the Governance Mechanism

The ICS cybersecurity governance mechanism under the background of intelligent manufacturing constructed in this paper takes the "three-dimensional governance framework" as the core, the "closed-loop full-process operation" as the path, and the "multi-stakeholder collaborative linkage" as the guarantee, forming a governance system with "horizontal and vertical coverage". The overall architecture is shown in Figure 1.

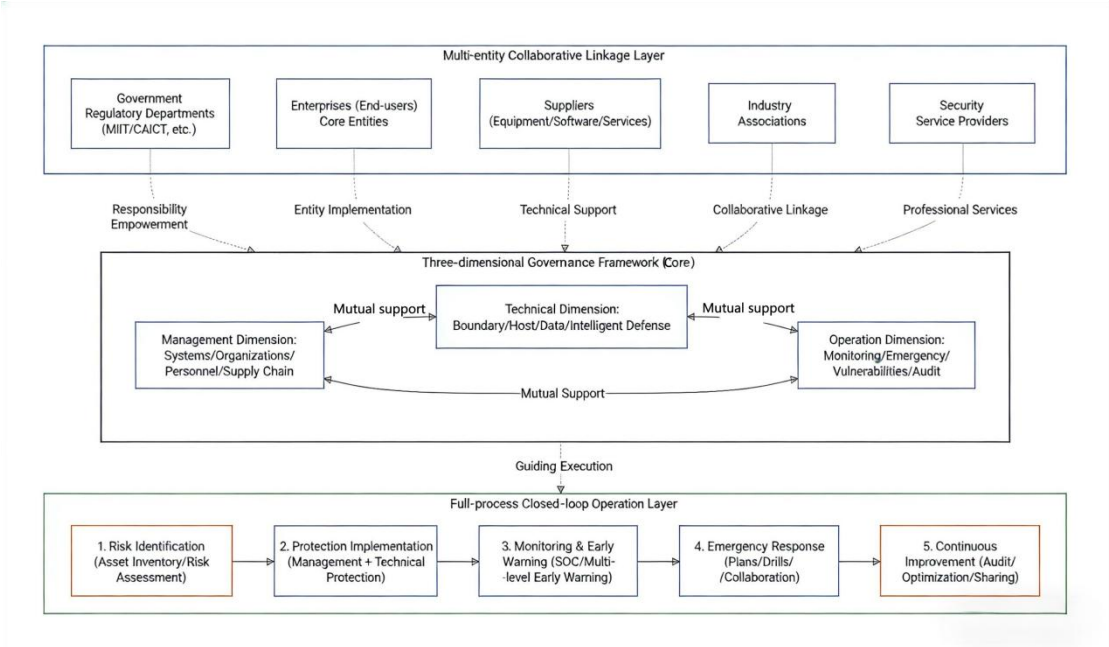

Figure 1 Overall Architecture of Network Security for Industrial Control Systems in the Context of Intelligent Manufacturing

3.3 Three-Dimensional Governance Dimensions

This paper divides the industrial control security governance dimensions into three core dimensions: management, technology and operation, which support and cooperate with each other. The management dimension focuses on the management of systems, personnel and supply chains, serving as the core guide for governance; the technology dimension deploys adaptive equipment around various protection needs, acting as the hard-core support; the operation dimension covers normalized security operation, being the long-term guarantee.

3.4 Closed-Loop Full-Process Operation

Based on the NIST Cybersecurity Framework and the requirements of China's *Protection Guidelines*, a closed-loop full-process operation system of "risk identification - protection implementation - monitoring and early warning - emergency response - continuous improvement" is designed to ensure the continuity and effectiveness of governance work.

3.5 Multi-Stakeholder Collaborative Linkage

3.5.1 Division of rights and responsibilities of governance subjects

In accordance with the principle of "who operates, who is responsible; who is in charge, who is responsible" and combined with the characteristics of the intelligent manufacturing supply chain, the core rights and responsibilities of each governance subject are clarified, as shown in Table 1.

Table 1 Division of Responsibilities for Cybersecurity Governance in Industrial Control Systems

Governance Subjects	Core Rights and Responsibilities
Government regulatory departments (MIIT, Cyberspace Administration of China, Communications Administration Bureaus)	1. Formulate industrial control security policies, standards and regulations; 2. Conduct security supervision of critical information infrastructure; 3. Establish a "double reporting" system and coordinate the disposal of major security incidents; 4. Promote the implementation and compliance of security standards
Enterprises (end users)	1. Bear the main responsibility for industrial control security and establish a security management system; 2. Conduct whole life cycle risk governance; 3. Implement hierarchical protection requirements and conduct regular risk assessments and emergency drills; 4. Sign security responsibility agreements with suppliers
Suppliers (equipment, software, services)	1. Provide products and services complying with national security standards and issue security certification reports; 2. Establish a product vulnerability notification and repair mechanism;

	3. Cooperate with enterprises in security testing and technical support
Industry associations	1. Build a collaborative governance platform and carry out policy publicity and technical exchanges; 2. Formulate industry self-regulation norms and promote experience sharing among enterprises; 3. Assist the government in standard implementation, compliance and evaluation work
Security service providers	1. Provide professional services such as risk assessment, penetration testing and emergency response; 2. Research and develop security technologies and products adapted to intelligent manufacturing; 3. Conduct personnel training to improve the security capabilities of enterprises

3.5.2 Design of the closed-loop full-process operation system

(1) Risk Identification

Risk identification is the starting point of industrial control security governance, whose core is to build a comprehensive, multi-dimensional and dynamic risk assessment system to accurately identify system security weaknesses and define risk levels. Enterprises need to comprehensively sort out all industrial control assets such as PLC, DCS and industrial hosts, establish a dynamic list and conduct hierarchical management and control according to business importance; conduct normalized risk assessments by means of vulnerability scanning and attack path analysis, and conduct special assessments before the construction, upgrade and external connection of systems, with at least one comprehensive assessment for important systems every year; divide risks into four levels in accordance with the Classified Protection 2.0 standard, formulate differentiated disposal plans for different levels, and clarify the responsible subjects and rectification time limits to lay a solid foundation for governance [7].

(2) Protection Implementation and Monitoring and Early Warning

Protection implementation is the core link of industrial control security governance. Relying on the results of risk identification and combining with the three-dimensional governance dimensions of management, technology and operation, a dual-track in-depth protection system of "technology + management" is built. In terms of management, improve security institutions and systems, strengthen personnel training, and strictly manage supply chain security; in terms of technology, consolidate the network boundary defense line, standardize host terminal management and control, implement data security protection, and realize accurate risk disposal with the help of intelligent defense equipment. As a key link, monitoring and early warning requires the construction of a normalized, intelligent and collaborative early warning system [8-9]. Rely on the industrial control security operation center to integrate security equipment, comprehensively monitor equipment operation and network traffic, build a hierarchical early warning mechanism, clarify disposal processes and responsibilities, and link multiple parties to build an intelligence sharing platform, so as to realize early detection, early warning and early disposal of risks and comprehensively consolidate the industrial control security protection line.

(3) Emergency Response and Continuous Improvement

Emergency response is the guarantee link of industrial control security governance, which requires the construction of a full-process system of "improved plans, practical drills, collaborative linkage, and traceability and review" to effectively reduce the harm of incidents. Enterprises should customize special plans combined with their own industrial control scenarios, revise and optimize them regularly, carry out normalized practical emergency drills, and implement review and rectification; in case of major security incidents, immediately launch the plan to stop losses, report to the competent department in accordance with regulations, link multiple parties to form a joint disposal force, and conduct a comprehensive traceability and review after the incident to make up for shortcomings. Continuous improvement is a long-term guarantee. Relying on the "assessment - rectification - optimization" mechanism, enterprises conduct regular compliance audits and third-party effect evaluations to quantitatively measure the effectiveness of governance, dynamically optimize the governance system and protection measures in light of technological iteration, policy updates and risk changes, and summarize practical experience and share excellent cases at the same time to promote the steady improvement of the overall industrial control security governance level of the industry.

4 IMPLEMENTATION PATH AND GUARANTEE MEASURES OF THE GOVERNANCE MECHANISM

4.1 Implementation Path

Combined with the actual situation of China's manufacturing enterprises, the implementation of the governance mechanism is divided into three phases to ensure the steady landing and gradual optimization.

4.1.1 Basic construction phase

Core Tasks: Sort out ICS assets and conduct the first comprehensive risk assessment; establish a security management institution and formulate core security management systems; deploy basic technical protection equipment (such as industrial firewalls and network gateways); formulate emergency plans and complete the first tabletop exercise.

Key Objectives: Clarify the asset list and risk levels, and build the basic framework of the governance mechanism.

4.1.2 In-depth construction phase

Core Tasks: Improve the security management system, and conduct special personnel training; deploy intelligent defense equipment such as SIEM platforms and industrial honeypots to realize the intellectualization of technical protection; establish a SOC operation center to realize normalized monitoring and early warning; carry out practical emergency drills and improve the collaborative disposal mechanism.

Key Objectives: Form a three-dimensional collaborative governance system of "management + technology + operation" and improve the risk disposal capacity.

4.1.3 Optimization and upgrading phase

Core Tasks: Conduct governance effect evaluation and compliance audit; dynamically optimize the governance mechanism in light of technological development and risk changes; participate in industry collaborative governance and share governance experience; promote the deep integration of industrial control security and intelligent manufacturing to realize "security empowering production".

Key Objectives: Build a long-term governance mechanism and realize a positive interaction between security and development.

4.2 Guarantee Measures

4.2.1 Policy guarantee

Government regulatory departments should accelerate the improvement of the industrial control security policy and regulatory system, promote the implementation of the 2026 version of the security standard for industrial automation control systems, and strengthen supply chain security review and cross-border data flow management; increase policy support for small and medium-sized enterprises, provide financial subsidies, technical guidance and other services to reduce governance costs; strictly enforce law and supervision, impose legal penalties on enterprises that fail to perform security responsibilities, and form a legal environment where "there are laws to abide by, laws must be observed, law enforcement must be strict, and violations must be prosecuted".

4.2.2 Technical guarantee

Increase investment in the research and development of industrial control security technologies, support universities, research institutions and enterprises to jointly research and develop security technologies and products adapted to intelligent manufacturing, such as AI-driven intelligent defense systems, IIoT device security hardening technologies and supply chain security detection technologies; establish a national industrial information security vulnerability database and threat intelligence platform to realize real-time sharing of vulnerability information and attack situation; promote the application of domestic cryptographic technologies and domestic industrial control equipment to improve the independent and controllable capacity of the supply chain [10].

4.2.3 Resource guarantee

Enterprises should increase investment in industrial control security to ensure that security protection measures are planned, constructed and used simultaneously with ICSs; establish a special security fund for equipment procurement, personnel training, emergency drills and other work; strengthen the construction of talent teams, introduce professional industrial control security talents, and cultivate compound talents who "understand production, technology and security".

4.2.4 Collaboration guarantee

Build a collaborative governance platform for the government, enterprises, suppliers, industry associations and security service providers, and regularly carry out policy publicity, technical exchanges, experience sharing and other activities; establish a collaborative disposal mechanism for major security incidents and clarify the response processes and responsibility division of each subject; promote industry self-regulation, formulate industry security norms, and form a sound governance ecosystem of "government supervision, enterprise main responsibility and social collaboration".

5 CONCLUSION

Focusing on the industrial control security protection needs, this paper takes risk identification as the foundation and the three-dimensional governance dimensions as the support, builds a hierarchical and zonal in-depth protection pattern, improves the dual protection system of "technology + management", and refines the various implementation measures at the management and technical levels, providing a feasible path for enterprises to consolidate the industrial control security protection barrier. With the continuous iteration of intelligent manufacturing technologies, the cybersecurity governance of ICSs still faces many new challenges. Future research can be deepened in three aspects: focus on the security risks of the integration of new technologies such as 6G and generative AI with ICSs, explore in-depth special governance paths, and improve the intelligent defense and responsibility definition system; develop lightweight and low-cost adaptive governance solutions for the pain points of insufficient funds and talents in small and medium-sized enterprises to make up for the shortcomings of industry governance; based on the global characteristics of industrial control security, promote research on international collaborative governance, unify industry security standards, and build a global co-governance protection pattern.

COMPETING INTERESTS

The authors have no relevant financial or non-financial interests to disclose.

REFERENCES

[1] Qin H. A Comparative Study on Information Security Protection of Industrial Control Systems between China and Germany and Its Application Practice. Shanghai Auto, 2026(01): 32-38.
[2] Fan X, Ma Rui. Implementation Path of Industrial Control System Cybersecurity Protection System Under the Background of New Industrialization. Cybersecurity and Informatization, 2025(08): 1-2.
[3] Wang L. Design of a Multi-layer Collaborative Linkage Control System for Intelligent Manufacturing Cybersecurity. Techniques of Automation and Applications, 2024, 43(08): 149-153.
[4] Li J. A Brief Analysis of Industrial Production Process Control System Cybersecurity. Software, 2025, 46(08):184 -186.
[5] Bhamare D, Zolanvari M, Erbad A, et al. Cybersecurity for industrial control systems: A survey. computers & security, 2020, 89: 101677.
[6] Nankya M, Chataut R, Akl R. Securing industrial control systems: Components, cyber threats, and machine learning-driven defense strategies. Sensors, 2023, 23(21): 8840.
[7] Khan S, Madnick S. Cybersafety: A system-theoretic approach to identify cyber-vulnerabilities & mitigation requirements in industrial control systems. IEEE Transactions on Dependable and Secure Computing, 2021, 19(5): 3312-3328.
[8] Ali R F, Muneer A, Dominic P D D, et al. Survey on cyber security for industrial control systems//2021 International Conference on Data Analytics for Business and Industry (ICDABI). IEEE, 2021: 630-634.
[9] Koay A M Y, Ko R K L, Hettema H, et al. Machine learning in industrial control system (ICS) security: current landscape, opportunities and challenges. Journal of Intelligent Information Systems, 2023, 60(2): 377-405.
[10] Ahmad F, Farooq A. Cybersecurity Challenges in Industrial Control Systems. Journal of the Artificial Intelligence Engineers Consortium, 2025, 1(02): 77-86.