Journal of Electronic Research and Application, 2025, Volume 9, Issue 3
http://ojs.bbwpublisher.com/index.php/JERA
ISSN Online: 2208-3510
ISSN Print: 2208-3502

Exploring the Nuclear Power DCS Network Security Management Method and Its Application

Yu Chen[1]*, Yongjie Fu[1], Yajie Wen[2]

[1]Huaneng Xiapu Nuclear Power Co., LTD., Ningde 355199, Fujian, China
[2]Huaneng Nuclear Power Development Co., LTD., Beijing 100031, China

**Author to whom correspondence should be addressed.*

Abstract: Given the grave local and international network security landscape, a national strategic level analysis indicates that the modernization and advancement within the Industry 4.0 era are closely correlated with overall competitive strength. Consequently, China proposed a strategy for the integration of industrialization and informatization, optimizing and adjusting its industrial structure to swiftly achieve transformation and upgrading in the Industry 4.0 era, thereby enhancing the sophistication of intelligent industrial control systems. The distributed control system in a nuclear power plant functions as an industrial control system, overseeing the operational status of the physical process. Its ability to ensure safe and reliable operation is directly linked to nuclear safety and the cybersecurity of the facility. The management of network security in distributed control systems (DCS) is crucial for achieving this objective. Due to the varying network settings and parameters of the DCS implemented in each nuclear power plant, the network security status of the system sometimes diverges from expectations. During system operation, it will undoubtedly encounter network security issues. Consequently, nuclear power plants utilize the technical criteria outlined in GB/T 22239 to formulate a network security management program aimed at enhancing the operational security of DCS within these facilities. This study utilizes existing network security regulations and standards as a reference to analyze the network security control standards based on the nuclear power plant's control system. It delineates the fundamental requirements for network security management, facilitating integration with the entire life cycle of the research, development, and application of the nuclear power plant's distributed control system, thereby establishing a network security management methodology that satisfies the control requirements of the nuclear power plant. Initially, it presents DCS and network security management, outlines current domestic and international network security legislation and standards, and specifies the standards pertinent to the administration of DCS in nuclear power plants. Secondly, the design of network security management for DCS is executed in conjunction with the specific context of nuclear power plants. This encompasses the deployment of network security apparatus, validation of the network security management strategy, and optimization adjustments. Consequently, recommendations beneficial to the network security management of nuclear power plants are compiled, aimed at establishing a management system and incorporating the concept of full life cycle management, which is predicated on system requirements, system design, and both software and hardware considerations. Conversely, it presents the notion of comprehensive life cycle management and suggests network security management strategies encompassing system requirements, system architecture, detailed hardware and software design and implementation, procurement, internal system integration, system validation and acceptance testing, system installation, operational

maintenance, system modifications, and decommissioning. We will consistently enhance the performance and functionality of DCS in nuclear power plants, establish a safe and secure operational environment, and thereby facilitate the implementation of DCS in nuclear facilities while ensuring robust network security in the future.

Keywords: Network security; DCS; Nuclear power plant; Network security management

Online publication: 5 June, 2025

1. Introduction

The escalating intensity of cybersecurity threats has attracted significant focus in the realm of national security. From a strategic standpoint, the modernization of industrial systems has markedly enhanced overall competitiveness. Simultaneously, China has advocated for a strategy that underscores the profound integration of industry with information technology. This project has enhanced industrial frameworks and facilitated progress in industrial control systems, increasing digitization levels. In light of the current intricate security threat environment, distributed control systems (DCS) are extensively utilized in nuclear power facilities and have become vital industrial control systems. DCS utilizes open digital information technology and integrated systems to improve productivity and efficiency in nuclear power facilities. Nonetheless, it also presents cybersecurity concerns. As a result, federal authorities have prioritized this matter, releasing guidelines and regulation documents. Nuclear power, a typical clean energy source, mandates that all manufacturing and construction activities adhere to rigorous industry rules, including implementing DCS cybersecurity management protocols.

2. Relevant concepts and theoretical foundations

2.1. Related concepts

The Distributed Control System (DCS), an essential industrial control system, is based on microprocessor technology. The design integrates sophisticated technologies that provide dispersed control, centralized display, and autonomous coordination [1]. Multi-tiered hierarchical frameworks and collaborative independence define it. Upon implementation in nuclear power plants, DCS improves its initial control modes, facilitating centralized management and distributed control. **Figure 1** depicts the configuration of a standard Distributed Control System (DCS).

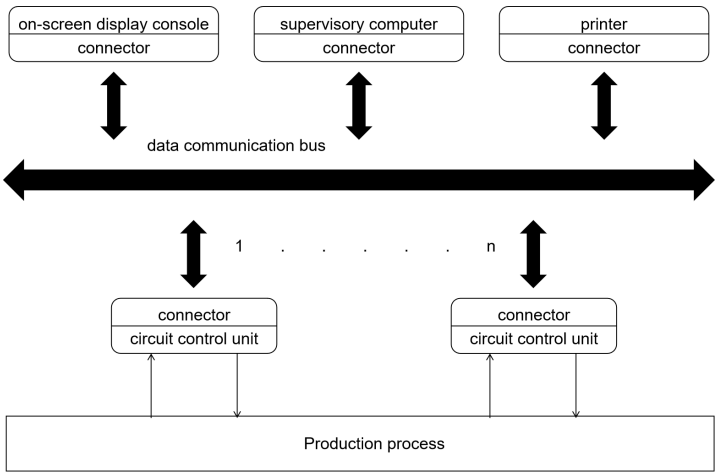

Figure 1. Diagram of the Distributed Control System (DCS)

The internal architecture of a Distributed Control System (DCS) of a nuclear power facility includes (1) Control station systems, which consist of hardware boards or modules, and (2) Human-Machine Interface (HMI) systems, which contain servers and engineering workstations. Nuclear power facilities effectively gather field data from sensors and perform control operations through these components. In reactors, the DCS functions as the "central nervous system," delivering real-time data for maintenance and operational decision-making.

2.2. Theoretical foundations

(1) Security policy and strategy theory: The existing condition of DCS network security management in nuclear power plants indicates that security policy and strategy theory constitute the theoretical basis for efficient cybersecurity management. Formulating security policies elucidates essential objectives and principles, facilitating focused management strategies [2]. Security rules also structure DCS-related criteria, including personnel, equipment, and application software.

(2) Risk assessment and management theory: Nuclear power facilities can systematically investigate potential DCS network security issues through risk assessment and management theory. This facilitates the identification and evaluation of hazards and the formulation of appropriate risk management frameworks. These frameworks encompass preventive techniques and control measures designed explicitly for the identified vulnerabilities.

3. Cybersecurity regulations and standards

3.1. Domestic management requirements

Since 1999, China has adopted a multitude of cybersecurity recommendations and legislation. The initial standard, GB17859–1999, set criteria for classifying computer information system security. In 2014, the National Development and Reform Commission promulgated the "Security Regulations for Power Monitoring Systems," introducing the sixteen-character policy: "zoning by security levels, dedicated networks, horizontal isolation, and vertical authentication" [3]. In 2019, GB/T 22239–2019 delineated 10 security control domains and established standards for Level 4 security comprising 250 control points, highlighting that security management constitutes 50% of the total requirements (**Figure 2** and **Table 1**). In 2022, the Energy Bureau introduced the "Cybersecurity Management Measures for the Electric Power Industry," advocating for extensive protection frameworks and explicit responsibility mechanisms.

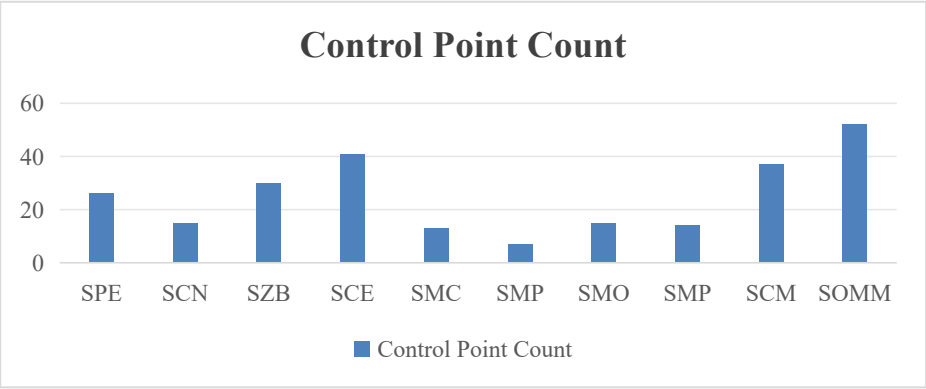

Figure 2. Security grade protection level 4 specifications

Table 1. The abbreviation for each element

Element name	Abbreviation
Secure physical environment	SPE
Secure communication network	SCN
Secure zone boundary	SZB
Secure computing environment	SCE
Security management center	SMC
Security management policy	SMP
Security management organization	SMO
Security management personnel	SMP
Security construction management	SCM
Security operation and maintenance management	SOMM

3.2. International management requirements

RG1.152 guide: The U.S. Nuclear Regulatory Commission (NRC) establishes cybersecurity mandates under federal regulations aimed at nuclear safety. It takes into account system design variety, defense-in-depth, and more factors [4]. The RG1.152 handbook encompasses the complete lifespan, from concept creation to decommissioning, addressing system design, security function implementation, and operational reliability.

RG5.71 guide: Alongside RG1.152, the NRC formulated RG5.71 to handle cybersecurity for computer systems in nuclear facilities [5]. This document delineates extensive supervision tactics focused on organizational frameworks, security technologies, and operational management, addressing potential threats, vulnerabilities, and harmful incursions.

4. Design of DCS cybersecurity management

4.1. Deployment of security equipment

This study's DCS cybersecurity design considers the practical requirements of nuclear power plants and employs a logical placement of security management devices. **Figure 3** depicts a suggested deployment strategy. When security management devices connect to the A-side of the Layer 2 network, operators can access the management interface through the engineering workstation. Operators can utilize the security network to back up logs and provide alerts for future threats [6]. **Table 2** delineates the functions and performance specifications of pertinent security management apparatus.

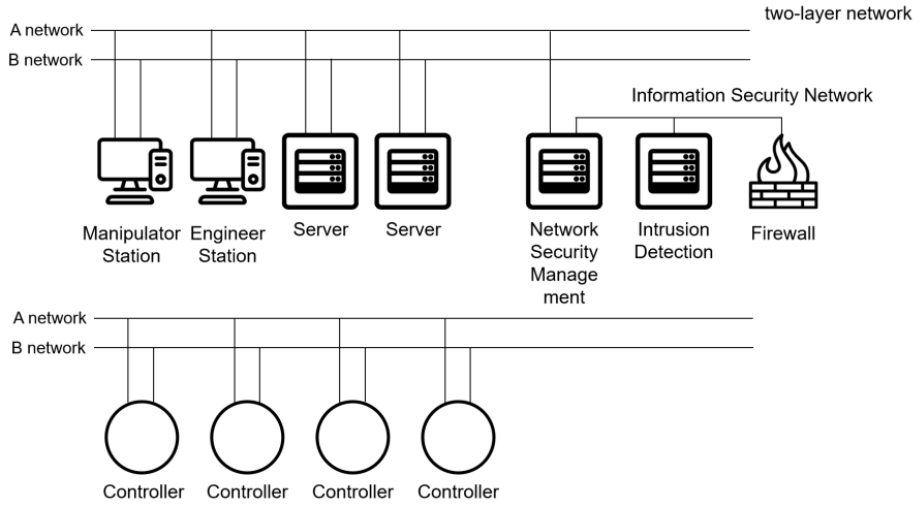

Figure 3. Security equipment deployment strategy

Table 2. Functions and performance of security management equipment

Function/performance		Description
Function	Security control interface	Integrates security monitoring data across all control systems. Provides centralized oversight and alerts for potential threats.
	Industrial safety monitoring topology	Establishes a comprehensive monitoring platform showing security data and network activity for DCS. Provides a physical topology for clear network status visualization.
	Centralized audit of control nodes	Audits network devices and second-layer nodes via the A network using Simple Network Management Protocol (SNMP).
	Audit logging	Displays and archives firewall and intrusion detection alerts in real-time.
Performance	Log collection rate	>10,000 logs/second
	Search time for 100 million records	<2 seconds
	Gigabit network ports	>2
	Alarm log retention	More than six months

4.2. Compliance verification

By the security criteria outlined in GB/T 22239–2019 for Level 4 protection, a fortified DCS must undergo compliance verification in system management, audit management, security management, and centralized control.

System management: Verifying the administrator's identity is essential for accessing resources and configurations. Actions require auditing. The engineering workstation facilitates offline configuration, online debugging, and data backup [7].

Audit management: Security audit records must be maintained in real time. Logs are available for examination and analysis, assuring adherence to regulations.

Security management: Security administrators establish security policies. Devices adhere to uniform policy configurations for security classification and validation [8].

Centralized control: Management zones are established, guaranteeing safe paths and surveillance of real-time network and device conditions [9].

4.3. Optimization

Recommendations for improving DCS cybersecurity encompass [10]:

Enhancing device compatibility: Improve interface compatibility among various security devices to reduce hazards associated with brand incompatibilities [11].

Employing a security management center: Centralize operational control by enhancing the design-phase security zones for thorough supervision [12].

Creating new interfaces: Facilitate uninterrupted communication between switches and security apparatus.

Redundancy mechanisms: Establish redundant networks with dual connections to enhance reliability and reduce hazards [13].

HMI enhancements: Facilitate instantaneous security notifications via integrated visual and auditory alarms.

5. Recommendations for DCS cybersecurity management

5.1. Building a security quality management system

A comprehensive security quality management system incorporates GB/T 19001–2016 and GB/T 45001–2020 standards through PDCA cycles, encompassing all aspects of the DCS lifetime. Management must consistently modify rules through system alterations, resource accessibility, and safety mandates [14].

5.2. Multi-phase lifecycle management

Effective network security management should be applied throughout the DCS lifecycle stages:

System specifications phase: Establish cybersecurity specifications for control systems [15].

System design phase: Detect weaknesses and enhance system architecture for robustness [16].

Procurement and integration: Effective supply chain management guarantees secure sourcing and execution [17].

Verification and testing: Stringent testing confirms design integrity and security [18].

Operational maintenance: Consistent risk evaluations ensure enduring security [19].

System modifications and decommissioning: Administer alterations judiciously to prevent the introduction of vulnerabilities [20].

6. Conclusion

This study underscores the necessity of robust cybersecurity solutions for DCS in nuclear power facilities. Nuclear power plants may establish strong defense mechanisms to safeguard vital systems from developing cybersecurity threats by integrating lifecycle management, adopting global standards, and optimizing security frameworks.

Disclosure statement

The authors declare no conflict of interest.

References

[1] Zhang S, 2024, Analysis of the Application of Safety Grade DCS in Low Voltage Distribution Systems of Nuclear Power Plants. Electrical Technology and Economics, (10): 100–102 + 106.

[2] Shi C, 2024, Installation and Debugging of External Redundant Backfilling Historical Database Based on IA-DCS System. Electrical Technology, (19): 206–208.

[3] Zhang X, Liu Q, Peng H, et al., 2024, Design and Implementation of Automatic Generation System for Nuclear Safety DCS Electrical Installation Information. Industrial Control Computer, 37(09): 17–19 + 22.

[4] He C, Zhang P, Liu S, et al., 2024, Research on Improvement of Logic Verification Scheme for Nuclear Power Plant Control System. Automation Instrumentation, 45(09): 20–26.

[5] Hu Q, Peng H, Liu H, et al., 2024, Research on Default Value Setting Strategy for Safety Level DCS in Nuclear Power Plants. Automation Instrumentation, 45 (09): 14–19.

[6] Wang P, Wang K, Liu Y, et al., 2024, Research on Engineering Design Optimization of Safety Level DCS T2 Periodic Test Cases Based on NASPIC Platform. Automation Application, 65(17): 155–158.

[7] Liu Y, 2024, Analysis of Interface Issues in Nuclear Power Plant Reactor Power Control System. China Nuclear Power, 17(04): 585–592.

[8] Chen J, Jin J, Xiao A, et al., 2024, Verification and Confirmation of Default Values for Safety Level Digital Instrumentation and Control Systems in Nuclear Power Plants. Instrumentation Technology, (04): 44–48.

[9] Liang K, Chu J, Cao Y, 2024, Research on the Design Method of Manual and Automatic Switching for Safety Level DCS in Nuclear Power Plants. Science and Technology Vision, 14(20): 31–34.

[10] Jiang M, He Q, 2024, Exploration of Improving the Quality of Digital Control System Design in Nuclear Power Plants. Science and Technology Perspective, 14(20): 47–49.

[11] Liu Y, 2024, Reliability Analysis of LOCA Monitoring System in Nuclear Power Plants and Construction of Redundant System. Electrical Technology, (13): 196–198.

[12] Dan W, Ren J, Peng W, et al., 2024, Research on Anti-Noise Coding for Next Generation Nuclear Power DCS Communication System. Nuclear Power Engineering, 45(04): 274–279.

[13] Leng Q, Yang Y, Hu Y, 2024, Communication Technology of Non-safety DCS System for Nuclear Power Based on Multicast. China Science and Technology Information, (12): 102–104.

[14] He J, Jiang L, 2024, Application and Implementation of CNN-based OCR Technology in DCS System Testing of Nuclear Power Plants. Nuclear Science and Engineering, 44(03): 543–550.

[15] Zhang B, 2024, Case Study on the Whole Process Innovation of DCS from Design to Debugging in a Nuclear Power Plant. China Instrument and Meter, (04): 35–38.

[16] Jing Z, 2024, Design and Research of Communication Framework for DCS System of Nuclear Power Plant Simulator. Application of Electronic Technology, (S1): 65–68.

[17] Deng Z, Wang G, Li G, et al., 2024, Design of Intelligent Online Inspection Based on Nuclear Power DCS System. Automation Expo, 41(03): 58–63.

[18] Xu Y, Yang W, Liu S, et al., 2024, Research and Practice on the Renovation Plan of Manual Operators in the Main Control Room of Nuclear Power Plants Based on Digital Systems. Nuclear Power Engineering, 45(02): 187–192.

[19] Wang T, Ma J, Peng Y, et al., 2023, Analysis and Response to the Problem of Automatic Loading of Chiller Units in a Certain Nuclear Power Plant. HVAC, 53(S2): 328–330.

[20] Yu G, Tian Q, Peng F, et al., 2023, Research on Information Security Protection Method of DCS Logic Configuration Software for Nuclear Power Plants Based on State Secrets Algorithm. Manufacturing Automation, 45(12): 61–64.