The Security Based on Wireless Network in Nuclear Power Plant

Dong Zhang(✉) and Sheng-Yong Liao

Beijing Institute of Nuclear Engineering I&C Division,
China Nuclear Power Engineering Co., Ltd., Beijing 100086, China

Abstract. The wireless communication technology has been widely used in daily life, bringing great convenience to our lives. Its low cost, easy maintenance and high flexibility can also bring benefits to the nuclear industry [1]. This paper analyzes the wireless network application prospects and benefits in nuclear power plants. For the application of wireless networks in nuclear power plants, the security risks of wireless networks are introduced, and the specific requirements of domestic and foreign network security standards on the application of wireless networks in industrial fields are combed. Finally, the security protection strategies and recommendations of wireless networks in nuclear power plants are proposed.

Keywords: Nuclear power plant · Wireless network · Security · Risk · Prevention

1 Application Background of Wireless Network in Nuclear Power Plant

Industrial wireless technology is a hotspot technology in the field of industry. It is a revolutionary technology that reduces the cost of industrial control systems and improves the efficiency of industrial control systems [1]. Most industrial sites have complex factory buildings and many installation equipments, which make it difficult to lay cables, maintenance, and cost. Nuclear power plants also have the above problems, and wireless technology has the following advantages in solving the above problems: low cost, high reliability, easy maintenance, and high flexibility [2, 3].

Wireless technology has been used for audio and video communication, mobile inspection and personnel positioning in nuclear power plants, which has brought great convenience to the operation and maintenance of nuclear power plants. With the gradual maturity of wireless technology and the inevitable trend of industrial Internet development, the application of wireless technology in nuclear power plants will become more and more extensive. In response to the business needs of nuclear power plants, the application of wireless networks has the following benefits [4]:

- Reduce operation and maintenance pressure and eliminate personnel injuries: reduce the pressure of personnel inspection and maintenance through video surveillance, mobile inspection and mobile maintenance technologies;

Y. Xu et al. (Eds.): SICPNPP 2020, LNEE 779, pp. 64–70, 2021.
https://doi.org/10.1007/978-981-16-3456-7_8

- Prevent human errors: The smart technology and smart meters supported by the wireless network have more standardized operation, which can reduce the intervention of personnel and improve the standardization of operation.
- Reduce the cost of power plant: After the wireless network is used to replace the wired network, the procurement cost of the wired cable can be reduced, and the laying cost and the maintenance cost at a later stage can be saved.
- Optimizing design ideas: Wireless technology provides new methods for the design of power plants, which can be used to optimize the design ideas of power plants. Under the premise of meeting the standards and regulations, the design of power plants will be optimized, and smart nuclear power plants will be built in conjunction with internet technology.

The application of wireless networks should meet the functional requirements of nuclear power plants and the particularity of application scenarios. These particularities include the following:

- The influence of the radiation dose of part of the nuclear power plant on the wireless network;
- The interaction between the electromagnetic interference of the wireless network and the existing equipment;
- The network security risks of open wireless technology standards, including the network security of mobile terminals and mobile application;
- The problem of wireless access to special closed room such as reactor buildings;
- Ease of maintenance.

Therefore, the wireless network should solve the above-mentioned matters and customize development accordingly before the application in nuclear power plants. This article will focus on introducing the network security risks of wireless networks, comparing and analyzing the standards and regulations of wireless network security in nuclear power plants, and proposing the precautions that need to be considered in the application of wireless networks in nuclear power plants.

2 The Security Risks of Wireless Network in Nuclear Power Plants

While wireless technology brings convenience, the accompanying network security risks should also be considered simultaneously. The main security problems faced by wireless networks are:

- Wireless intrusion: Because the wireless network uses radio waves as the transmission medium, the physical range of the network is difficult to control, and it can be spread to areas outside the expected location, making illegal intrusion an opportunity.
- Improper device configuration: The user's security awareness is weak. After the wireless device is enabled, the default configuration is not modified in time, and no security configuration such as encryption is performed.

- Unauthorized AP (Access Point) access: Unauthorized APs can connect to the network without authorization, such as forged IP (Internet Protocol) or MAC (media access control) address attacks.
- Advanced intrusion: The wireless network is a directly exposed boundary device. Once the wireless network device is invaded, a new intrusion can be initiated directly into the internal network through the device.
- Wireless viruses: Wireless network viruses can destroy wireless devices and computer hosts in the wireless device network through the network.
- Equipment backdoor: Wireless network equipment also contains software and systems, facing manufacturers or developers who keep program backdoors during the development process. Due to the particularity of wireless network equipment, these backdoors are more likely to be used to launch network attacks.

Therefore, the application of wireless networks must be premised on proper network security protection.

3 Analyses of Wireless Network Security Regulations and Standards

Different wireless technologies separately follow the technical requirements of standards, such as IEEE 802.11, IEEE 802.15 and other series of standards. These standards require the security of the wireless technology from protocol. This paper analyzes and compares the specific requirements of wireless technology from industrial and nuclear power network security standards, which are additional requirements on wireless for security. The main standards selected in this paper are GB/T22239, IEC62988, IEC62443, NIST-SP800-82 and NIST-SP800-94, required scope of the standards, see Table 1 for details [5, 7–10]. Wireless physical security, identity authentication, access control, boundary isolation, intrusion prevention, security audit, configuration management and data backup and recovery are mentioned.

Table 1. Scope analysis of wireless security standards

Items	GB/T22239	IEC62443	IEC62988	NIST SP800-94	NIST SP800-82
Physical security	√	√	√	—	√
Identity authentication	√	√	√	—	—
Access control	√	√	—	—	√
Boundary isolation	√	—	√	—	—
Intrusion prevention	√	√	√	√	√

(*continued*)

Table 1. (*continued*)

Items	GB/T22239	IEC62443	IEC62988	NIST SP800-94	NIST SP800-82
Malicious code prevention	√	√	√	—	—
Security audit	—	—	√	—	—
Configuration management	√	—	√	—	√
Data backup and recovery	√	—	—	—	—

Note:
"√" means the standard has the related requirement;
"—" means the standard has no related requirement.

- GB/T 22239 is the basic requirement of domestic information system network security for information system. Among them, the expansion requirements of mobile internet and industrial control system stipulate the general requirements of wireless network security, which can cover the basic requirements of wireless network security. However, the underlying standards for wireless applications in the industrial field are not perfect, and detailed guidance is lacking.
- IEC 62443 is a series of standards of industrial communication network security. Among them, the 2–4 sub-standards "Security program requirement for IACS service providers" stipulate the application scope and main protection points of wireless networks in industrial control systems, and emphasize wireless protocol should be compatible with the network of the industrial control system to ensure that wireless technology will not negatively affect the industrial control system.
- IEC 62988 is a wireless selection and application requirement for nuclear power plant safety important instrumentation and control systems. It stipulates the application scope of wireless technology in different function classification instrumentation and control systems of nuclear power plants. It also provides wireless security requirements, such as isolation requirements between networks, wireless monitoring and logging requirements, etc.
- NIST-SP800-94 is one of the standards of the American Institute of Standards and Technology for network security. It introduces the application principles, technical guidance, and product selection of intrusion detection and prevention systems (IDPS). From the perspective of security equipment, clear requirements for wireless network security.
- NIST-SP800-82 is the guidance of the American Institute of Standards and Technology for industrial control system network security. It provides a brief provision on wireless network identity authentication, encryption methods and the relationship with industrial control systems.

These standards consider the security of wireless networks. The application of wireless networks in nuclear power plants should comply with the requirements of IEC62988 for the application scope, integrate the security considerations of various standards, and analyze and study the protection strategies that wireless networks should consider in the application of nuclear power plants.

4 Nuclear Power Plant Wireless Network Security Protection Strategy

4.1 Application Range of Wireless Network

Due to the special consideration of wireless technology network security, its application in nuclear power plants should be limited to a specific range. From different perspectives, the application limitations of wireless networks are as follows:

- From the perspective of business characteristics, the application of wireless communication technology is limited to non-production business and production business unrelated to safety [6].
- From the perspective of functional classification of nuclear power plants, the application of wireless communication technology is limited to the implementation of category C and NC class functions required by IEC61513, and is prohibited to perform the functions of category A and B.
- From the perspective of the functional structure of the DCS system, wireless communication technology is limited to the data exchange between the layer 1 network and the layer 0 wireless instrument, layer 2 network and layer 3 network.

4.2 Wireless Network Security Protection Measures

Nuclear power plant wireless network security should follow the defense strategy of defense-in-depth, and prevent and control from the perspective of basic protection, security detection, security audit, and security operation and maintenance. The prevention and control measures cannot cause unacceptable impact on the functional safety of the system. The protection strategy is shown in Fig. 1.

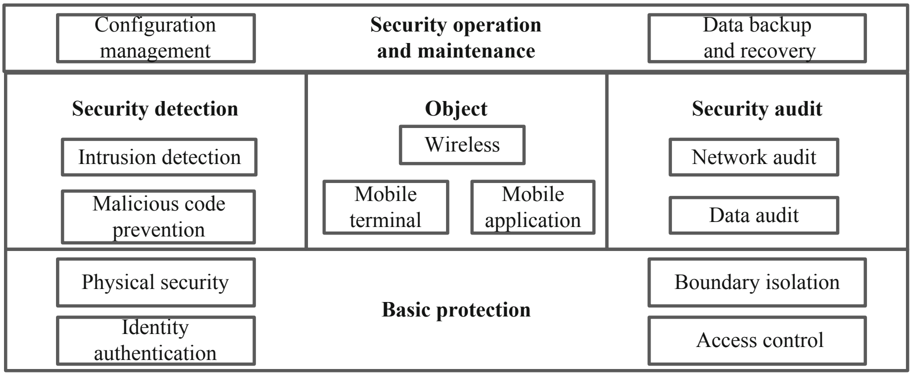

Fig. 1. The protection strategy of wireless network in nuclear power plant

(1) Object
The objects of nuclear power plant wireless network security protection are mainly wireless network sites, switches and access points. In addition, we should also consider the security of wireless sensors, mobile terminals, and smart mobile applications connected to it to achieve comprehensive protection.

(2) Basic protection
Basic protection is the basic requirement for the network security of the protected objects, mainly including physical security, identity authentication, boundary isolation and access control.

- Physical security: The positioning of wireless equipment is considered in combination with environmental conditions, power supply, grounding, and wireless power requirements;
- Identity authentication: The wireless network should use a unique identity for authentication, and all messages should be authenticated;
- Boundary isolation: Ensure that the access and data volume between the wired network and the wireless network boundary pass through the isolation device for boundary protection to prevent the wireless network risk from spreading to other networks that interface with it, especially high-security-level networks;
- Access control: The wireless access device should enable the access authentication function, use a unique service setting identifier (SSID), and allow the device with the minimum IP and MAC address identification to access.

(3) Security detection [11]
Security detection requires detection and prevention of internal and external intrusions in wireless networks.

- Intrusion detection: It should detect unauthorized wireless devices in the operating environment and report unauthorized access or interference with the system.
- Malicious code prevention: Wireless network communication should be encrypted.

(4) Security audit
The wireless network should be equipped with audit equipment to record the data and network status of the wireless equipment.

(5) Security operation and maintenance
The configuration and management of wireless network equipment, as well as data backup and recovery after a network attack, should be considered from the perspective of operation and maintenance.

- Configuration management: Establish wireless device library to identify illegal wireless access devices; the requirements, impacts and procedures of configuration changes should be clarified and can be implemented after strict approval.

- Data backup and recovery: According to the needs of the business, the backup method, backup frequency, storage medium, and storage period should be specified. Establish data recovery procedures and clarify implementation methods and personnel responsibilities.

5 Summaries

The application of wireless networks in the industrial field is at an exploratory stage and is currently mainly considered in the non-production business of nuclear power plants. But precisely because it is in its infancy, it should consider its network security risks as a whole and deploy network security measures to improve its business level while ensuring that network security risks are manageable.

With the maturity of wireless technology and the improvement of security, it will also bring huge benefits to the production business of nuclear power plants [12]. Of course, this process requires the improvement of relevant standards and regulations and the exploration of technicians to work together to achieve the standardization and secure application of wireless networks in nuclear power plants.

References

1. Zeng, P., Xu, D.-K.: Applications of industrial wireless technologies in oil-gas industry. Technology of Industrial Wireless Communication (2008)
2. Fang, Y.-B.: Discussion of industrial wireless network engineering design. Automation in Petro-Chemical Industry (2012)
3. Fang, Y.-B.: Device types of industrial wireless network. Process Automation Instrumentation (2015)
4. Zeng, P.: Standardization and application of industrial wireless. China Instruments (2008)
5. GB/T 22239: Information security technology-baseline for classified protection of cybersecurity (2019)
6. IEC 62859: Requirement for coordinating safety and cybersecurity (2016)
7. IEC62988: Nuclear power plants-Instrumentation and control systems important to safety-selection and use of wireless devices (2018)
8. IEC62443: Security for industrial automation and control systems – part 2–4: security program requirements for IACS service providers (2017)
9. NIST-SP800-82: Guide to industrial control systems (ICS) security (2015)
10. NIST-SP800-94: Guide to intrusion detection and prevention system (IDPS) (2015)
11. Li, W.-Y., He, W.-X., Tan, B.: Research and practice of wireless security monitoring and protection. Cyberspace Security (2018)
12. Gao, H.-R.: The situation and future development of wireless industrial networks. China Instruments (2008)