New cybersecurity standards for IACS of the nuclear power industry in China

Yun Guo[1], Junjie Wang[1]

Abstract: As of June 2022, China has ranked second with respect to the number of nuclear power plants (NPPs) under construction and in operation in the world. It's expected that China's installed nuclear power capacity will reach about 70 million kilowatts by 2025 [1]. At present, industrial control systems of China's new NPPs have adopted digital industrial ones, and existing NPPs are gradually evolving from a mixture of digital and analog to full digital technology, which has brought great challenges to the cyber security of nuclear power plants. The cyber attack on the industrial control systems of NPPs may not only lead to interruptions in the production process, but also may cause nuclear safety incidents. Therefore the Standardization Administration of the People's Republic of China and relevant industry regulatory departments have respectively developed national and industry level standards regarding the cybersecurity of industrial control systems of nuclear power plants in recent years. This report introduces China's new standards on the cyber security of industrial control systems in NPPs, analyzes their relationship with relevant international standards, puts forward the issues that need to be considered regarding the coordination of those standards, and provides reference for the subsequent development of new international standards.

Keywords: nuclear power plants, cybersecurity standards, nuclear safety, Industrial Automation and Control System, I&C

1 Introduction

The Industrial Automation and Control Systems (IACSs) of the nuclear power plants (NPPs) perform the monitoring, control and protection functions of the entire NPP. For a long time, IACSs of NPPs have physically isolated from other external systems and use dedicated hardware and software to run proprietary protocols, so it is viewed traditionally that the IACSs of NPPs are less likely to be affected by cyberattacks. However, with the trend of digitalization, networking and intelligence of global industry, IACSs of NPPs have been facing more and more cyber challenges, mainly reflected in: First, with the need for digital development, the communication between IACSs and external systems has increased, such as the connection between a SIS and distributed control system (DCS) to obtain relevant production data. Secondly, there are also more ways to break through physical isolation, such as reserving backdoors and implanting viruses during the development phases, spreading worms through mobile media during the operational phase, stealing information through laptop access during the maintenance phase, and even breaking through physical protection systems through social engineering

[1] Huaneng Shandong Shidao Bay Nuclear Power Company, ShanDong, China

doi:10.18420/inf2022_137

methods. Finally, the proprietary nature of IACSs and protocols can only temporarily increase the difficulty of the attack and the threshold for the attack is constantly lowered, since IACSs begin to use more and more common schemes, such as industrial communication based on Ethernet and TCP/IP protocol, workstations based on Windows operating system, HMI based on web browser mode. Along with the improvement of the open interconnection, those general solutions also leads to the increasingly serious cybersecurity threats. From the "Stuxnet" incident in Iran in 2010 [2]to the nationwide blackout in Ukraine in 2016, events in recent years have shown that cybersecurity has become an important influencing factor in the operational safety as well as more serious nuclear safety consequences of nuclear facilities[3]. Therefore, the cybersecurity of IACSs of NPPs have attracted great attention of the nuclear energy related community.

To dress those issues, countries around the world and relevant international organizations have carried out relevant research on the issue of IACS cybersecurity in NPPs and formulated corresponding standards and regulatory requirements. For example, the International Electrotechnical Commission (IEC) began to develop an international standard IEC 63096 [4]in 2016, with the aim of providing detailed security control guidelines based on hierarchical and lifecycle-specific method for IACSs of NPPs, helping all stakeholders of NPPs prevent, detect and react to cyberattacks to ensure the availability, integrity and confidentiality of IACSs. Also, the U.S. Nuclear Regulatory Commission (NRC) has developed computer security guideline RG 5.71 [5]for nuclear facilities in accordance with the protection requirements of the Federal Regulations for digital computers, communication systems and networks, with the purpose of ensuring that digital computers and communication systems and networks related to nuclear facilities are adequately protected from cyber attacks. As the second country in the world in terms of the number of nuclear power units currently in operation and under construction, China has also made exploration of relevant standards in recent years. With regard to actual cybersecurity implementation, NPPs often need to consider multiple standards, thus making the coordination of different standards essential and critical. To this end, this paper introduces China's relevant standards on the cybersecurity of IACSs in the nuclear power industry, analyzes their relationship with relevant international standards. Based on that, the paper puts forward the problems that need to be considered when coordinating the use of those standards, providing a reference for implementing the security measures in NPPs as well as a reference for the subsequent development of relevant international standards.

2 New cybersecurity standards for IACSs of NPPs in China

2.1 Series of Standards for Classified Protection of Cybersecurity

Beginning in 1994 with the State Council's Decree “Regulations on the Security Protection of Computer Information Systems of the People's Republic of China”, China’s classified protection of cybersecurity was gradually promoted in an orderly

manner and was fully applied in various industries. The series of classified protection standards including more than 10 standards such as GB/T22239 [5]、GB/T22240 [6]、GB/T25070 [7]、GB/T 28448 [8]、GB/T 28449[9], which covers classification guide, baseline requirements, implementation guide, assessment requirements, etc. At the same time, the series of those standards have also been updated in a timely manner according to the new situation and new risks in cyberspace. Those standards and release time is listed in table 1.

Table 1: series of standards for classified protection of cybersecurity

Number	Name	Release time
GB/T 22239	Baseline for classified protection of cybersecurity	2019
GB/T 25070	Technical requirements of security design for classified protection of cybersecurity	2019
GB/T 28448	Evaluation requirements for classified protection of cybersecurity	2019
GB/T 28449	Testing and evaluation process guide for classified protection of cybersecurity	2018
GB/T 36958	Technical requirements of security management center for classified protection of cybersecurity	2018
GB/T 25058	Implementation guide for classified protection of cybersecurity	2019
GB/T 22240	classification guide for classified protection of cybersecurity	2020

The relevant standards for cybersecurity classified protection 2.0 have been released since May 2019, and a significant change in the new standards is to change the original security requirements to security general requirements and security extension requirements, of which the security general requirements are still divided into technical requirements and management requirements, but the lower-level requirements are changed from the previous standards. Under this framework, the technical requirements and management requirements both include five second-level requirements and they are listed as table 2.

Table 2: baseline requirements of for classified protection of cybersecurity

First-level requirements	second-level requirements
general technical	secure physical environment

requirements	secure communication network
	secure area boundary
	secure computing environment
	security management center
general management requirements	management system
	management organization
	management personnel
	construction management
	operation and maintenance management
extension requirements	cloud computing security
	mobile connecting security
	IoT security
	IACS security

The main differences between the new series and the previous series include:

- The new standards expand the scope incorporating cloud computing, mobile internet, Internet of Things, IACS etc. into the scope of standards.
- It is now recommended to use the triple protection architecture supported by secure communication network, secure boundary and secure computing environment along with the management center.
- The requirements of TC (Trusted Computing) technology are strengthened in this version.

2.2 GB / T 41241-2022 Management requirements for cybersecurity of industrial control systems in nuclear power plant

In 2022, the Standardization Administration of China issued GB/T 41241[10] "management requirements for cybersecurity of industrial control systems in nuclear power plant", which is based on the basic requirements of GB/T 22239 and combines the actual needs of NPPs to stipulate the requirements for the management, technical protection and emergency management for cybersecurity of industrial control systems NPPs. This standard applies to cybersecurity activities of all phases of the life cycle of IACSs of nuclear power plants (including design, development, engineering

implementation, operation and maintenance, decommissioning, etc.). It also applies to system maintenance activities that guide users of IACSs of NPPs to improve and enhance the cybersecurity protection capabilities.

This standard proposes the concept of cybersecurity fortification degree which is divided into 1-5 levels, and recommends that the fortification degree be classified according to the maximum consequences of the impact on nuclear safety and power generation after a successful cyber attack on the system. This standard provides a recommended correspondence between the cybersecurity fortification degree and that of the national classified protection series of standards.

3 Issues to be considered in the coordination of standards

3.1 Coordination of Security Degree

The most significant feature of IACSs in NPPs compared with traditional IT systems and IACSs of other industries is that the character of a hierarchical strategy used by IACSs in NPPs. To be specifically, IACSs of NPPs perform functions related to nuclear safety. From the design stage, IACSs of NPPs needs to implement the "classification strategy", that is, the instrumentation and control (I&C) function is first classified according to its nuclear safety importance, and then IACSs that perform different functional categories is classified according to the functional classification. Therefore, the cybersecurity of IACSs in NPPs need to consider its correlation with nuclear safety in terms of determining the degree of protection and the choice of protective measures.

At present, whether it is China's national standards or the relevant standards of international organizations such as IEC, they have put forward proposals for hierarchical protection for IACSs of NPPs, but the criteria for grading seems different intuitively. For example, IEC 63096 inherits the method of cybersecurity grading in IEC 62645[11]. Upon that, based on the classification of I&C functions and the analysis of the maximum consequences imposed on the nuclear safety level and performance of power plants after the successful implementation of cyberattacks, the cybersecurity degree of IACSs in NPPs is divided into S1, S2, S3. Further, IEC 63096 also defines a "BR" degree which means all IACSs in NPPs that are not classified as S1, S2, S3 are classified as BR and should follow the security control recommendations of the BR degree. In this sense, it can be considered that IEC 63096 includes 4 cybersecurity degrees for IACSs, whereas there is 5 degrees in China’s classified protection system and the cybersecurity fortification degree in GB/T 41241 is also divided into 5 levels. Therefore, how to establish an appropriate correspondence between these degrees due to different standards is crucial to the actual implementation work. It should be noted that this correspondence is usually not a one-to-one correspondence.

3.2 Coordination of Security Controls

The Chinese national standard GB/T 22239 puts forward protection requirements for different degrees of systems from three aspects: general management requirements, general technical requirements and expansion requirements, whereas IEC 63096 also proposes the security controls applicable to different life cycle stages for IACSs of NPPs with different security degrees. In fact, there is a strong overlap between the two. For example, the relevant requirements for the recruitment of personnel in the basic requirements for classified protection include "a) special departments or personnel shall be designated or authorized to be responsible for the recruitment of personnel; b) the identity, security background, professional qualifications shall be reviewed, and the technical skills possessed by the recruited personnel shall be assessed; c) confidentiality agreements should be signed with the recruited personnel and post responsibility agreements should be signed with the key positions", and the control measures on the "Prior to employment" of human resource security in IEC 63096 propose that "the organizational units in charge of I&C platform development, I&C system engineering and construction/ operation should have inventory of assets relevant to cybersecurity. They should develop a policy with associated procedures to review any potential individual when hired for a specific cybersecurity role, by consideration of the following:

Verification that the individual has the necessary cybersecurity awareness to perform the assigned role (e.g. based on performed trainings, existing certificates or respective job experience); Verification that the individual can be trusted to take on the role, especially if the role is critical for the organization". Therefore, , the coordination of security control measures between different standards should be fully considered before a power plant actually carries out cybersecurity work so as to better reduce time costs and investment costs.

3.3 Coordination Between Security and Nuclear Safety

Nuclear safety is of paramount importance to NPPs. Since IACSs of NPPs perform functions related to nuclear safety, especially those IACS important to safety, special attention should be paid to the coordination between nuclear safety and cybersecurity. The coordination should include at least two aspects. On the one hand, according to IEC 62859[12]], when the implementation of security controls may affect nuclear security functions, nuclear safety should be prioritized, and it is recommended that the above situations should be documented. On the other hand, it is suggested that the emergency response should ensure the nuclear safety when a cybersecurity incident occurs.

4 Conclusion

At present, we are carrying out the conversion of the IEC 63096 to the national standard, which is also the second one in the field of IACS cybersecurity of NPPs. With the deepening application of new technologies in NPPs such as cloud computing, big data,

Internet of Things, block chain and so on, IACSs of NPPs will face more known and unknown cybersecurity threats in the future. It's sure that international organizations, national standardization organizations and industry regulatory agencies will continue to develop relevant standards and regulatory requirements. The issues proposed in this paper that need to be considered in the process of coordinating the use of relevant standards by NPPs are also applicable to the coordination of future standards. Furthermore, if those issues are fully considered in the development process, the practicality of new standards will be further improved.

Acknowledgement

We thank all the reviewers.

Bibliography

[1] The China Nuclear Energy Association. China ranked second regarding the number of NPPs under construction and in operation, https://www.china-nea.cn/site/content/41339.html

[2] [1]KUSHNER, K., The Real Story of Stuxnet, https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

[3] Jianghai Li, Xiaojin Huang. Control System Security in Nuclear Power Plant[J]. Atomic Energy Science and Technology , 2012(46Suppl): 411-416.

[4] International Electrotechnical Commission. IEC 63096:2020 Nuclear power plants – instrumentation, control and electrical power systems – security controls[S]. Geneva: IEC, 2020.

[5] SAC/TC260, GB/T 22239-2019: Information Security Technology-Baseline for Classified Protection of Cybersecurity, Standardization Administration of The People's Republic Of China, 2019.

[6] SAC/TC260, GB/T 22240-2020: Information Security Technology-Classification Guide for Classified Protection of Cybersecurity, Standardization Administration of The People's Republic Of China, 2020.

[7] SAC/TC260, GB/T 25070-2019: Information Security Technology-Technical requirements of security design for classified protection of cybersecurity, Standardization Administration of The People's Republic Of China, 2019.

[8] SAC/TC260, GB/T 28448-2019: Information Security Technology-Evaluation requirements for classified protection of cybersecurity, Standardization Administration of The People's Republic Of China, 2019.

[9] SAC/TC260, GB/T 28449-2018: Information Security Technology-Testing and evaluation process guide for classified protection of cybersecurity, Standardization

Administration of The People's Republic Of China, 2018.

[10] SAC/TC40, GB/T 41241-2022: Management Requirements For Cybersecurity Of Industrial Control Systems In Nuclear Power Plant, Standardization Administration of The People's Republic Of China, 2022.

[11] IEC COMMITTEE 45, IEC 62645 Nuclear Power Plants – Instrumentation and Control Systems – Requirements for Security Programs for Computer-based Systems, IEC, 2014.

[12] IEC COMMITTEE 45, IEC 62859 Nuclear Power Plants – Instrumentation and Control Systems – Requirements for Coordinating Safety and Cybersecurity, IEC, 2016.