Research on Forward Design Process of Network Security Protection Design for Instrument and Control System in Nuclear Power Plant

Chu-Hao Xi[1,2], Yan-Feng Zhao[1,2], Long-Qiang Zhang[1,2], and Jing-bin Liu[3(✉)]

[1] China Nuclear Power Engineering Company LTD., Shenzhen 518045, Guangdong, China
[2] State Key Laboratory of Nuclear Power Safety Monitoring Technology and Equipment, China Nuclear Power Engineering Co., Ltd., Shenzhen 518172, Guangdong, China
[3] China Nuclear and Radiation Safety Center, Taiyuan 100082, China
Liujingbinjob@163.com

Abstract. Network security protection design for instrument and control (I&C) system in nuclear power plant is an important measure to ensure safe and stable operation of instrument and control system in nuclear power plant. Relevant national departments have put forward a number of regulatory requirements for network security design of instrument and control system, including the general principles of safety protection of power monitoring system proposed by Energy Bureau, Guidelines for grading of classified protection of cyber security by Ministry of Public Security and the technical policy requirements of network security of nuclear power plant proposed by China Nuclear and Radiation Safety Center. How to coordinate network security protection measures to meet multiple regulatory requirements is an important issue in the design of nuclear power plant network security protection. This paper introduces a forward design process of network security that coordinates and considers the above regulatory requirements, and analyzes and explains the design elements and reference standard for the design process, such as zoning and domain design, grading of classified protection, and critical digital asset classification protection.

Keywords: Network security protection design · instrument and control system · nuclear power plant

1 Introduction

The I&C system of nuclear power plant undertake the important responsibility of ensuring the safety and normal operation of nuclear power plant, and belongs to the national key information infrastructure. The network security design of the I&C system of nuclear power plant should meet the requirements of the Network Security Law of the People's Republic of China. In order to implement the Cyber Security Law, the Ministry of Public Security issued Guidelines for grading of classified protection of cyber security. Then, the Energy Bureau promulgated the "Overall Plan for Safety Protection of Power Monitoring System", which requires the implementation of the overall principles of safety

P. Gu et al. (Eds.): SICPNPP 2023, LNEE 1055, pp. 269–273, 2023.
https://doi.org/10.1007/978-981-99-3455-3_26

protection of power monitoring system, such as “safety zoning, network dedicated, horizontal isolation and vertical certification”. And, China Nuclear and Radiation Safety Center released the technical policy requirements of network security of nuclear power plant. Many regulations have brought difficulties and challenges to the network security protection design of nuclear power plants, so it is necessary to plan a reasonable forward design process, that is, to implement the requirements of different regulators step by step, and at the same time, to coordinate and unify the protection measures among different regulatory requirements.

2 The Route Map of the Forward Design Process

According to the practical experience of nuclear power plants, this paper proposes the following design process to coordinate and deal with the regulatory design requirements of various departments, as shown in Fig. 1.

Step1. Implement zoning protection in nuclear power plants according to the regulatory requirements of the Energy Bureau, and further divide network security zones into domain(sub-zone) in order to facilitate the Guidelines for grading of classified protection of cyber security (abbreviation to grading protection) in Step 2. See the third part of this paper for detailed design instructions.

Step2. According to the regulatory requirements of the Security Bureau, determine the grading of protection class for each security domain, and then determine the requirements of network security protection measures for the corresponding security domain according to standard GB/T 22239. See the fourth part of this paper for detailed design instructions.

Step3. According to the regulatory requirements of the Safety Audit Center, identify critical digital assets (CDA) according to the correlation degree with nuclear safety, security and nuclear emergency, and implement protection measure by asset type for CDA. See the fifth part of this paper for detailed design instructions.

Step4. After completing the design of asset protection measures, it is necessary to analyze whether the requirements of grading protection are met from the perspective requirement of security domain in step 2. In terms of the situation that the technical control means can not meet, it is necessary to properly adjust the division of security domain or the design of system network. In terms of the situation that the security domain or system network design cannot be modified, it is necessary to carry out Arguments and replace technical control means equivalently through necessary management means.

Through the above four steps, the network security protection design can form a forward design process which considering multi-party regulatory requirements, and form a design closed loop, so that the design scheme can be iteratively optimized continuously.

3 The Network Security Zone and Domain

Based on the requirements of the Energy Bureau, nuclear power plants can be easily divided into control zones (zone I), non-control zones (zone II), production management zones (zone III), office intranet zones (zone IV) and office extranet zones (zone V). However, if the safety zone of nuclear power plant is directly taken as the object for

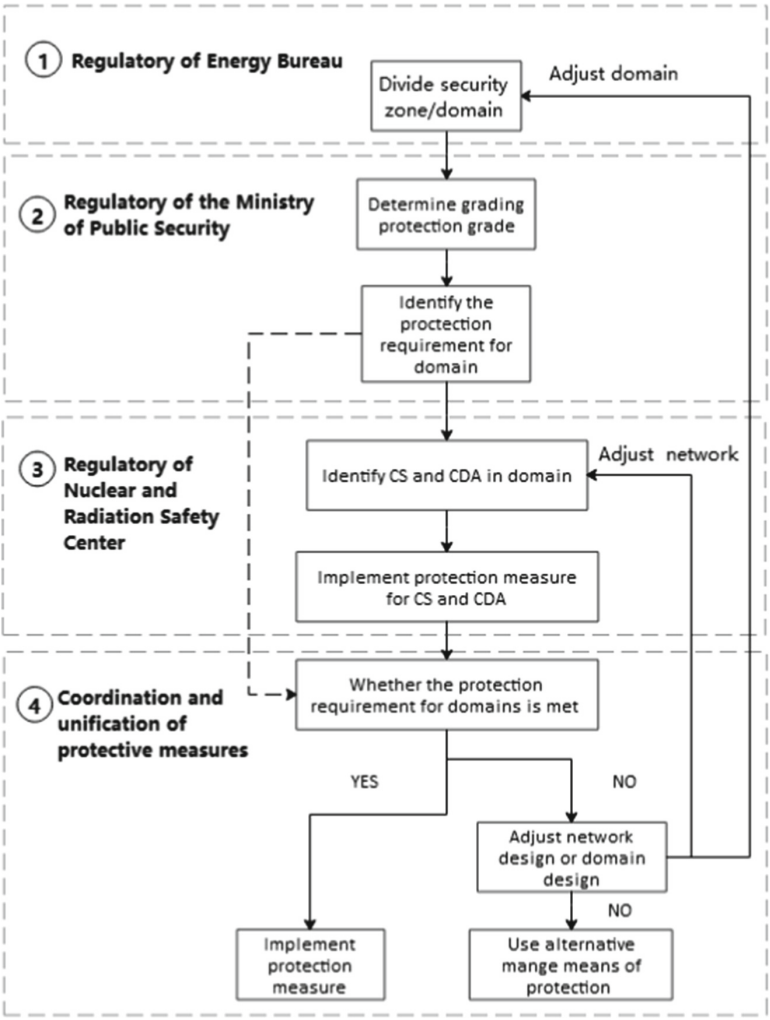

Fig. 1. Forward design process

grading protection, the protection requirements of some systems will be too high due to the large control particles, resulting in waste of protection resources. Therefore, in order to reasonably implement the requirements of grading protection, it is necessary to further split the above zones to form a network security domain, and then take the network security domain as the grading object to complete the grading protection.

Network security domain is a logical zone, which merges I&C systems with similar importance (such as security class, security class, power station capability requirements, etc.) for network security management and protection.

According to IEC 62645, besides importance, the factors considered in the design of network security domain can include organizational responsibility, layout location, overall network structure and technical characteristics of the plant, etc.

1) The security domain should conform with the Defence in Depth strategy of nuclear power plant network architecture, that is, it is not appropriate to classify information or instrument control systems of different and Defence in Depth into one safety domain;
2) The boundary of network security domain should not cross the boundary of security zones;
3) Systems with similar functions and performance requirements should be merged into the same network security domain;
4) Different safety divisions of the same system should be divided into the same network security domain;
5) Multiple systems that share the same network or have multiple network communication between systems should be merged into the same network security domain;
6) The system in the same security domain should have similar nuclear safety class, and physical security class.

4 Grading Protection for Security Domain

According to GB/T 22240, the grade of grading protection is mainly determined by two elements, namely, the intruded object and the damage degree of intruded object. The intruded object needs to consider two aspects of damage, including business information security and system service security. The grade of grading protection of intruded objects is determined by the higher grade of business information security protection and system service security protection. For specific protective measures, please refer to GB/T 22239.

5 Identification and Protection for CDA

According to the regulatory requirements of China Nuclear and Radiation Safety Center, critical systems in the security domain and critical assets in the system should be identified, and system/assets performing the following functions should be identified as critical systems (CS) or critical digital assets (CDA):

1) Systems or assets that implement or support functions for nuclear safety, physical security and emergency response;
2) Systems or assets that affect nuclear safety, physical protection and emergency response functions or that affect the performance of related functions by CS or CDA;
3) A system that provides a path for the above-mentioned CS or CDA to be attacked by cyber attacks, and the path provided by the system may lead to damage and degradation of nuclear safety, physical protection and emergency response;
4) Systems or assets supporting the above-mentioned CS or CDA;

5) Systems or assets that protect such CS or CDA from cyber attacks.

It should be noted that for support systems or equipment that are not directly related to nuclear safety, physical protection and emergency response functions, the operating unit should conduct correlation analysis, and if the analysis shows that it will cause adverse effects, it should also be CS or CDA.

CS or CDA also implement protection by asset type, and the requirement for each asset type please refer to NEI 13–10.

6 Conclusion

This paper introduces a forward design process of network security with closed design loop that coordinates and considers the multiple regulatory requirements, and analyzes and explains the design elements and reference standard for the design process. It is help for the design practise for network security design of nuclear power plant,and it is already used in the design of commercial nuclear power plant which is iteratively optimized continuously.

References

1. Cyber Security Law of the People's Republic of China (Order No.53 of the President of the People's Republic of China)
2. Regulations on the Protection of Key Information Infrastructure (Order No.745 of the State Council)
3. "Nuclear Power Plant Network Security Technology Policy" (China Nuclear [2020] No. 298)
4. Regulations on Safety Protection of Power Monitoring System (China Energy Order No.14 [2014] of the National Development and Reform Commission)
5. "Overall Plan for Safety Protection of Power Monitoring System" (China Energy Security [2015] No. 36)
6. GB/T 32919–2016 Information Security Technology Industrial Control System Security Control Application Guide
7. RG 5.71–2010 Cyber Security Programs for Nuclear Facilities
8. NEI 13–10–2017 Cyber Security Control Assesses
9. IEC 62645–2014 Requirements for security programmes for computer-based systems
10. GB/T 22239–2019 Information security technology-Baseline for classified protection of cybersecurity
11. GB/T 22240–2020 Information security technology- Classification guide for classified protection of information system