Information Systems and Economics (2023)
Clausius Scientific Press, Canada

DOI: 10.23977/infse.2023.040307
ISSN 2523-6407 Vol. 4 Num. 3

Exploration on the Construction of Security Protection System for Nuclear Power Critical Information Infrastructure

Anman Luo[1,*], Youqin Hu[1], Xianhe Shang[2], Yalin Xiao[2], Nan Wu[1]

[1]China Nuclear Power Operation Management Co. LTD, Network Security Division, Information Management Office, Jiaxing, China
[2]China Nuclear Power Operation Management Co. LTD, Jiaxing, China
[*]Corresponding author

Keywords: Nuclear power enterprises; Critical information infrastructure; Safety protection; System construction

Abstract: With the promulgation of the "Network Security Law", "Personal Information Protection Law", "Data Security Law" and other laws and regulations, the state implements the "Regulations on the security protection of critical information Infrastructure" supporting the security protection of critical information foundation, which will be officially implemented on September 1, 2021, marking the maturity of laws and regulations in the field of the security protection of critical information infrastructure. Nuclear power enterprises should carry out substantive work in accordance with the safety technology and safety management requirements mentioned in laws and standards, and do a good job in the network security protection of the critical information infrastructure of nuclear power enterprises. Based on the work experience in the security protection management of critical information infrastructure, this paper considers and studies the construction of the security protection system of critical information infrastructure in nuclear power enterprises, summarizes and puts forward relevant suggestions for the development of the security protection management procedures of critical information infrastructure.

1. Introduction

The Cyber Security Law of the People's Republic of China, which came into effect on June 1, 2017, makes it clear that the protection of critical information infrastructure is to implement key protection on the basis of the network security level protection system. On September 1, 2021, the "Regulations on the Security Protection of Critical Information Infrastructure" was officially implemented. The "Regulations" have made more specific provisions on a series of elements related to the security protection of critical information infrastructure. At the same time, the legal liabilities that the operators of critical information infrastructure should bear if they do not seriously perform the responsibilities of network security protection are also clearer. It is imminent for the operators of critical information infrastructure to formulate their own critical information infrastructure

security protection management system in accordance with the "base-based" related security protection management measures and regulations promulgated by the superior unit. The routine inspection or random inspection of the security protection work of the critical information infrastructure by the superior supervision department is gradually orderly[1].

As one of the basic preparation materials for the inspection, the document of the security protection management system of the critical information infrastructure of the unit needs to be effective and released. From the perspective of practical work of network security management engineers of critical information infrastructure operators, this paper continuously explores work experience in security protection management of critical information infrastructure, combines with the current situation of operation and maintenance of critical information infrastructure of the unit, and formulates appropriate management rules without changing the existing working mechanism. Promote the orderly implementation of the security protection of the key information infrastructure of the unit.

2. What Needs to be Defined in the Management System

2.1 Clarify the Principles for the Security Protection of Critical Information Infrastructure

The security protection of critical information infrastructure should always be guided by the thought of socialism with Chinese Characteristics for a new era[2], based on the implementation of the network security hierarchical protection system and the security protection system of critical information infrastructure, and focus on the protection of critical information infrastructure security and data security[3]. The security protection measures of critical information infrastructure must be planned, constructed and used simultaneously with the construction of critical information infrastructure. To implement network security level protection system, the implementation of network security protection "actual combat and systematism and normalization" and "dynamic defense, active defense, defense in depth, accurate protection, integrated control and prevention, defense from spreading," "three six" measures[4], follow the "who supervises, who is responsible for, who operate, who is responsible, tube business must tube safety" requirements, The security protection of critical information infrastructure shall be included in the daily production safety management system, the implementation of the security protection of critical information infrastructure shall be included in the company's production safety responsibility system assessment and departmental production performance assessment, and the implementation of the security protection measures of critical information infrastructure service providers shall be included in the company's supplier assessment method.

2.2 Clarify Key Information Infrastructure Security Protection Organizations and Positions

Network security Law and "Regulations" clearly stipulate that operators of critical information infrastructure should set up a special security management organization responsible for the security protection of critical information infrastructure.[5] Considering that the operation and maintenance responsibility of the critical information infrastructure of nuclear power plant may be divided into the maintenance department, the equipment management of the critical information infrastructure may be placed in the technical department, and the position of network security may be placed in the information department or security management department, combined with the company's business situation, It seems unlikely that a single security authority would be fully responsible for protecting critical information infrastructure. Therefore, in the process of the actual work, through the network security work office will be the key information infrastructure security protection of each professional person in charge and key position personnel centralized, and then relying on an

entity department for centralized management and operation, in the company's network security leading group and chief network security officer under the leadership of the specific work.

The company sets up a network security leading group, led by the main person in charge of the leading group of the company, including the chief network security officer and other leading members of the company; The company's network security leading group has a network security work office, which relies on physical departments (e.g. The Information Department is operated by the Chief Network security Officer as the director of the network security work office, and the members are composed of the key information infrastructure security management responsible person, the head of other departments involved in the security protection of the key information infrastructure and the network security supervision personnel; The Network Security Work Office sets up a working group for the security protection of the base. The members of the group are composed of personnel involved in the operation and maintenance posts, network security posts and equipment management posts of the security protection work of the base, and each group is assigned a leader. Thus, a complete and secure three-layer stepped security management organization [6] is constructed to ensure the normal implementation of network security protection management measures for critical information infrastructure. As shown in Fig 1.

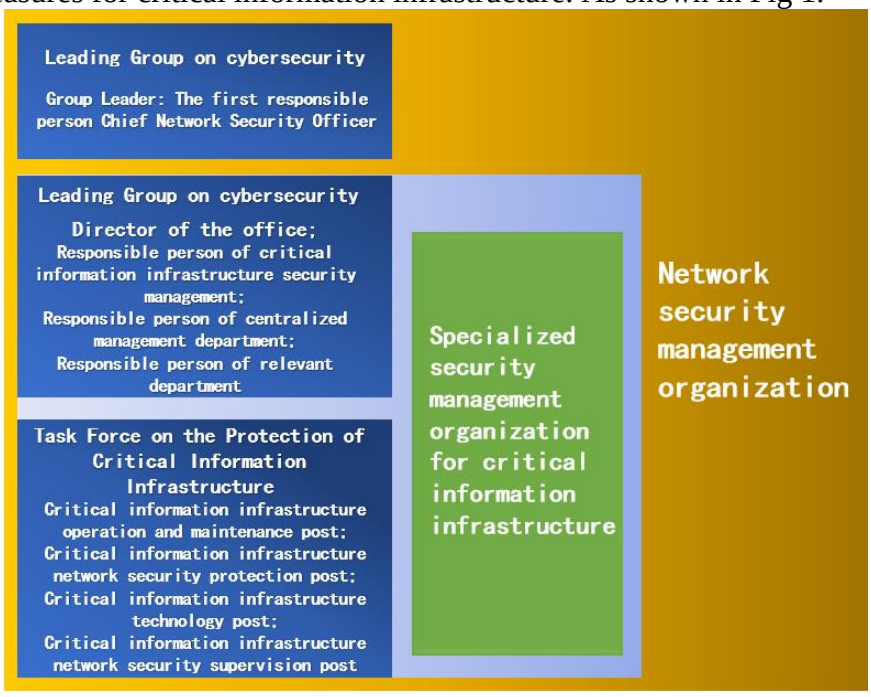

Figure 1: Refer to the specialized security management body for critical information infrastructure

2.3 Define the Responsibilities of Critical Information Infrastructure Operations Management

Combined with the network security management organizations and positions that have been set up, further define the responsibilities of the corresponding responsible persons and personnel in key positions. The network security leading group leads the security protection of the company's critical information infrastructure and the disposal of major network security incidents. Responsible for the security protection of the company's key information infrastructure; the chief cybersecurity officer is a member of the leadership team who is responsible for securing critical information infrastructure. The office operates on the basis of the entity department. As the specialized management organization of critical information infrastructure, the office implements specific

measures for the security protection of critical information infrastructure, and also participates in the company's network security and informatization decision-making. The person responsible for security management shall be directly responsible for the construction, alteration, operation and maintenance of key information infrastructure; the head of the organization and personnel in key positions shall undergo background checks and attend cybersecurity education and training, among which the personnel in key positions shall have additional assessment requirements in cybersecurity skills and technical training. Training shall be organized and implemented by the training department and training logs shall be recorded. Background review shall be carried out by the human resources department. Improve the system and norms for the security protection of critical information infrastructure, carry out the network security monitoring of critical information infrastructure on a regular basis, and carry out the detection and evaluation at least once a year; Formulate emergency plans for network security incidents of critical information infrastructure and carry out emergency drills as required; Establish a network security incident monitoring and reporting system, so as to timely report and deal with network security incidents; The human, financial and material inputs needed for the security protection of critical information infrastructure shall be guaranteed by the company's business planning department and financial department; Work involving state secrets, trade secrets, security, public opinion control and other aspects requires the participation of corresponding functional departments.

2.4 Clarify the Work that Needs to be Carried Out to Secure the Operation of Critical Information Infrastructure

According to the newly released "Basic Requirements for the Security Protection of critical information Infrastructure of Information Security Technology" standard content, the security protection of critical information infrastructure should focus on key activities such as analysis and identification, security protection, detection and evaluation, monitoring and early warning, active defense and incident handling. And network security risk management runs through the whole process of key information infrastructure security protection, forming a complete network security supervision work closed loop. After completing the preparatory work such as the establishment of the special management organization of the base and the staff allocation of the critical information infrastructure, the first work to be carried out is the analysis and identification. The critical information infrastructure operators complete the business identification, asset identification, risk identification and major change identification around the critical information infrastructure of the unit, laying the foundation for the follow-up of other activities. According to the key business list, asset list and security risk list, security management and technical protection measures shall be implemented in the aspects of security management system, security management organization, security management personnel, security communication network, security computing environment, security construction management, security operation and maintenance management, and security protection work shall be carried out to ensure the safe operation of critical information infrastructure.

Detection and evaluation, monitoring and early warning, active defense and incident disposal are closely related to the operation and maintenance of the base and problem rectification. On the one hand, it is necessary to establish a detection and evaluation system and determine the process and content of detection and evaluation, so as to facilitate personnel in key positions to carry out safety detection and risk assessment with reference to the system and process, and check the effectiveness of safety protection measures. Discover network security risks in a timely manner, analyze security events that may be caused by potential security risks, continuously rectify and track potential security risks, and dynamically remove discovered risks; On the other hand, it is necessary to

establish a network security monitoring, early warning and information notification system, timely warning and prompt for the occurrence of network security incidents or discovered network security threats in accordance with the system, gradually improve the ability to proactively detect attacks, adopt measures such as convergence of exposed surface, capture, traceability, interference and blocking, and combine offensive and defensive exercises and threat intelligence collection. Improve the ability to analyze and actively defend against cyber threats and attacks. The operation safety of critical information infrastructure emphasizes the safety of daily operation and important guarantee period. Specific work is divided into responsibilities according to key positions such as base security supervision engineer, base operation and maintenance engineer, base network security and protection engineer and base technical engineer, so as to clarify the elements of each work and implement specific base security protection work to the post. Establish internal and external communication channels, mobilize the coordination of various departments within the company, do a good job of internal security protection and system construction, also actively accept external supervision and inspection, complete the information submission requirements of superior regulatory authorities.

2.5 Clarify the Assessment of Responsibility for the Security Protection of Critical Information Infrastructure

The requirements for the network security responsibility system and accountability system are clearly stated in relevant laws and regulations and documents. The "Regulations on the Security Protection of Critical Information Infrastructure" not only clearly lists the responsibilities and obligations of the operators of critical information infrastructure, but also specifies the legal responsibilities that the operators should bear when they violate the relevant regulations. Operators should extract the daily work items according to the "regulations", and at the same time, the responsibilities should be decomposed and implemented to each key information infrastructure employee. The special security management institutions of the base need to establish and improve the evaluation system, organize the assessment of network security work, and put forward suggestions on rewards and punishments. In work practice, assessment related to network security responsibilities is an important part of production safety and management performance assessment.[7] In order to achieve systematic support in network security assessment, a network security supervision system can be established according to the operation characteristics of the company and with the help of the existing safety production responsibility management tools, covering the assessment of all violations related to network security. Network security is included in the company's safety, quality and environmental protection assessment and accountability system, and the list of common network security violations and deviations is added to the safety, quality and environmental protection assessment documents. Network security violations are also applicable to the safety and quality assessment tools.[8] Production-oriented enterprises usually set up a safety production committee, which shows the safety production indicators of the whole company in the month in the monthly regular meeting. Through this way, the company's leadership can understand the risks of network security and make appropriate decisions. At the same time, the role of network security assessment tools can be enhanced.

On the other hand, the network security assessment will be included in the company's business performance assessment system, combined with the monthly and daily frequency indicator display, forming the network security assessment and evaluation link. A complete network security supervision system is formed by combining the modules of procedure and specification, supervision and disposal.[9] Through the continuous operation of the system, a closed loop of network security supervision is formed, and a network security responsibility system and accountability system are

established.[10]

3. Conclusion

The security of critical information infrastructure is the top priority of network security protection. The critical information infrastructure of nuclear power has the characteristics of special network architecture and various types of industrial control protocols, which leads to certain particularity of its security protection. Once the critical information infrastructure of nuclear power is attacked, it will not only affect the normal operation of DCS system, but also threaten the safety of reactor operation.

This paper expounds the contents to be covered in the security protection system of nuclear power critical information infrastructure from five aspects, improves the overall security protection capacity of nuclear power critical information infrastructure through the construction of management system, responds to complex and changing new challenges, and provides specific practices for the security protection work of nuclear power critical information infrastructure. It is of great significance to improve the security protection level of nuclear power critical information infrastructure.

References

[1] Krundyshev V. M., Kalinin M. O. Mathematical Model of the Spread of Computer Attacks on Critical Information Infrastructure. Automatic Control and Computer Sciences, 2023, 56(8).

[2] Yu H C. Exploration and Thinking of Network security operation in petrochemical industry. Petrochemical Technology, 2020, 27(3):218, 215. (in Chinese)

[3] Wei Chengfei, Jiang Jie. Global cross-border dimensional logical data security governance and China's response to Books and intelligence: 1-8 [2023-02-22]. http://kns.cnki.net/kcms/detail/62.1026.G2.20230221.1533.001.html

[4] Zhao Zhiyuan. Endogenous Security Framework to realize the "Three chemical and six prevention" of equal protection and customs protection. Network security and Informatization, 2020 (10):11-12.

[5] Xinhua News Agency. Promulgation of Regulations on Security Protection of Critical Information Infrastructure. Internet World, 2021, (8):2.

[6] Bolcato Matteo, Beverina Ivo. Organisational strategies for the safe management of intravenous iron therapy: a revolutionary tool for implementing Patient Blood Management. Blood transfusion=Trasfusione del sangue, 2022, 20(2).

[7] Zhang Yawen. Research on Optimization of Performance Appraisal System of Internet Emergency Center in Gansu Province. Lanzhou University, 2021.

[8] Zou Jing, Wang Ying, Liu Yi. Comprehensive improvement of safety and quality management level of distribution network construction by taking the Four Modernizations into consideration. Agricultural Electricity Management, 2022 (01):40-41.

[9] Zhu D F. Network security protection System of critical information infrastructure. Information and Computer (Theoretical Edition), 2018 (13):198-199+202. (in Chinese)

[10] Zhang Bin, Chen Yi, Wang Xinxia, et al. Research on Network security protection system of key information infrastructure in industrial field. China Informatization, 2022, (3):60-61.