New infrastructure-oriented power network security supervision innovative mechanism and system architecture

Chao Liu¹, Jiaxuan Yang²*, Ren Qiang², Linlin Yuan², Wei Ju³, Yongxin Xia³ and Nawaraj Kumar Mahato²

¹State Grid Corporation of China, Xicheng District, Beijing, 100031, China
²Beijing Engineering Research Center of Energy Electric Power Information Security, North China Electric Power University, Changping District, Beijing, 102206, China
³State Grid Information and Communication Industry Group Co., Ltd., Changping District, Beijing, 102209, China

*Corresponding author’s e-mail: 120192201653@ncepu.edu.cn

Abstract. Under the framework of latest digital infrastructure, the application of emerging technologies in the power system has become more in-depth, and the security of power networks has ushered the new challenges. Facing new challenges, power network security inspectors need to keep pace with the times and make innovations in response to the new circumstances. This paper summarizes and analyses the existing network security supervision specifications and practical experience of the State Grid Corporation of China, and combines the laws, regulations, standards and corporate document requirements such as the Cyber Security Law and the Classified Protection 2.0 National Standard, based on the new network security characteristics of the new power digital infrastructure, research the innovative mechanism and system architecture of the network security supervision of power grid enterprises from the aspects of management and technology. Based on the new requirements of Classified Protection 2.0, this paper proposes a network security inspection evaluation system to help grid companies build new lines of network security.

1. Introduction

In June 2020, State Grid Corporation of China released ten key construction tasks of "digital new infrastructure", focusing on big data, industrial Internet, 5G, artificial intelligence, and other areas. The swift implementation and unfolding of "digital new infrastructure" not only indicates the further acceleration of the application of new technologies such as "cloud university material transfer intelligent chain" in power system but also urges power grid enterprises to actively carry out innovation in management ideas, methods and means of safety products based on existing safety management work. Presently, the State Grid Corporation of China (SGCC) focuses on ensuring the four major security of large power grid, personal safety, equipment security, and network security. In particular, network security faces great security challenges. There are many weak links in technology, and there are several flaws and frailty in management. It is crucial to improve and optimize the normal supervision mode of network security in combination with the requirements of network and information security index of power enterprises. The existing network security supervision is not comprehensive, the hidden risks and hazards rectification is not thorough, and the problem notification is not appropriate.

The purpose of network security supervision is to supervise and inspect, supervise the implementation,
supervise the rectification of hidden dangers, continuously improve the ability of network security protection, and realize the controllable, controllable, and under control of network security from two aspects of technology and management. The scope of supervision covers information system planning, design, construction, online, operation, abandonment, and other aspects of the information system life cycle. In the more than ten years of waiting for Classified Protection 1.0 before 2019, the State Grid Corporation's network security management supervision [4] includes five aspects: security management system, security management agency, personnel security management, system construction management, and system operation and maintenance management; the technical supervision includes five aspects: physical, network, host, application, data, which well guarantees the network security of power grid enterprises.

With the formal implementation of Classified Protection 2.0 on December 1, 2019, and the grand start of the new digital infrastructure of electric power in June 2020, it is of great significance [5] for power grid enterprises to better comply with the new development of power grid digitization and new requirements of network security, actively promote the innovation of network security supervision mechanism, and build a more comprehensive and perfect network security supervision system. Therefore, based on inspecting and analyzing the existing network security supervision specifications and practical experience of State Grid Corporation of China, combined with the requirements of laws and regulations, standards and enterprise documents, such as the network security law and the national standard of Classified Protection 2.0, and based on the new characteristics of network security in the new digital infrastructure of electric power, this paper studies the innovation mechanism and system architecture of network security supervision of power grid enterprises from the aspects of management and technology to assist power grid enterprises build a new defense line of network security.

2. Analysis of the current situation of power network security supervision

2.1. Network security in the context of "new infrastructure"
Under the global epidemic evolution and economic challenges, the "new infrastructure" scheme has become the focus of the industry. Even if there is no epidemic, high-quality development and digital transformation are also the directional issues in front of countries and enterprises. Now, China's "new infrastructure" has accelerated its pace. As the new infrastructure promotes the construction of digital infrastructure, the derived cyber-attacks, and cyber threats [6] are also growing in frequency and scope of influence. While supporting the upgrading and transformation of network security enterprises to meet the needs of digital infrastructure [7], the relevant departments of the state also support enterprises with a high degree of digitization and strong security protection ability in various industries to export their security capability and promote the application of their Cyberspace Security Infrastructure Capability and methods in different application scenarios in a wider range.

2.2. Review of relevant regulations on power network security
Network security may have a serious impact on national security, social security, and people's safety. Therefore, network security will be the most important cornerstone of the "new infrastructure", and the requirements for network security construction will gradually increase. Based on this, the Ministry of State Administration of safety and security analyzes and analyzes the requirements of network security from six aspects: national laws, administrative regulations, ministries and regulations, company regulations, industry standards, and general secretary Xi Jinping's important exposition.

Among them, national laws are the fundamental requirements, administrative regulations and ministerial rules are the basic requirements, company regulations and industry standards are also indispensable as power enterprises and industry requirements. Meanwhile, in recent years, General Secretary Xi's important discussion on network security as an important policy of network security construction cannot be ignored.
2.3. Practice of on-the-spot inspection

(1) Standardize special supervision and inspection mechanism

Power grid enterprises should formulate the key contents of network security supervision and inspection, and carry out special supervision and inspection. They need to formulate the work plan and scheme of network security supervision and inspection, determine the personnel of the inspection team and clarify the key contents of the inspection, division of labor, and time arrangement of the inspection group. After the supervision and inspection, the inspection unit shall prepare the supervision and inspection work report and the summary table of problems found in the network security supervision and inspection, issue the problem rectification notice, specify the rectification requirements and work suggestions, and keep them for future reference. The inspected unit shall, within 5 working days after receiving the rectification notice and supervision and inspection report, complete the rectification plan, specify the responsible department, rectification measures, and completion time, and report to the inspection unit after approval by the leader in charge; after the rectification is completed, the rectification feedback form shall be submitted to the inspection unit.

(2) Clarify information system classification and focus of supervision

According to the descriptions of Type 1, Type 2, and Type 3 information systems in the "State Grid Corporation Security Incident Investigation Regulations" and the national level protection regulations, the information systems responsible for operation and maintenance are sorted out and classified from the aspects of business association, data interaction, and level protection. For different types of systems, further, clarify the main points of supervision and key supervision content.

(3) Fully configure various professional network security supervision posts

The safety supervision department, marketing department, transportation inspection department, and control center of the power supply company shall set up network security supervision posts and allocate relevant personnel. The training of network security rules, regulations, and standards shall be incorporated into the annual training plan of all levels of the company, to improve the professional level of network security supervisors at all levels. According to the supervision standards, the personnel in charge shall be specified one by one, and self-examination and supervision and inspection shall be carried out in-depth.

(4) Innovatively carry out information communication and power monitoring safety evaluation

Actively carry out information communication and power monitoring safety evaluation, and organize and complete expert inspection and evaluation work for all units. Innovative evaluation methods, entrusting a third-party organization to conduct comprehensive network security vulnerability scanning and security diagnosis analysis on all units of the company.

3. New infrastructure and network security supervision mechanism

The vigorous development of new digital infrastructure has pushed the construction of information infrastructure to a peak, laid a good foundation for the arrival of a new round of industrial digital revolution, and has become a powerful engine driving the industry production mode and national economic trend[8]. For the steady construction of digital infrastructure, the application of the network is bound to be indispensable. The new generation of network information infrastructures such as industrial Internet, artificial intelligence, and big data center is the focus of digital transformation in the new infrastructure. People should not only ensure the security of the new algebraic infrastructure but also pay attention to the network security. Therefore, network security and digital new infrastructure are accompanied and closely linked, which is an important cornerstone to ensure the steady development of new infrastructure. Given this, the supervision and inspection of network security is an important link in the process of promoting the new infrastructure, and it is an effective way to inspect the network security under the new infrastructure from the business management level.

3.1. The security supervision system architecture of power network under the new infrastructure

At present, for the control of network security, China has issued a series of laws on network security,
such as the national security law of the people's Republic of China implemented in 2015, the network security law of the people's Republic of China implemented in 2017, the network security Classified Protection 2.0 series standards and the key information infrastructure security protection regulations implemented in 2019 Legal system. This has played an effective role in promoting the improvement of China's network security management system and the creation of a network security management innovation mechanism under the new infrastructure.

![Power network PDCA whole life cycle supervision system architecture](image)

Therefore, on the basis of following the national laws and regulations, starting from the cyberspace security control, compliance management, risk management and business control management modes, and based on the scenario of energy network energy flow, information flow and business flow depth integration and interaction contained in the digital new infrastructure, OICT (operational technology operation technology, information) is adopted CPS (cyber-physical) based on technology information technology and communication technology The technology development model of systems information physical system, using network business function security as the core and network information security as the guarantee, establishes the supervision system architecture of power network PDCA (Plan, Do, Check, Action) life cycle management and control, so as to achieve a safe and healthy power network environment in the process of digital plus new infrastructure construction To ensure the continuous and reliable operation of the power system. The whole life cycle supervision architecture of power network PDCA is shown in Figure 1.

### 3.2. Innovation mechanism of power network supervision based on Classified Protection 2.0 under new infrastructure construction

Under the new digital infrastructure, the new mechanism of power network security supervision and inspection based on the Classified Protection 2.0 series standards mainly includes personnel interview, document review, configuration inspection, field observation and tool test, etc., as follows.

1. **Personnel interview**
   
   The members of the inspection team went to the site to communicate with the relevant personnel of the company to be inspected. Through the exchange, they understood the safety awareness of the personnel, the degree of knowledge about safety management and the mastery of safety technology, and collected a large number of useful information to understand the importance of services provided by the company to be inspected and the importance of the data carried.

2. **Document review**
   
   Members of the inspection team arrive at the scene, with the cooperation of relevant personnel of the company to be inspected, verify the compliance of existing documents of users with the requirements of evaluation standards by checking documents and information security-related management systems. It mainly refers to whether the system, strategy, operation procedures, and other documents prepared by
the organization are complete, whether there are complete records of system implementation, and review and analyze the above documents to check their integrity and internal consistency.

3. Configuration check

Members of the inspection team go to the site, with the cooperation of relevant personnel of the company to be tested, check the deployment and implementation status of the system security policies, and check whether the security policies set in the company are effective. It mainly uses the method of computer verification to check whether the configuration of application software, host system, database system, and network equipment is correct.

4. Field observation

The members of the inspection team go to the system operation site to judge the safety awareness, business operation, management procedures, and system physical environment through field observation of personnel behavior, technical facilities, and physical environment.

5. Tool testing

(1) Vulnerability scanning

Members of the inspection team use professional vulnerability scanning tools to scan the vulnerabilities of the equipment and systems (including the host, operating system, application system, network equipment, security equipment, etc.) involved in the company. The scanning mode is remote network scanning or local network scanning. The vulnerability scanning process is shown in Figure 2.

![Vulnerability scanning flow chart](image)

Network and security equipment vulnerability scanning can be divided into two scanning modes: system vulnerability scanning and database vulnerability scanning. The system vulnerability scanning includes web scanning, buffer overflow scanning, malformed packet sending, and worm scanning, while database vulnerability scanning includes password guessing, local buffer overflow scanning, and denial of service attack scanning.

(2) Penetration test

According to the supervision plan, the members of the inspection team select the target and conduct a full range of remote penetration tests in the simulated environment for the information system within the scope of this project of the company from different angles. The purpose is to detect the real protection ability of the target network/system/host/application through in-depth detection and enhance the protection and detection ability of system intrusion and attack. The ability to deal with the problem in
life, pay attention to the severity of security vulnerabilities, and find the most vulnerable links in the system.

4. Innovative mechanism for power network security supervision at the technical level under the new infrastructure

The deployment and promotion of new infrastructures such as 5G, industrial Internet, artificial intelligence, and data centers have greatly improved the implementation of security guarantees for the power network in technical applications. From a technical perspective, the strong networked attributes of the new infrastructure are irrelevant. Avoid the hidden safety hazards laid by the ground for the construction of new infrastructure. This requires the integration of network security technical guarantees and new infrastructure construction and deployment.

Regarding the technical level, the protection of network security mainly uses network information security inspection tools for supervision and inspection. The network information system security toolbox is composed of three modules: a toolbox management system, a technical inspection tool library, and auxiliary inspection equipment. The toolbox management system is installed on the special tools for grade protection inspection and integrates the inspection index library, the inspection knowledge base, the human-computer interaction interface, the tool management module, the system management module, and its dedicated interface. The toolbox management system and related auxiliary equipment including portable printers, digital cameras, voice recorders, portable scanners, and law enforcement recorders form integrated toolbox management and inspection module. The technical inspection tool library contains a series of system software inspection tools such as Windows/Linux host configuration inspection tools, network and security equipment configuration inspection tools, virus inspection tools, and Trojan horse inspection tools, and then the collected inspection data will be put into the toolbox management system thus performs software data checking. The overall structure of the network information system security inspection toolbox is shown in Figure 3:

![Network Information System Security Inspection Toolbox](image)

**Figure 3.** The overall structure of the network information system security inspection toolbox

The tool function system is divided into three layers. The first layer is the information system level protection security inspection data collection function layer, using the U port inspection tool library and network port inspection tool library. This layer mainly implements Windows host configuration check, website malicious code check, host-virus check, host Trojan horse check, Linux host configuration check, network, and security device configuration check, weak password check, database security check,
system vulnerability check, and website security check, and further, realize the function of collecting data. The second layer is the information security level protection security inspection data analysis layer, which is mainly based on the security inspection index database, the information system inspection knowledge base, the special inspection support database, the inspection knowledge base of the industry authority, and the information system filing unit inspection knowledge base. Realize the research and analysis of the collected data on the Internet. The third layer is the data analysis layer of information security level protection security inspection, which mainly realizes the research and analysis of the collected data based on the security inspection indicator base, information system inspection knowledge base, special inspection support base, industrial competent department inspection knowledge base and information system filing unit inspection knowledge base. The framework of the tool function system model is shown in Figure 4.

![Figure 4. Tool function system model](image)

5. Network Security Supervision Evaluation System Based on Classified Protection 2.0

With the continuous emergence of new forms of energy development such as the energy Internet and integrated energy systems, as well as the background of "digital new infrastructure", there has been an upsurge in the application of new technologies such as the Internet of Things, blockchain, and artificial intelligence in the field of energy and power. It can be seen that in response to the new network security requirements of "clear levels, enhanced protection, and normal supervision" in Classified Protection 2.0, power network security inspections must strictly follow the 16-character "network dedicated, security partition, horizontal isolation, and vertical certification". The basic security policy keeps pace with the times, strengthens requirements, and actively develops, conforms to the 16-character enhanced security policy of "manageable and controllable, precise protection, visible and credible, and intelligent defense", and carries out network security supervision and management of the whole business system.

For network security inspections, a reasonable network security evaluation system only facilitates the assessment of power network security, but also provides intuitive comparisons for network security inspections[11]. Therefore, this paper builds a network security inspection evaluation system based on Classified Protection 2.0.
5.1. Evaluation index selection

Based on the understanding of Classified Protection 2.0 and cybersecurity inspection work, combined with the actual situation, the following evaluation indicators are selected from the technical and management levels, as shown in Figure 5.

![Network Security Evaluation Index System](image)

**Figure 5. Network Security Inspection Evaluation Index System**

5.2. Evaluation index calculation

For the calculation of evaluation indexes, the commonly used Analytic Hierarchy Process (AHP) has the problem that consistency is difficult to guarantee when there are many evaluation indexes. Aiming at the deficiencies of the AHP, the Fuzzy Analytic Hierarchy Process is selected here, which to a certain extent solves the problem of lack of scientific basis for the consistency judgment standard, and it can effectively improve the deficiencies of the AHP.

The specific steps of the fuzzy analytic hierarchy process are as follows:

(1) Determine the judgment matrix.

Suppose the judgment matrix is R. The element $R_{ij}$ $(1 \leq i, j \leq n)$ in R represents the degree of membership of criterion (or index) $r_i$ more important than criterion (or index)$r_j$. The larger $r_{ij}$ is, the more important $r_i$ is than $r_j$. The importance scale of 0.1-0.9 is used to construct the judgment matrix.

(2) Calculate the weight of the single rank order.

Suppose there are n criteria in the criteria layer, and their weights are $W_1^t$, $W_2^t$, ..., $W_n^t$. Each criterion $a_i$ $(i=1, 2, ..., n)$ includes s indicators, which are $b_1, b_2, ..., b_s$, and their weights are $W_{1i}, W_{2i}, ..., W_{si}$. According to the above assumptions, the criterion level single ranking weight can be expressed as

$$W^t_i = \frac{1}{n} - \frac{1}{2\alpha} + \frac{1}{n\alpha} \sum_{k=1}^{n} r_{ik}, \quad r \in \{1, 2, ..., n\}$$  \hspace{1cm} (1)

In the equation (1): $\alpha$ is the index factor of the difference in importance between the criterion $a_i$ and criterion $a_j$ ($W^t_i - W^t_j$), The smaller the $\alpha$, the more important the experts pay attention to the difference in importance between the criteria and $\alpha \geq (n-1)/2$. To highlight the differences between the criteria, $\alpha = (n-1)/2$ is generally used in practical applications. The index level single order can be expressed as

$$W^t_{ij} = \frac{1}{s} - \frac{1}{2\beta} + \frac{1}{s\beta} \sum_{k=1}^{n} r_{ik}, \quad j \in \{1, 2, ..., s\}$$  \hspace{1cm} (2)

In the equation (2): $\beta$ is the index factor of the difference in importance between the criterion $b_i$ and criterion $b_j$ ($W^t_i - W^t_j$), The smaller the $\beta$, the more important the experts pay attention to the difference in importance between the criteria and $\beta \geq (s-1)/2$. To highlight the differences between the criteria, $\beta = (s-1)/2$ is generally used in practical applications. The total ranking weight vector of all indicators is

$$W = (W^t_1, W^t_2, ..., W^t_n)$$  \hspace{1cm} (3)

(3) Calculate the total ranking weight of the hierarchy.
The total order of the levels varies with the order of the level list. Also, suppose there are a total of \( m \) indicators in the hierarchical structure, namely \( b_1, b_2, \ldots, b_m \), and their weights for the criterion \( a_j \) the level single ranking is \( W_{i1}, W_{i2}, \ldots, W_{im} \) (if \( b_j \) is not the corresponding indicator under criterion \( a_i \), then \( W_{ij} = 0 \)). According to the above level single ordering formula, the level total ordering weight formula of each index of index level \( B \) is

\[
W_j^B = \sum_{i=1}^{n} W_i^A W_{ij}
\]

After the weights are obtained, the scores of each indicator item are multiplied by their respective weights, and the scores of each indicator item are set in the \((0, 100)\) interval to obtain the comprehensive value of the network security inspection evaluation.

6. Conclusion

The construction and implementation of latest developed infrastructure has received great attention from the country and various industries and is booming. Future-oriented new technologies are constantly being promoted by the new infrastructure. Networking and informatization are just under this great change. The head or leader of the company always focuses on network security to ensure the stability and health of the digital new infrastructure construction process. The power industry has long been regarded as an indispensable supply-side unit by the country and the people and has become an important part of new infrastructure. Given this, power network security is the backbone to fully guarantee the effective construction and application of new infrastructure. The supervision and inspection of power network security is an issue that runs through it.

Based on the national laws and regulations related to network security, this paper firstly developed a corresponding innovation system for power network security supervision and inspection from the management level, thus establishing the power network PDCA full life cycle management and control system architecture model, and how the power network under the new digital infrastructure achieving safe operations and how to ensure the stable operation of related industries and enterprises have a crucial impact. Then, through a full interpretation of the current stage of the Classified Protection 2.0 national standard, and absorbing the program methods of network security supervision and inspection, a set of supervision and inspection mechanisms including personnel interviews, document reviews, configuration inspections, field inspections, and tool tests were established. For the technical level of power network security supervision and inspection, software and hardware inspection tools such as inspection index libraries, inspection knowledge bases, and human-computer interaction interfaces are mainly used to perform corresponding index inspections and data analysis, finally, from a technical perspective, the effectiveness, convenience and reliability of network security supervision and inspection have been realized. The construction of new digital infrastructure will inevitably bring infinite opportunities so that progressively large number of people will share the dividends given by the new infrastructure. However, a series of threats and unstable factors generated by it will also flood all walks of life. Large industries such as power are the first to bear the effects. Therefore, how to ensure the stable and safe operation of the power industry is a key issue raised for new infrastructure, and grasping the threshold of power network security inspection is the top priority.

References

[1] Xinhuanet client, 2020. State Grid released ten major tasks of "Digital New Infrastructure". V https://baijiahao.baidu.com/s?id=1669622654511077939&wfr=spider&for=pc.
[2] Liu W.N., Dong N., Hou B.T., Jia Z.Z. (2018) Research and application of normal supervision of network and information security in the power industry. J. Hebei Electric Power Technology., 37: 37-39.
[3] Lin Y., Liu P., Wang H., Wang W.J., Zhang Y.Q. (2020) A survey of cybersecurity threat intelligence sharing and exchange research. J. Computer Research and Development., 57: 2052-2065.
[4] Sun P. (2020) New infrastructure, new outlets, new security, and new empowerment-"Internet Information Military and Civilian Integration" magazine interviews academician Wu Jiangxing on how to build the foundation of new infrastructure security. J. Internet Information Military-civilian Integration, 05: 15 -18.
[5] Sun H.F. (2020) New trends in network security from the perspective of "new infrastructure". J. China Information Security, 125: 43-45.

[6] Rong X.Y., Liu H.F., Liu G.W., et al. (2020) Research on Cloud Computing Network Security Matrix Control Based on Risk Control and Compliance. J. Information Security Research, 3: 266-271.

[7] Hu R., Wang X.M. (2019) Configuration management system backup and backup validity detection design. J. Electronic Technology and Software Engineering, 09: 201+261.

[8] Editorial Department of this journal. (2020) New opportunities for network security under the new infrastructure. J. Network security and information technology, 08: 46-47.

[9] Zhang J., Gao W.P. (2020) The application of network technology in power information communication under the new situation. J. Communication Power Technology, 197: 234-235+237.

[10] Du P., Tao H.Z., Gao B.C., Zhang Y., Guo L.X., Yan L., Wen Z.Q., Chen Q.S. (2015) Multi-application-oriented general data acquisition technology scheme. J. Automation of Electric Power Systems, 39: 26-30.

[11] Q. Li, Z. Liu, Y. Chen, G. Gong, S. Yang and N. K. Mahato. (2019) "Energy Data Security and Multi-Source Coordination Mechanism Based on Blockchain," In: 2019 IEEE Sustainable Power and Energy Conference (iSPEC), Beijing. pp. 1979-1983.