MATEC Web of Conferences **363**, 01018 (2022)
AMME 2022
https://doi.org/10.1051/matecconf/202236301018

Discussion on safety protection of on-line monitoring in self provided power plant

Lingkai Zhu [1, *], Jiyan Liu[2], Weishuai Wang[2], Wei Zheng[1],Ziwei Zhong[1], Zhiqiang Gong[1], Junshan Guo[1], Panfeng Shang[1]

[1]State Grid Shandong Electric Power Research Institute, Jinan, China
[2]State Grid Shandong Electric Power Company, Jinan, China

Abstract. This paper expounds the necessity of formulating the security protection strategy for the flexible interactive platform between the captive power plant and the power grid, analyzes the overall security protection strategy, and divides the security zone of the platform according to the overall security protection principle.

1. Introduction

Smart grid integrates power, computer, communication, network and other advanced technologies on the basis of traditional power grid, and is the main direction of current power grid development [1]. "Strong intelligent power grid" is strong because it has ultra-high voltage backbone network and multi-level power grid coordination. Intelligent power grid refers to the transformation of traditional power grid into a new modern power grid by using network communication, informatization and automatic control technology [2]. The intelligence and robustness of the smart grid are mainly guaranteed by three systems: the intelligent infrastructure system, the intelligent management system and the intelligent protection system. With the expansion of the power grid scale and the increasingly complex structure, it is increasingly difficult to ensure the safe and stable operation of the power grid. The network security problem is a major challenge [3].

Participating in the power market competition, captive power plants can promote the power supply and demand balance of the power grid from the load side, which can reduce the disadvantages of traditional regulation and generation side to ensure the power balance of the power grid due to the shortage of power coal supply, the increase of temporary repair and output reduction of thermal power units, and the increase of new energy penetration[4]. On the basis of the research on the operation characteristics, evaluation and market mechanism of the captive power plant, combined with the achievements of the demonstration project to improve the theory and technology research, the flexible interactive platform between the captive power plant and the power grid has the functions of archive management, resource adjustable potential analysis, operation status detection, energy consumption analysis, transaction management, etc. of the captive power plant, and has formed an operable and popularized evaluation system and market mechanism[5,6].

The "flexible interactive platform between self owned power plant and power grid" is connected with the State Grid System and becomes a part of the smart grid.In order to strengthen the security protection of the flexible interactive platform between the captive power plant and the power grid, ensure the security of business data in the process of generation, storage, transmission and use, resist malicious damage and attacks on the platform by hackers and malicious codes, and other illegal operations, and prevent the paralysis and out of control of the flexible interactive platform between the captive power plant and the power grid, as well as the resulting transaction interruption or failure, a system accident of the power plant and other accidents, It is necessary to adopt a number of security protection technical means to build a comprehensive security defense system in depth. Through multi-level information security protection measures, the security problems caused by the breakthrough of some protection layers are prevented, so as to effectively ensure the security of the platform. In order to achieve cost control, it is not necessary to deploy the whole system in an all-round way when building the security defense system. Instead, multi-level security protection configuration is adopted for key nodes, and security protection measures with relatively low protection intensity are adopted for common areas[7].

2. Overall protection principle of platform

"Flexible interaction platform between captive power plant and power grid" is a system connection with State Grid Corporation of China, which has certain particularity. The research on flexible interaction security protection strategy between captive power plant and power grid will be completed on the basis of complying with relevant national regulations and information management regulations of State Grid Corporation of China. The

[*] Corresponding author: zhulingkai@woyoxin.com

general principle of security protection is "security zoning, network dedicated, vertical authentication"[8] .

2.1 Security partition

Safety zoning is the structural foundation of flexible interactive safety protection system between captive power plant and power grid[9]. The internal business system of the captive power plant based on computer and network technology is divided into production control area and management information area in principle. According to the importance of the business system, the production control area can be divided into control area and non control area, and the management information area can be divided into production management area and management information area.

The business system or its functional module in the control area is an important part of power production. It is the focus and core of security protection to directly realize the real-time monitoring of the primary power system and vertically use the power dispatching data network or special channel. The main users of all systems in the control area are dispatchers and operators. The real-time data transmission is at the millisecond level or second level. Its data communication is transmitted through the real-time subnet or special channel of the power dispatching data network.

The business system or its functional module in the non control area is a necessary part of power production. It operates online but does not have control function. It uses the power dispatching data network and is closely connected with the business system or its functional module in the control area. The main users of various systems in the non control area are power dispatchers, hydropower dispatchers, relay protection personnel and power market traders. The data acquisition frequency of non control area is minute level or hour level, and its data communication uses the non real time subnet of power dispatching data network.

The production management area mainly includes the production management system. The typical systems are lightning monitoring system, meteorological information access, etc. the external communication boundary of the area is the power data communication network.

The information management area is the management information area. The area includes office management information system, customer service, etc. the external communication boundary of the area is power data communication network and Internet.

Different safety protection requirements are determined for different safety zones, and the control zone has the highest safety level. On the premise of meeting the general principles of security protection, the setting of security zones can be simplified according to the actual situation of the business system, but the formation of vertical cross connection of different security zones should be avoided.

2.2 Security partition

The power trading module undertakes the online trading business and needs to be linked with the power trading platform of the State Grid. Therefore, it can be combined with the special channel of the power dispatching data network at the power plant end to use independent network equipment for networking. The power dispatching data network is a special data network for the production control area, which carries the power real-time control, online production transaction and other businesses. The security protection isolation strength between the external boundary networks of the security zone should match the security protection isolation strength between the connected security zones. The power dispatching data network shall use independent network equipment for networking on the dedicated channel, and adopt different channels, different optical wavelengths, different fiber cores and other methods based on sdh/pdh to realize the safe isolation from other data networks of power enterprises and external public information networks at the physical level. The power dispatching data network shall adopt the following security protection measures: network route protection, network boundary protection, security configuration of network equipment, layered and partitioned setting of data network security. In addition, the data networks at all levels should be safely isolated through route restriction measures. When a public communication network is used within an area, it is prohibited to interconnect with the dispatching data network to ensure that network failures and safety events are limited within the local area.

2.3 Vertical certification

Vertical encryption authentication is the vertical defense line of the security protection system of the platform. Adopt authentication, encryption, access control and other technical measures to realize the remote secure transmission of data and the security protection of vertical boundaries. The vertical connection between the platform terminal and the platform shall be equipped with a dedicated vertical encryption authentication device or encryption authentication gateway and corresponding facilities that have been tested and certified by the designated department of the state to realize two-way identity authentication, data encryption and access control. Vertical communication in the secure access area shall adopt security measures such as one-way authentication based on asymmetric key technology, and two-way authentication can be adopted for important services.

3. Division of safety zone for interaction platform between captive power plant and power grid

The flexible interactive platform between captive power plant and power grid has functional modules such as file management, resource adjustable potential analysis, operation status monitoring, energy consumption analysis, transaction management, etc. the databases involved are: captive power plant equipment, captive power plant terminal, power grid information, flexible interactive strategy and other databases. According to the above concept of safety zone and the principle of dividing safety zone, the division of safety zone for each business system in the interactive platform between captive power plant and power grid is shown in Table 1.

Table 1. Security zone division of platform business system.

Numble	Module name	Large area	Region
1	File management	Management information region	Information management area
2	Analysis of resource adjustable potential	Management information region	Production management area
3	Operation status monitoring	Production control area	Uncontrolled area
4	Energy consumption analysis	Management information region	Production management area
5	Transaction management	Management information region	Production management area

According to the overall security protection principle and the system security zone division, the security protection methods developed by this platform mainly include border security protection, terminal security protection, network security protection and comprehensive security protection, as shown in Table 2.

Table 2. Platform safety protection method.

Numble	Safety protection classification	Safety protection measures
1	Border security protection	Lateral boundary protection Longitudinal boundary protection Third party border security protection
2	Terminal safety protection	Terminal virus protection Malicious code protection Patch management Terminal security management
3	Network security protection	Network equipment security protection Network information security protection Network channel security protection
4	Comprehensive safety protection	Intrusion detection Host and network equipment reinforcement Safety inspection and analysis Network security management Backup and disaster recovery User interface security protection Data interface security protection

The overall security protection scheme needs to divide the security zones of the involved systems in combination with the management similarity and business similarity of each application system, so as to design the security protection measures of each system more pertinently. The security zone division of the information system can decompose the complex security protection problems, help to realize the hierarchical protection of the information system, implement targeted application boundary protection, and prevent the proliferation of security problems.

4. Summary

During the operation of the smart grid software system, due to business expansion and other reasons, it is necessary to add new information systems or access a large number of intelligent terminal equipment, which makes the original system scale increase, the business dependence become stronger and stronger, and the system application environment becomes more and more complex. The security of each region has an important impact on the safe operation of the entire power grid system. The security control strategy for the power grid system is mainly considered from three aspects: control security, access security and application security. Control security effectively prevents illegal intrusion initiated by external users, access security prevents illegal user intrusion, and application security mainly improves the availability and reliability of the system.

Based on the self-developed system "flexible interactive platform between self-contained power plant and power grid", this paper expounds the overall strategy of system security protection, divides the security zone according to the specific business content of the system, and formulates specific protection rules under the guidance of the overall strategy, effectively ensuring the safe operation of the platform.

This work was supported by The Science and Technology Project of State Grid Corporation of China - Research on low-carbon regulation oriented coal-fired captive power plants' participation in power grid supply and demand regulation and source grid load coordinated operation technology.（5400-202236173A-1-1-ZN）.

References

1. Xiaofeng Zhu, Kejie Cui, Jianwei Huang. Research on integrated security protection of power monitoring systems[J]. Electrical Technology, 2021,(07):114-115+119.
2. Jie Cheng, Zhijie Shang, Wei Hu, etc. Security hidden dangers and countermeasures of smart grid information system[J]. Electrical applications, 2020,39(04):99-102.
3. Han Qian, Jie Gu. Analysis of network security protection strategy of smart grid system[J]. Application of integrated circuit, 2021,38(09):42-43.
4. Shijun Liu, Qing Cai, Yuhui Bi. Research and judgment on restrictive policies and development

direction of enterprise owned thermal power units[J]. Baosteel Technology, 2016,(5):6-12.

5. Yifan Huang, Haijing Zhang, Lei Wang, etc. Evaluation method for flexibility regulation of captive power plants based on production characteristics of enterprises [J]. Power demand side management, 2021,23(1):61-66.
6. Lingkai Zhu, Weishuai Wang, Haijing Zhang, etc. Application prospect of captive power plant in future comprehensive energy field [J]. Shandong Electric Power, 2022,49(2):12-16.
7. Yanwei Shang. Research on security protection of power grid information platform[J]. Automation technology and Application, 2018,37(7):126-129.
8. Xiasheng Gao, Shaoxiong Huang, Xiao Liang. Safety protection elements of power monitoring system [J]. Computer knowledge and technology, 2017,13(8):212-214+222.
9. Weihua Zhang. Discussion on network security protection of power monitoring system [J]. Information recording materials,2017,18(6):46-47.