Challenges and Prospects of Power Network Security Protection in the Context of a New Power System: A Case Study of Jiangxi

Yongcai Xiao[1(✉)], Jian Xu[1], Kuangye Liu[1], Jingjing Ge[2], Lei Hu[3], and Chenxi Wang[3]

[1] Jiangxi Provincial Key Laboratory of Operation Control of New Energy Power System, State Grid Jiangxi Electric Power Co., LTD. Electric Power Research Institute, Nanchang 330013, Jiangxi, China
441028731@qq.com

[2] East China Jiaotong University, Nanchang 330013, Jiangxi, China

[3] Jiangxi Normal University, Nanchang 330013, Jiangxi, China

Abstract. In recent years, the power grid in Jiangxi Province has entered a new phase of construction in the context of a new power system. However, the traditional network security protection system of the company is facing increasing security risks [1]. This paper first elucidates the network structure characteristics of the new power system and identifies the security risks it faces. Subsequently, combining the characteristics of boundary protection and static protection in the existing network security protection system, this paper analyzes the challenges faced by the protection system from aspects such as power source structure, grid configuration, business models, and technical foundations. Based on the content of security challenges, the paper proposes the requirements for network security protection in terms of trusted access, intelligent perception, and precise protection. Lastly, in conjunction with the development trends of security systems and new technologies, the paper summarizes the technological development directions in areas such as perception technology, blocking technology, security detection and evaluation technology, and validation technology.

Keywords: new power system · network security · trusted access · intelligent perception

1 Introduction

1.1 A Subsection Sample

With the advancement and development of the national strategy for "carbon peaking and carbon neutrality," the drawbacks of the traditional energy system, such as high carbon emissions, excessive energy dependence, and unstable energy supply, have become increasingly prominent. The evolution of the new power system is imminent [2]. The new power system aims to accelerate the popularization of renewable energy, particularly

Y. Cao and X. Shao (Eds.): DIONE 2023, LNICST 515, pp. 209–215, 2025.
https://doi.org/10.1007/978-3-031-80713-8_15

solar and wind energy; utilize intelligent technologies to optimize energy production, transmission, and utilization; promote the development of distributed energy, encouraging consumer participation in energy management; construct an energy internet to facilitate cross-regional scheduling and trading of energy. Through the promotion of renewable energy, intelligent technologies, and distributed energy, the new power system aims to achieve cleaner, smarter, and decentralized energy. However, in the process of developing the new power system, it also introduces new network security risks to the traditional power networks.

2 Network Security Challenges Faced by New Power Systems

2.1 Power Generation Structure

With the advancement and development of the national strategy for "carbon peaking and carbon neutrality," the drawbacks of the traditional energy system, such as high carbon emissions, excessive energy dependence, and unstable energy supply, have become increasingly prominent. The evolution of the new power system is imminent [2]. The new power system aims to accelerate the popularization of renewable energy, particularly solar and wind energy; utilize intelligent technologies to optimize energy production, transmission, and utilization; promote the development of distributed energy, encouraging consumer participation in energy management; construct an energy internet to facilitate cross-regional scheduling and trading of energy. Through the promotion of renewable energy, intelligent technologies, and distributed energy, the new power system aims to achieve cleaner, smarter, and decentralized energy. However, in the process of developing the new power system, it also introduces new network security risks to the traditional power networks.

2.2 Grid Configuration Aspects

In new power grid systems such as direct current (DC) grids, hybrid AC/DC interconnected grids, and microgrids, the grid structure becomes more intricate, and interactions occur with higher frequency. Due to the presence of multiple power sources and users, both information transmission and energy flow become more complex. Moreover, the smart integration of various energy sources within the adjustable load energy internet further enhances the coordinated control of energy production, transmission, and consumption across multiple stages. Consequently, the complexity of grid systems is further amplified.

2.3 Business Model Aspects

In the context of new power grid systems, the increasing application demands of distributed renewable energy integration, precise load control, and novel distribution grid protection require higher bandwidth, lower latency, improved reliability, enhanced security, and greater cost-effectiveness in power communication [5]. Furthermore, the growing number of participants in the power market trading leads to the transmission, storage,

and utilization of various sensitive data across multiple links, thereby exacerbating the risks of data leakage and tampering. Consequently, higher requirements are placed on the integrity, confidentiality, and availability of data assets within the new power grid systems. Additionally, emerging entities in the power market, such as virtual power plants and load aggregators, introduce new third-party actors that necessitate more open communication networks to support their business needs. The existing monitoring systems have not fully covered the diverse resources of the new power grid systems, leaving certain terminals inadequately supervised. Therefore, to ensure the secure and stable operation of the new power grid systems, it is imperative to introduce secure and reliable wireless communication methods and extend the security monitoring capabilities from the core network to the periphery and various domain-specific operations.

2.4 Technical Foundations

Emerging technologies such as artificial intelligence, big data, cloud computing, edge computing, and 5G have been extensively applied to support comprehensive analysis of power grid data, enhance the level of grid intelligence, and enable the sharing and utilization of power-related data. However, these new technologies also face inherent security issues. Among them, 5G communication technology is a vital strategic resource and a new infrastructure supporting energy transformation. However, its virtualized infrastructure and IoT platforms are susceptible to external attacks. The distributed nature of cloud computing weakens the controllability of security measures. Blockchain technology, characterized by decentralization, openness, tamper resistance, and traceability, finds widespread application in real-time power trading, source-grid-load-storage interaction, and multi-energy complementarity [6]. However, risks still exist in terms of protocol security and smart contract security. Therefore, in the context of new power grid systems, it is necessary to continue strengthening the security measures of these new technologies to ensure their stable operation. Additionally, the integration of new technologies and power grid security should be promoted to facilitate the sustainable development of the power industry.

3 New Power System Network Security Protection Requirements

3.1 A Subsection Sample

With the continuous development of new power systems, the importance of trusted access technology for power terminals has increased [7]. Firstly, it is necessary to ensure the identity authentication and secure access of power terminal devices to prevent unauthorized devices from entering the system. Secondly, data encryption and integrity verification are required during data transmission to ensure data integrity and prevent tampering or theft. In addition, remote configuration, upgrading, and monitoring functionalities need to be implemented to improve operational efficiency and reduce management costs. To meet these requirements, several technologies are currently available for trusted access to power terminals, such as digital certificate technology based on the Public Key Infrastructure (PKI), bidirectional identity authentication technology based

on Pre-Shared Key (PSK), and tunneling technology based on Virtual Private Networks (VPN). These technologies effectively ensure the secure access and data transmission of power terminal devices, making them indispensable in new power systems.

3.2 Intelligent Perception

With the escalating network security landscape, the new power system needs to transition from traditional passive defense to proactive defense strategies. To counter unknown network security risks, it is imperative to establish an intelligent perception system that actively perceives, identifies, and detects malicious activities, thereby enhancing defense and deterrence capabilities and providing comprehensive and systematic protection [8]. In the new power system, intelligent perception mechanisms for network security events need to be established at each stage, including generation, transmission, and consumption, to achieve proactive awareness of network security risks. Furthermore, it is crucial to strengthen the aggregation of the overall network security situation and enhance monitoring and early warning capabilities. This entails expanding the scope of situational awareness, integrating the network security situational awareness capabilities of various entities, and constructing a network security situational awareness technical architecture that aligns with the new power system. Regarding technical implementation, it is essential to deepen the breadth and depth of information collection through distributed deployment of terminals. Additionally, a unified security model library should be established, based on the distinctive feature fingerprints of the massive devices in the new power system. Employing multidimensional security event data fusion technology, intelligent analysis modules can be developed to facilitate the transition from experience-based to intelligent security analysis. These measures will significantly contribute to enhancing the network security protection capabilities of the new power system.

3.3 Precision Protection

In the context of the new power system, precise protection measures are essential to address the specific challenges associated with distributed renewable energy, distributed energy storage, next-generation power dispatch and control, and next-generation load management applications. These measures focus on deploying protective measures around intelligent perception and secure access to ensure the secure integration and comprehensive awareness of distributed devices, as well as the observability and controllability of edge device networks at the network security level. It is crucial to analyze the characteristics of the business applications and network security risks and implement targeted security protection measures to achieve on-demand protection. By doing so, the security immune capabilities of the new power system can be further strengthened.

4 Prospects for Research and Application of Network Security Technologies in New Power Systems

4.1 Perception Technologies

Future new power systems will require more intelligent and efficient security perception technologies to cope with the growing network security threats. On the one hand, security perception methods based on artificial intelligence, big data analysis, and other technologies will become essential means for ensuring the security of power systems in the future. By collecting, storing, processing, and analyzing various types of data within the system, timely monitoring and early warning of security events can be achieved. This enables rapid response and handling of security incidents while mitigating potential security risks [9]. On the other hand, the application of Internet of Things (IoT) and blockchain technologies will also provide strong support for security perception in new power systems. Through the implementation of IoT technology, interconnectivity between information collection devices can be achieved, thereby improving the reliability and accuracy of information. Additionally, the introduction of blockchain technology can ensure the security and integrity of information, particularly in addressing supply chain security issues and data privacy protection.

4.2 Disruption Technologies

Threat disruption technologies for new power systems will evolve in the following directions: Firstly, threat identification and defense technologies based on artificial intelligence and machine learning will be widely applied [10]. These technologies enable rapid identification of anomalous behaviors through monitoring and analyzing massive amounts of data. Consequently, effective defense and isolation measures can be implemented to mitigate potential security threats. Secondly, trusted computing techniques achieved through encryption and Internet of Things (IoT) technologies will serve as vital means for threat disruption. Trusted computing techniques ensure the integrity and security of information during transmission, preventing tampering or unauthorized access. Additionally, IoT technology facilitates secure communication and authentication between devices, guarding against illegal access and attacks.

4.3 Security Detection and Assessment Technologies

Security detection and assessment technologies are effective methods for identifying and evaluating security vulnerabilities and risks in power systems. Firstly, security detection methods based on artificial intelligence and machine learning will be widely adopted. These technologies enable the monitoring and analysis of massive data to identify potential security vulnerabilities and risks, facilitating rapid response and mitigation. Secondly, security detection methods based on Software-Defined Networking (SDN) and Network Function Virtualization (NFV) will also become a future trend. SDN enables network programmability and flexibility, enhancing the efficiency and precision of security detection and defense. NFV, on the other hand, enables the virtualization of network functions, allowing for flexible and scalable combinations in different scenarios, thus

improving the agility and scalability of security detection and defense. Additionally, the application of blockchain technology and edge computing will contribute to enhancing the security detection and assessment capabilities of new power systems. Blockchain technology ensures the security and integrity of information, particularly in addressing supply chain security and data privacy protection. Meanwhile, edge computing enables rapid response and processing between devices, effectively mitigating issues such as network congestion.

4.4 Verification Technologies

Verification technologies aim to simulate and test various network attacks and security vulnerabilities in power systems, enabling the timely detection and resolution of these issues. Firstly, highly accurate and reliable network simulation technologies will gradually gain widespread adoption. These technologies can rapidly establish and validate complete power system network topologies based on real-world scenario data and network configuration information. They facilitate simulation and testing of multiple types of attack and defense scenarios. Secondly, testing methods based on artificial intelligence and machine learning technologies will also become a future trend. These technologies enable the monitoring and analysis of attack and defense data, identifying potential security vulnerabilities and risks, and facilitating rapid response and mitigation. Additionally, the application of virtualization and cloud computing technologies will contribute to enhancing the capabilities of network security simulation and testing. Virtualization technology helps in the rapid construction and simulation of network environments, while cloud computing technology enables efficient collection and analysis of attack and defense data, thereby improving the efficiency and accuracy of the testing process.

5 Conclusion

As the new power system gradually expands and becomes operational in Jiangxi, the company is facing an increased number of network security risks. This paper has elucidated the network structure characteristics and security risks of the new power system. It has identified the challenges faced by traditional network security protection systems in terms of power structure, grid configuration, business models, and technological foundations. There is a need to enhance the capabilities of network security protection in areas such as trusted access, intelligent perception, and precise defense. Additionally, ongoing research and application of perception technologies, blocking technologies, security detection and assessment technologies, and verification technologies are essential. By continuously strengthening the construction of the network security protection system, we can safeguard the development of the power grid in Jiangxi.

References

1. Zhang, S., Deng, Y.: Research on security risk assessment and countermeasures in Jiangxi power Grid. Sci. Innov. Appl. **05**, 109–110 (2021)

2. Hu, P., Jia, J.: Network security protection in new power systems. Electron. Des. Eng. **27**(17), 22–24 (2019)
3. Wang, C., Zhong, Y., Li, Y.: Research on network security protection of power systems based on precise perception. Power Autom. Equip. **03**, 188–192 (2022)
4. Zhang, H., Cao, H.: Security risks and precautions in the construction of intelligent power systems in Jiangxi power grid. Intell. Comput. Appl. **10**(04), 28–32 (2020)
5. Sun, Y., Li, S., Wang, Y.: Research on security situation awareness and early warning of Jiangxi power grid based on big data technology. Power Syst. Tech. **42**(03), 584–590 (2018)
6. Li, H., Wu, Z.: Research on network security of power systems based on blockchain. Power Syst. Tech. **44**(05), 1479–1488 (2020)
7. Wang, S., Xu, J.: Risk assessment of network security in smart grids. Power Autom. Equip. **03**, 24–28 (2019)
8. Zhang, B., Zou, P., An, Z.: Network security issues and countermeasures in the construction of intelligent power grid in jiangxi power grid. Sci. Inform. **02**, 83–84 (2021)
9. Liu, J., Zhao, Z.: Security analysis in the construction of intelligent power systems in Jiangxi power grid. Power Sci. Eng. **38**(04), 46–50 (2022)
10. Xiong, Y., Luo, L., Dou, Y.: Construction of security protection system for Jiangxi power grid based on threat intelligence. Power Syst. Protect. Control **50**(06), 1–6 (2022)