The security protection technology and architectural design of distributed generation scheduling control systems

Xiao Zhang*, *Xiaoming* Chen, and *Yuan* Liu

State Grid Hubei Electric Power Co., Ltd. Wuhan, China

Abstract. This paper delves into the pivotal role of Distributed Generation Scheduling Control Systems in the power grid and addresses critical network security issues. It analyzes key concerns like data collection, security monitoring, and device management during distributed generation integration, proposing a comprehensive set of security technologies and architectural designs. The research covers network security identification for these systems and secure access and management for distributed generation terminals. The goal is to ensure the security and reliable operation of Distributed Generation Systems within the power grid.

1 Introduction

In recent years, in response to the challenges posed by the integration of large-scale distributed generation sources such as wind and photovoltaic power, the concept of cluster control mode [1-2] has gradually gained attention from scholars both domestically and internationally. The concept of distributed generation clusters does not change the way individual distributed generation sources are connected to the grid. Instead, it aggregates distributed generation units that are geographically close, have similar functional characteristics, or complement each other, using advanced control, measurement, and communication technologies. This is achieved through a specific software framework that enables the coordinated and optimized operation of multiple distributed generation units [3-4]. The security of the Distributed Generation Scheduling Control System, as a critical component, not only affects the normal operation of the power system but also relates to the stability and security of the national power supply. Therefore, security protection technologies for The Distributed Generation Scheduling Control System are of paramount importance.

Currently, as a complement to centralized power generation, distributed power generation and its system integration technology [5] [6] have matured. Despite the many advantages brought by the Distributed Generation Scheduling Control System, its security faces serious challenges. With increased system interconnectedness, the threat of network attacks is also on the rise. Security threats such as malicious intrusions, data leaks, and service interruptions can severely impact the system's operation and availability. Therefore,

* Corresponding author: 108279397@qq.com

this paper will delve into the challenges that the Distributed Generation Scheduling Control System faces in the field of network security and propose solutions to ensure system stability and data confidentiality.

The research objective of this dissertation is to carry out an in-depth study on the cybersecurity of the Distributed Generation Scheduling Control System and to propose key technologies and strategies to guarantee the security and stability of this system. The research work of this thesis includes the following aspects:

- Authentication Mechanism Research: Propose authentication techniques applicable to distributed power scheduling control systems to ensure that only legitimate users and devices can access critical resources.
- Network Security Risk Analysis: Conduct a comprehensive network security risk analysis of the distributed power scheduling control system, and gain an in-depth understanding of the system's working mechanism, networking methods, and possible vulnerabilities and threats.
- Research on Communication Encryption Technology: Explore communication encryption technology to ensure the confidentiality and integrity of communication data between terminals and prevent data leakage and tampering.
- Security Policy and Privilege Management: Research on the design of security policy and the implementation of privilege management to ensure that the operation of the system is restricted and only authorized users can perform specific tasks.
- End-Side Security Management: Emphasizes on end-side security management, including techniques such as monitoring network activities, recording security event logs, and responding to potential threats in order to maintain the security of end devices.

2 Security risk analysis of distributed generation scheduling control system

The security of the Distributed Generation Scheduling Control System is of paramount importance. Therefore, this chapter will conduct a thorough analysis of the system's network architecture to identify potential network security risks, including possible attack points and vulnerabilities.

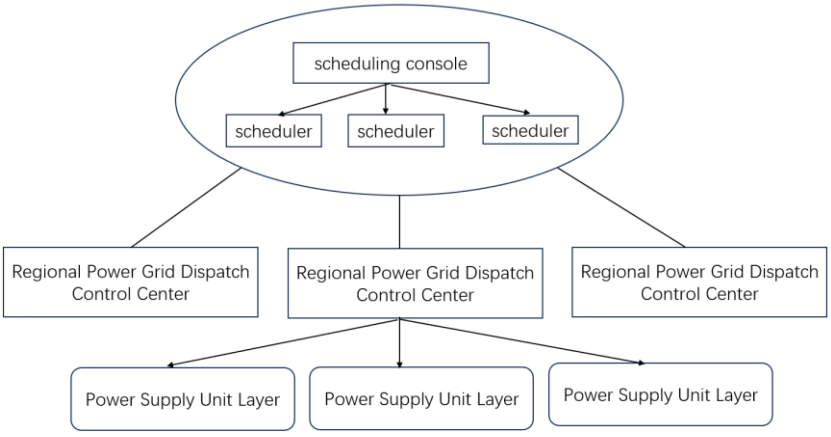

Fig. 1. The structure of a distributed power dispatch control system.

The Distributed Generation Scheduling Control System can be divided into four levels following the Internet of Things architecture: 'Cloud,' 'Management,' 'Edge,' and 'End.' In this context, 'Cloud' represents the cloud control platform for Distributed Generation (DG) clusters, 'Management' refers to the communication methods of the control system, 'Edge' represents the computing and processing elements near the data source, and 'End' signifies DG smart terminal devices [7].We need to gain a deep understanding of the system's internal communication architecture to identify potential points of intrusion and data transmission pathways. Fig. 1Outline of the structure of a distributed power dispatch control system. We will carefully examine the data transmission processes within the system and assess their security. This includes the processes of data collection, transmission, and storage. We will examine the risks of data tampering, hijacking, or unauthorized access, as well as determine whether encryption and authentication measures are employed in data transmission

Following a comprehensive analysis of the system's network architecture and data transmission processes, we will focus on identifying potential network security risks. This will involve the identification of attack points and vulnerabilities, including but not limited to the following: Intrusion Risks, Vulnerability Risks, Data Security Risks. In the following chapters, we will discuss in detail how to address these potential risks to ensure the security of the system.

3 Design of security protection architecture for distributed generation scheduling control system

The design of the security architecture encompasses several critical aspects, covering network security, data security, device security, and more, all organized within a comprehensive and hierarchical security framework. This framework enables the system to better withstand potential threats and attacks. The security architecture is shown in Fig. 2.

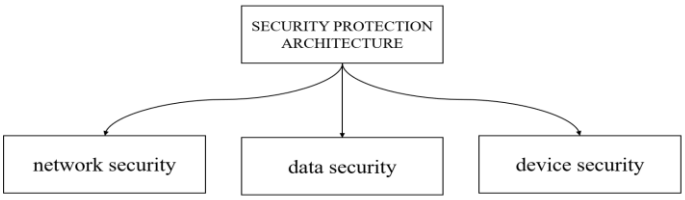

Fig. 2. Security architecture.

The security architecture of The Distributed Generation Scheduling Control System forms the foundation for ensuring system stability and security. It is not only essential for the system's operational reliability but also directly impacts the stability and security of the nation's power supply. Therefore, a comprehensive security architecture is of paramount importance.

We will design network perimeter protection strategies to safeguard The Distributed Generation Scheduling Control System from threats originating from external networks. This will include the deployment of security devices such as firewalls, intrusion detection systems, and intrusion prevention systems, as well as the implementation of strict access control policies to limit external access to the system.

The Distributed Generation Scheduling Control System relies on accurate data collection to support decision-making and operations. Therefore, ensuring data security is of utmost importance. The data collection strategy will explicitly define which data needs to be collected, along with the frequency and method of collection. Collecting only necessary data helps reduce potential risks. Data is transmitted using encrypted communication to prevent data theft or tampering during transmission. Furthermore, data integrity verification is employed to detect any malicious alterations during data collection and transmission.

To further enhance system security, we will propose security zoning strategies. This will aid in dividing the system internally into different zones, each assigned different security levels and permissions. This strategy ensures that even within the system, sensitive data and critical functions are adequately protected.

Security monitoring and analysis serve as the frontline defense for system security. They are used to promptly detect potential threats and anomalous behavior and take appropriate measures. If anomalies or threats are detected, the system will trigger alerts for immediate action.

To ensure system security, we will effectively manage and control critical security devices. Firewall and network device configurations will be regularly reviewed and updated to adapt to new threats.

Through these security protection measures, The Distributed Generation Scheduling Control System will establish a robust security foundation to fend off various potential cybersecurity threats, safeguarding the system's normal operation and data confidentiality.

4 Network security recognition technology

Network Security is of paramount importance in The Distributed Generation Scheduling Control System. Intrusion Detection Systems (IDS) are crucial components for protecting the system against unauthorized access and malicious attacks. IDS detects potential intrusions and abnormal behavior by monitoring network traffic and system activities. Here are key aspects of IDS in The Distributed Generation Scheduling Control System:

1) Intrusion Detection Technology Selection: Choosing appropriate intrusion detection techniques, including signature-based detection and behavior-based detection, to cover various network threats.
2) Real-time Monitoring and Log Recording: Establishing real-time monitoring mechanisms to promptly detect potential threats and recording all network activities for subsequent analysis.
3) Alert and Response Mechanism: Setting up an alert system to issue timely alerts when IDS detects abnormal activities and taking necessary response actions, such as isolating infected devices or terminals.

Network monitoring is a critical component of ensuring network security. It helps in identifying potential threats and abnormal activities in real-time.

Malicious traffic identification refers to recognizing malicious activities in network traffic, such as malware propagation, network attacks, or data leakage. Here are some key technologies and methods related to malicious traffic identification:

1) Signature Recognition: Identifying malicious traffic by detecting specific characteristics of malicious software, attacks, or malicious traffic, such as malicious URLs or virus signatures.
2) Behavioral Analysis: Monitoring traffic behavior, including packet frequency, size, source, and destination, to detect abnormal or malicious behavior.
3) Machine Learning: Using machine learning algorithms to train models to detect novel malicious traffic and threats.

4) Sandbox Analysis: Isolating potential malicious traffic in a secure environment for analysis to determine malicious behavior.

Malicious traffic identification helps prevent network attacks and data breaches, enhancing the security of networks and systems.

In The Distributed Generation Scheduling Control System, analyzing network threats is crucial. And security event response is a crucial aspect of network security operations, helping to reduce potential risks and damage.

Network security identification technologies play a vital role in The Distributed Generation Scheduling Control System. They enable timely detection and response to network threats, ensuring the system's availability, integrity, and confidentiality. By comprehensively applying IDS, network monitoring, and network threat analysis technologies, the system can better protect the power network from potential risks and attacks.

5 The security access and management techniques for distributed power source terminals

In a distributed power generation system, ensuring the legitimate access of terminal devices and protecting the security of communication between terminals is of paramount importance. The following three key technologies are crucial for the security of distributed power generation terminals:

1) Access Authentication Technology
2) Data Encryption and Identity Authentication Schemes
3) Terminal-Side Security

These key technologies and practices will contribute to ensuring the secure access and management of distributed power source terminals, thereby enhancing the overall security and stability of the system.

6 Conclusion

In this paper, we have delved into the network security issues of the Distributed Generation Scheduling Control System and proposed a series of key technologies and strategies to safeguard the security of this critical system. The main research work and achievements of this paper include:

1) We extensively discussed network security identification technologies, including intrusion detection systems, malicious traffic recognition, and security incident response strategies. These technologies and strategies provide vital support for the security protection of the Distributed Generation Scheduling Control System.
2) Authentication mechanisms, communication encryption techniques and security policies with rights management are discussed in depth.
3) Secure access and management techniques for distributed power terminals are presented, emphasizing security management and monitoring measures on the terminal side to ensure that only legitimate devices and users can access the system.

These works and achievements provide important theoretical and practical foundations for ensuring the security and stability of the Distributed Generation Scheduling Control System.

Throughout the research process, we have also faced some challenges and limitations:

1) Rapidly evolving threats: Network threats and attack methods continue to evolve, requiring continuous updates and improvements in security measures to adapt to new threats.

2) Complexity and cost: Implementing advanced security technologies and strategies may increase system complexity and costs, necessitating a balance between security and usability.
3) Compliance requirements: Compliance requirements in the power industry are constantly changing, requiring assurance that security measures comply with the latest regulations and standards.

Future research should continue to focus on the security of the Distributed Generation Scheduling Control System to adapt to the evolving threat landscape.

References

1. HAN Y, ZHANG K, LI H, et al. MAS-based distributed coordinated control and optimization in microgrid and microgrid clusters: a comprehensive overview [J]. CSEE Journal of Power and Energy Systems, 2019, 5(3): 409-422.
2. XUE Feng, CHANG Kang, WANG Ningbo. Coordinated control frame of large-scale intermittent power plant cluster [J]. Automation of Electric Power Systems, 2011, 35(22): 45-53.
3. GU Chenxiao, GU Wei, CHEN Chao, et al. Distributed power cluster control and research on power information real-time simulation [J]. Automation of Electric Power Systems, 2020, 48(4): 64-71.
4. WAN Qingzhu, XUE Chan. The new progress on technology of regional micro-grids [J]. Journal of Electrical Engineering, 2017, 12(3): 53-5.
5. ACKERMANN T, ANDERSSON G, SODER L. Distributed generation: a definition. Electric Power Systems Research, 2001, 57(3): 195-204
6. WANG Jian, LI Xingyuan. QIU Xiaoyan. Power system research on distributed generation penetration. Automation of Electric Power Systems, 2005, 29(24): 90-97.
7. LIANG Zhifeng, YE Chang, LIU Ziwen, et al. Grid-connected Scheduling and Control of Distributed Generations Clusters: Architecture and Key Technologies. Power System Technology, 2021, 45(10): 3791-3802.