Research on Security and Protection of Grid System Information Communication Network

Lisha Wu, Tao Luo, Hao Wu, Yonghong Zhan, Linli Wang, Wupeng Zhao, Zhuxing Shao and Chi Feng*

State Grid Anqing Power Supply Company, Anqing City, Anhui Province, 246000, China

*Corresponding author’s e-mail: fchi@163.com

Abstract. Smart Grid is the product of deep integration of power system and information network. It applies advanced control technology, communications, information and networking to power systems. In the power generation, transmission, substation, power distribution, power consumption and dispatching, the integrated two-way flow of power flow and information flow is realized in the power grid. The smart grid information exchange is frequent, the coverage is large, the related equipment is complex, and any node may have information security problems, which causes the smart grid to malfunction and cause different degrees of harm to the society. Therefore, information security issues have become an important factor affecting the development of smart grids. This paper discusses the development overview, architecture and key technologies of smart grids and analysis the security risks of current smart grid information systems. Aiming at the information security problem in smart grid information communication system, an access control scheme is proposed to facilitate key management and maintenance, which improves the security of the communication system in the smart grid, enabling the smart grid system to operate more safely and reduce the harm caused by grid damage to society.

1. Introduction

In the development of society, the power industry is a very important industry, and its role in economic development and people's lives is irreplaceable. In the power station, various other energy sources are converted into electric energy, which is transmitted to various parts of the country and distributed to various factories and residents' homes, which provides great convenience for the people's production, life and social development. The stable power grid system is a prerequisite for the stable development of society [1].

The grid system can operate safely and stably, and it is inseparable from the stable operation of the information network. Without a stable network, the entire grid system will also be paralyzed. As a smart grid of the new power grid, it integrates advanced technologies such as information technology, automation control technology and communication technology and integrates with the physical grid. Reliable network security is indispensable for the stable operation of the smart grid. If there is a safety problem in the course of operation, it will have a very serious impact. Therefore, the network security of smart grid has long received the attention of various countries, and many scholars are committed to research in this area to improve the stability of smart grid network operation [2][3].
2. Grid system overview
At present, the smart grid is still in the development stage. The definitions in different countries and even regions are not identical, but the ideas are the same. The basic idea is to integrate modern science and technology with traditional power grids. A smarter grid system is created by the integration of grid resources with modern advanced science and technology. The architecture of the smart grid is shown in Figure 1.

![Smart grid architecture diagram](image)

It can be seen from Figure 1 that the architecture diagram of the smart grid includes the entire process from power generation to power consumption, which is mainly divided into six parts: power generation, dispatching, transmission, substation, power distribution, and power consumption. This division is based on the technical level and is divided according to the technology used. But no matter how it is divided, the power system is the most important core.

Through the above analysis, this paper believes that the smart grid can be summarized as follows: based on the traditional power grid, the smart grid is integrated into the traditional power grid by adopting the most advanced information communication technology, automation technology, sensor technology and other technologies, enabling access at each node. It is achieving hierarchical distribution control and power management, maximizing power resource utilization, ensuring safe and stable operation of power systems, improving power users’ electricity experience, and improving power supply quality [4].

3. Key technology of the power grid
In the future, SG will introduce more renewable energy sources such as wind power and photovoltaics, change the energy structure of existing power grids, and realize diversified supply of power resources [5]. The relationship between computer network systems and smart grids will be closer. The main differences between the traditional grid structure and the smart grid structure are shown in Table 1.

| Traditional power grid | Smart grid |
|-----------------------|-----------|
| Centralized power generation | Centralized & distributed generation |
| One-way communication | Two-way real-time communication |
| No implementation feedback | Set up monitors and sensors |
| Closed/proprietary/distributed | Open / standardized / integrated |
| Manual operation | Automation (self-monitoring, self-removal) |
| Passive consumption | Active consumption |
| Vulnerable | Highly secure (end-to-end protection) |
The power flow information is integrated into the computer information environment, which changes the closedness of the traditional power grid. The power energy structure is improved by introducing renewable energy such as wind power and photovoltaic. To unify power planning and scheduling. The key technologies of the smart grid are shown in Figure 2.

![Figure 2. Key technologies of smart grid](image)

The smart grid integrates communication technology, information technology, sensing and measurement technology, and power grid technology, and comprehensively utilizes intelligent devices to build an intelligent and high-speed information communication system to achieve flexible access to a variety of different services. The physical grid and the information network are combined to form a multi-energy and communication information system.

4. Grid system network security status

After the deployment of the grid system network, due to the relatively poor natural conditions, each unit will face an external attack and cannot guarantee its security. The sensor network uses broadcast communication, and the transmitted information is easily intercepted. Multiple nodes are deployed in the sensor network. Due to the limitation of energy, WSN is not suitable for encryption or authentication technology when data processing is performed. As a result, there are many potential problems in the WSN, which affects the normal operation of the network. Grid system network security is mainly threatened in the following aspects [6]:

- **Information theft.** Since the communication network of the grid system broadcasts and transmits data to the neighbor nodes, other external devices can capture the information transmitted by the nodes within the effective frequency range, so that the information leaks and the security of the grid communication data is compromised.
- **Sensor node is captured.** In a wireless network environment, network devices are easily captured, making sensor nodes face the threat of malicious attacks.
- **Destroy the network.** In the communication network of the power grid system, once the network node is attacked, the node fails or the energy is exhausted, the node will exit the network, causing the sensor network to lose connection.
- **Tampering with information.**

5. Grid network security protection measures

5.1. Information security technology
Compared with the traditional grid system network, when the smart grid fails, it will bring more serious harms: damage some data and information, cause major economic losses, and cause harm to the lives of the people and cause social turmoil. Greater harm. Therefore, relevant information security technologies are adopted to strengthen the protection of network communication in the power grid system to ensure that the communication system can operate safely and stably.

- **Firewall technology.** A firewall is used to separate an untrusted network from a trusted network.
- **Antivirus technology.** Computer viruses seriously affect information communication systems. Anti-virus technology can be divided into virus prevention technology, virus detection technology and virus removal technology, and belongs to the category of computer security technology.
- **Intrusion detection technology.** Intrusion detection technology is a security protection method behind the firewall. It actively protects the network system from network attacks and effectively complements the firewall technology. Once an abnormal intrusion activity is discovered, the protection policy is immediately activated to cope with the abnormal intrusion behavior of the network.

### 5.2. Smart grid information security design

In the smart grid communication information network, timely and complete transmission of information is achieved as the highest priority. Therefore, in the smart grid system communication network, the integrity of the information must first be ensured, and the request to access the system is strictly verified to ensure that the malicious threat can be completely blocked. In the power system, once the communication system has problems, it will lead to the paralysis of the entire power grid system. Therefore, the availability of the power grid system is the premise of the normal operation of the power grid, and it should be considered in the intelligent grid information security design.

In the information communication network of the smart grid, it is possible to ensure the credibility and accuracy of transmitting and receiving information, and privacy is a secondary consideration. On this basis, this paper presents a security scheme based on access control and data integrity authentication to ensure that only legitimate devices are allowed to access the system, thus preventing the transmitted data from being tampered with by illegal devices.

The JADE-based Smart Agent Security Communication Model (SASCM) is shown in Figure 3 below. Its components mainly include: ECDH-based key interaction unit, ECDSA-based identity authentication unit, and encrypted data transmission unit. The main purpose of the SASCM module design is to serve two communicating entities to provide secure communication services. The SASCM module is designed based on ECC and AES. The core security technologies of this module mainly include ECDH key agreement algorithm, ECDSA fast digital signature algorithm, MD5 hash function and AES symmetric key technology. The reliability of key transmission is realized by the negotiation algorithm using ECDH key; the communication integrity is realized by MD5 hash; the confidentiality of data transmission is realized by AES symmetric key; the security between agents is realized by digital signature technology to prevent malicious data.
In digital substation, SASCM design can solve the communication security problem between intelligent agents. However, in the process of network information interaction, information security problems still exist. These problems can be solved by measuring application transparency. The encryption granularity is a key. Parameters, the security performance of the SASCM module has a lot to do with this parameter. The network layer where data encryption is located determines the choice of encryption granularity. The lower the network hierarchy, the higher the transparency of the application. Therefore, the larger the system communication bandwidth resources occupied, the greater the impact on the network performance of the system. Through analysis, the SASCM secure communication module can meet the information interaction requirements between agents, reduce the consumption of resources, and can adapt to the network system in the digital substation [9][10].

After analysis, it is found that the SASCM secure communication channel model mainly includes the following two advantages:

- During the interaction process of the communication module, the data has confidentiality and integrity: in the data transmission, the 256Bite AES encryption algorithm is adopted, and the message verification code is realized by calculating the MD5 hash, thereby realizing the confidentiality of the data and Integrity.
- Transparency in data transmission: Data exchange between agents in the substation is completed through the Agent platform, without the participation of third-party systems.

6. Conclusion
This paper introduces the smart grid, compares the difference between the traditional grid and the smart grid, and highlights the advantages of the smart grid. However, one of the most important concerns of the development of the smart grid is the network security of the information communication system. The security situation was analyzed and a security scheme was designed to improve the security of the current network system. The network security of smart grids is still under constant research. As a theory and core technology, cryptography can provide data security services for information communication systems.

References
[1] Chen Shuyong, Song Shufang, Li Lanxin, et al. Overview of Smart Grid Technology[J]. Power System Technology, 2009, 33(8): 1-7.
[2] Kosut O, Jia L, Thomas R J, et al. Malicious data attacks on the smart grid [J]. Smart Grid, IEEE Transactions on, 2011, 2(4): 645-658.

[3] Amin S M, Wollenberg B F. Toward a smart grid: power delivery for the 21st century [J]. Power and Energy Magazine, IEEE, 2005, 3(5): 34-41.

[4] Mei Shengwei, Wang Yingying, Chen Laijun. Reviewing the status quo and some prospects of smart grid information security from the perspective of complex networks[J]. High Voltage Engineering, 2011, 37(3): 672-679.

[5] Hu Yan, Xie Xiaorong, Han Yingwei, et al. Overview of the design method of power information system security system[J]. Power System Technology, 2005, 29(1): 35-39.

[6] Ma Wei, Li Wei, Zhu Shaohua, et al. Discussion on key issues of smart grid information and communication technology [J]. Electric Power Automation Equipment, 2010 (5): 87-91.

[7] Yu Yong, Lin Weimin, Deng Song, Che Jianhua. Cloud computing application and security research in smart grid[J]. Information network security. 2011(06)

[8] Li Bin, Bo Zhiqian: Protection and Control System for Smart Grid[J], Automation of Electric Power Systems, 2009, 33(20): 7-12

[9] Yang Yixian, Li Yang. Information Security Technology of Smart Grid[J]. ZTE Communications, 2010(8).

[10] Ding Champion, Fan Bangkui, Lan Haibin, Long Teng, Wang Jing, Chen Zhiyong. Research on Information Security Threat and Defense Strategy of Smart Grid[J]. Power System Technology, 2009, Vol.33(8): 1-7