Research on Smart Grid Energy Internet of Things Technology and Network Security

Guang Tao¹, *, Qian Zhang²
¹Wuhan University of Bioengineering, Wuhan 430415, China
²Wuhan Qingchuan University, Wuhan 430415, China

*Corresponding author e-mail: 19295940@qq.com

Abstract. With the rapid development of smart grid technology, energy IoT technology has become a new direction for the development of power grid enterprises. The energy Internet of Things covers the state of perception, information transmission and intelligent processing of the smart grid, and comprehensively improves the depth, breadth and density of information perception of the grid. The construction of smart grid energy IoT is an important development direction under the smart grid. The article analyzes the technology and network security of the smart grid energy Internet of Things. Based on the characteristics of the smart grid energy Internet of Things and the security risks it faces, the full-scenario network security protection technology adapted to the smart grid energy Internet of Things is analyzed. The suitable intelligence is studied from four aspects: perception layer, network layer, platform layer and application layer. The architecture and content of the full-site network security protection system of the grid energy Internet of Things provides ideas and methods for effectively ensuring the network security of grid enterprises.

1. Introduction
With the rapid growth of electricity demand in society, the safety of power grid operation has become an issue of increasing concern. However, due to the evolution of the network application model, the complexity of the application environment and the wide application of new network technologies, new security issues are brought to the power Internet of Things [1]. The article deeply analyzes and studies the characteristics of power Internet of Things and the security threats and attack modes faced by each level, proposes corresponding security protection measures, and gives the security protection architecture and system of power Internet of Things, which provides strong support for power Internet of Things security.

The power industry is directly related to the national economy and people's livelihood, and has high requirements for reliability and safety. The introduction of the Internet of Things technology into the smart grid has better realized the advantages of the smart grid. At this stage, the smart grid is a modern power grid that combines advanced sensing, information communication, analytical decision-making, automatic control and energy and power technologies, and is highly integrated with the grid infrastructure. The core of the smart grid is an integrated, high-speed two-way communication network [2]. And advanced information communication. Compared with traditional power grids, smart grids are more interactive, open and complex in information interaction. With the increasing interaction between
systems and the wide application of smart sensors, information security issues are becoming more and more important [3].

Power Internet of Things is the application of the Internet of Things technology in the business of smart grid. In the power generation, transmission, substation, power distribution, power consumption and other aspects, the terminal device with information sensing capability, edge computing capability and management execution capability is fully deployed. Effectively integrate power system infrastructure resources and communication infrastructure resources, promote full-scenario perception, information fusion and intelligent assistant decision-making in the whole process of grid operation and enterprise operation, improve the utilization efficiency of existing infrastructure of power system, and provide full chain management for power grids [4].

2. Smart grid energy IoT network security risk analysis

The smart grid energy IoT architecture is from bottom to top: sensing, transport, platform and application. Smart Grid Energy IoT Logical Architecture.

The sensing collects raw data from a variety of smart devices such as smart meters, sensors, handheld terminals, cameras, and PCs, and is the source of all data for the grid company. The network transmits the data collected by the sensing to the platform securely and reliably through network communication technologies such as a power communication network and a wireless private network. The platform stores, clusters, and analyzes data to provide data support for the application [5]. The application provides data to the user for service. Although the smart grid energy Internet of Things is a kind of network, it is denser than ordinary Internet sites, and the types of equipment are more complicated. The Smart Grid Energy IoT adopts the "data acquisition centralized control regional autonomy" mode, which shifts from a single functional terminal to an integrated service terminal, and is faced with a change in the business model provided by various types of services or services in an open platform. More complex security threats.

Figure 1. Smart grid energy IoT network security risk analysis structure
2.1. Security risks in the sensing
In the smart grid energy IoT environment, the risks of smart terminals such as the original collection and operation of the grid company still exist, and a large number of computing and storage restricted terminals access the network, which brings new security risks [6]. Smart grid energy IoT terminals are wide-ranging and large-scale, and the risk of cyber-attacks is high, which directly causes service interruptions and even affects the security of key information infrastructure of the power grid. Terminal computing and storage resources are limited, and traditional technical defense measures are invalid, which poses a major security risk. Edge-based agent security protection is not included in the existing security protection system.

2.2. Security risks in the transport
The new business model has changed the way business interacts, posing new challenges to the traditional security protection system [7]. Communication methods and network protocols are complex, and network security protection is more difficult.

2.3. Security risks in the platform
The smart grid energy IoT platform includes an integrated "national network cloud", a full-service unified data center, and an IoT management platform. Currently, the State Grid Corporation has developed a cloud platform protection solution, but the data, the IoT management center and other security mechanisms. Lack of security risks. In the smart grid energy IoT environment, the amount of data is large, the types are large and the interaction is complex, which further aggravates the risks of data leakage and illegal access. As an important part of implementing security protection, the IOT management center is particularly important for its own security.

2.4. Security risks in the application
The new business model poses challenges to existing protection systems and may touch national policy risks. The application of the Internet of Things model involves a wide range of applications and a large user scale, which poses new challenges to the application management mechanism and the application itself. The security responsibility interface is not clear and there is a security management gap. The smart grid energy Internet of Things lacks a complete network security protection standard, and lacks systematic and standardized guidance for grid company network security protection.

3. Smart grid energy IoT information security protection system construction
The energy IoT faces multiple information security risks. Based on the requirements of the power Internet of Things and smart grid, this paper starts from the sensing, the network and the use layer, and establishes a security protection system to prevent the power Internet of Things system according to the grid operation and management requirements and related regulations. Functional disruption, information disclosure, or tampering to prevent hackers or malicious manipulation of sensing devices or smart terminals.

3.1. Sensing security protection
The sensing realizes comprehensive collection of information such as device status, environmental information, geographical location, and real-time image by embedding sensing devices such as electronic tags, sensors, and cameras in the terminal device, and accesses information through short-range wireless and carrier technologies. Because a large number of terminal devices are exposed to the external environment, the wireless layer is connected to the network, and the sensing faces a serious security threat.

(1) Attack threat to device identity. Because the number of power IoT terminals is large, the deployment is scattered, and the surrounding environment is uncontrollable, this can cause an attacker to deploy malicious nodes within the network, impersonate legitimate devices, steal information, and even use malicious nodes as a springboard to attack the network.
(2) Threats to data transmission. In the cognitive network, the terminal devices are mostly simple in structure, and the information is transmitted through broadcast, multicast, etc., and is limited by the device information processing capability, and the information cannot be effectively encrypted and protected. When the data is transmitted in a wireless environment, the attacker is vulnerable to attackers. The destruction caused the data transmission to be interrupted, the data was intercepted, or falsified or forged.

(3) Data consistency threats. When the collected data is transmitted through broadcast, multicast, etc., the same data may be transmitted through different paths to generate multiple copies. If one of the copies has an error, the data receiving node may not be able to determine whether the data is true or not, resulting in convergence. When a node processes a different copy from the same data, it cannot determine the authenticity of the data.

Figure 2. Construction of Intelligent Grid Energy IoT Information Security Protection System

3.2. Network security protection
The network security protection is mainly aimed at various communication security of data aggregation and transmission in the power Internet of things, such as short-range wireless communication network security, wireless public network security, and optical fiber backbone network security.

3.2.1. Short-range wireless communication network security. Perceptual devices usually form wireless sensor networks. Because of their large amount of devices, limited resources, and open channels, they are vulnerable to various attacks. Therefore, data link layer or network security mechanisms are usually established, and encryption algorithms are used to establish a multi-channel key management system. To achieve equipment collection and transmission security; use the message authentication code and other mechanisms to complete the certification. At the same time, a routing security mechanism is established, and a wireless multi-path or channel filtering mode is adopted to prevent attacks such as DoS.

3.2.2. Network security of the wireless public network. Wireless transmission has the advantages of convenience and easy deployment. However, since the wireless transmission channel is open, it is very important to perform secure access and secure transmission. If the key facilities need to use the wireless public network to transmit service data, VPN or APN service should be adopted, and the end-to-end secure cryptographic algorithm should be adopted to ensure the confidentiality, integrity and freshness of the data transmitted on the wireless public network.
3.2.3. The boundary between the server and the communication network is secure. The communication network is responsible for data transmission, and various network attacks are often encountered at the boundary between the system server side and the communication network. To ensure border security, it is common to deploy independent security devices for network security access authentication, border access control, and information content filtering. At the same time, the audit algorithm is adopted to implement security mechanisms such as network connection restriction, intrusion prevention, and malicious code prevention to achieve boundary security control.

![Smart Grid Energy IoT](image)

**Figure 3.** Smart grid energy security protection technology implementation measures structure

3.3. Application security protection

3.3.1. User account security. Limit the range of network addresses that can be logged in to the terminal, authenticate the users of the access device, and control user access to resources. Establish a user behavior auditing system to audit important events such as user login and logout, connection timeout, configuration changes, and time changes. At the same time, the interface access control protocol is established, and the user is securely accessed through sharing passwords, so as to realize data exchange security between the Internet of Things system and other systems.

3.3.2. Operating system security. The operating system and middleware are responsible for system-level functions. They must follow the information security level protection requirements, refer to the operating system security level, select the security operating system or implement the operating system security mechanism configuration, and adopt the lowest available principle, combined with identity authentication, access control, and security audit. Security functions and mechanisms such as residual information protection for security protection.

3.3.3. Database system level security. Data is an important resource, database system security should also be in accordance with the corresponding information security protection level requirements, according to the database security level, select the appropriate security database or implement the database security mechanism configuration. At the same time, due to the particularity and importance
of the data, the data must be properly backed up. Develop a realistic data backup strategy, use disaster recovery technology and compatible storage media for backup.

3.3.4 Business application security. Business applications are complex and preventive from the business itself, business operations, and business storage access. Including identity authentication, access control and permission restrictions, security audits, and residual information protection, etc., in turn, security design, development, and online operations.

4. Smart grid energy security protection technology implementation measures

4.1. Adopting identity authentication technology
Each IoT terminal should have a unique identifier, each terminal has its own certificate key, and the massive IoT terminal faces the problem of how the identity and certificate are bound and corresponding. Identity authentication technology is an effective solution to the process of confirming the identity of an operator in a computer network. At present, the identity authentication systems of power grid enterprises are mostly based on public key infrastructure technology. They have the disadvantages of not being able to generate public keys on a large scale, need to run certificate directories online, and easily form performance bottlenecks, and cannot achieve large-scale applications. The combination public key cipher came into being, which was proposed by Nanxiang Hao, a famous cryptographer in China. Based on the new key management algorithm and mapping technology, it is an identification-based authentication mechanism that can effectively solve the problems and achieve scale. Applications.

4.2. Using Combined Public Key Technology
The public key technology is used to associate the identifier with the key certificate, and the public key matrix mapping algorithm is used to directly calculate the user certificate. The software and hardware password protection module is used to realize the fast authentication basis of the identifier, that is, the certificate, and the decentralized and lightweight secret is constructed. Key management system, which supports massive distributed applications of IoT terminals, supports end-to-end identity authentication and end-to-end data security transmission, supports offline identity authentication mechanism, and avoids the key management center becoming the bottleneck of IoT applications. The terminal authentication system for the Internet of Things is similar to the traditional authentication products in terms of product implementation. It can be constructed from three aspects: back-end system, software application and terminal-side deployment. It has the characteristics of lightweight, system and high efficiency.
The distribution of IoT security protection is based on the connection of people, things and things, and provides security protection from the sensing, network, platform and application, mainly improving the distribution of IoT intelligent terminals, and the authentication in the segmentation interaction process. Ways to promote the comprehensive perception and intelligent services of the distribution of Internet of Things, and build a security protection system for the distribution of IoT networks. The sensing focuses on strengthening the capability of terminal data encryption, terminal authentication and authorization, and basic hardening to ensure the security of the terminal body and access behavior. The network focuses on strengthening data transmission protection, access authentication, network isolation, and network security gateways to ensure data transmission and service access security of distribution terminals. The platform and the application focus on strengthening cloud security protection capabilities, security monitoring capabilities, and situational awareness capabilities to ensure access security for power distribution applications.

5. Conclusion
The construction of the smart grid energy IoT full-scenario network security protection system can effectively protect the overall network security protection capability of the power grid enterprise. In terms of management effectiveness, the first is to improve the security management and control capabilities of the IOT terminal through security chips and key technical defense measures. The unified identity security management and control of the terminal solves the user's identity security mark and verification problem; the second is the improvement of the security interaction capability of the object, the trust problem and the security and reliability problem when the Internet of Everything is solved, and the interactive authority can be controlled and the interaction behavior can be checked. Sensitive interaction is confidential. In terms of economic benefits, through unified design of modular and standardized terminal security protection technical measures, the requirements of business security protection can be quickly met by dynamic configuration and combined reuse, and unified security building situation awareness, panoramic security monitoring and intelligent disposal, etc. Infrastructure
to avoid redundant construction on basic security protection and save construction costs. In terms of social benefits, a full-site network security system will be established to drive the industrial ecology to lay a solid foundation for safety and interaction in the energy industry. The smart grid energy Internet of Things covers all aspects of information sensing, data transmission and intelligent disposal of smart grids. It plays a huge role in power grid construction, production management, operation and maintenance, and user services, and can comprehensively improve the information perception depth of all aspects of smart grid. And breadth. With the continuous promotion and application of the smart grid energy Internet of Things, new security protection issues will continue to emerge, and in the future, new technologies can be introduced to further enhance the security of the power Internet of Things.

References
[1] Ding Geyuan, Li Zhenjiang, Sun Bin, Yin Haitian. Smart Grid and Its Information Security Analysis. Microcomputer & Applications, Vol. 11 (2015), p.112 - 115.
[2] Zhang Benli, Liu He. Research on the Institutional Framework and Application of Internet of Things in Smart Grid. Communication Management and Technology, Vol. 6 (2016) p. 89 - 93.
[3] Xia Xianghong. Analysis of Internet of Things Technology and Its Application for Smart Grid. Shandong Industrial Technology, Vol. 6 (2016), p.95 - 98.
[4] Luo Qiaohua. Internet of Things technology and its application analysis for smart grid. Electronic Technology and Software Engineering, Vol. 2 (2015) p.103 - 105.
[5] Ling Junbin, Liu Ting. Analysis of Internet of Things Technology and Application for Smart Grid. Mechanical & Electrical Engineering Technology, Vol. 11 (2016) p.91 - 93.
[6] Zheng Xiaoyan, Li Runzhe. Research on IoT Architecture and Application Scheme for Smart Grid. Science and Technology Outlook, Vol. 2 (2016), p.65 - 68.
[7] Wang Jimpeng, Yin Wei, Li Wenhui, Yu Zhihao, Zhang Hao. Application Research of Internet of Things Technology in Smart Grid. Electromechanical Components, Vol. 3 (2016) p.74 - 78.