# Research on Power Network Security Technology and Protection

Aidong Xu[1],Kai Fan[2],Hang Yang[1]

[1]Electric Power Research Institute.CSG,Guangdong,510700,China
[2]China Southern power grid,Guangdong,510700,China

**Abstract.** With the rapid development of information technology construction in the power industry, research on network security has become a problem that cannot be ignored. This paper introduces the use of information communication network equipment at home and abroad in power system; analyzes the security risks of foreign network equipment in power system, shows the risk of power system network and the urgent need for localization of network equipment and analyzes the security of internal network of power system Risks; specific measures for the safety control of network equipment in the whole process are proposed to provide reference for power system network security protection.

## 1 Introduction

In the 1950s, some developed countries began to study the application of computer technology in business management, management, design, manufacturing, etc., and information technology gradually evolved from stand-alone, information islands to enterprise information integration. From the 1980s, China began to apply information technology to various fields. Due to its late start, the resources of foreign information communication network equipment were generally borrowed and introduced in the process of information construction[1].In February 2014, the central government established the "Network Security and Informatization Leading Group", which highlighted the important position of information network security in national security. Network security and informatization are a daunting task because it involves all network devices, and device security is an important aspect of overall network security [2?3]. At the same time, with the rapid development of power information technology, the information construction of various units has gradually deepened. As a basic industry related to people's production and life, power information construction is an important manifestation of the safety production and productivity level of power companies.

## 2 Status of use of information communication network equipment at home and abroad in power systems

The hardware devices used in the power system information communication network mainly involve network devices, communication devices, hosts, servers, and storage devices. The foreign hardware devices introduced mainly involve minicomputers, high-end servers, high-end storage devices, and some network devices, and minicomputers. High-end storage devices in the short-term domestic manufacturers can not compare with foreign manufacturers, while other devices such as servers, low-end storage devices, network equipment, the current domestic product features and performance can meet the relevant requirements of the power industry. Especially for network equipment, with the improvement of the functions and performance of related network equipment products in China, it has the ability to replace foreign network equipment in the power system information communication network. The foreign information communication network equipment currently used by the power system includes Cisco, IBM, HP, Juniper and other vendors, mainly based on Cisco network equipment, accounting for 95.82% of foreign information and communication network equipment. Domestic information and communication network equipment used includes H3C, Huawei, Maipu, ZTE, and Bonfire. The main products are H3C and Huawei network equipment. H3C network equipment accounts for 65.17% of domestic information and communication network equipment[2].Authenticated bypass vulnerabilities and remote control vulnerabilities, such as being exploited, can cause network communication disruptions, network devices, and even remote execution of malicious programs. At the same time, foreign network equipment may have undiscovered security vulnerabilities or malicious code embedded in advance, so accelerating the implementation of localization of power system network equipment is necessary to ensure network security[3].

## 3 Power system information communication network security risk analysis

### 3.1 Overview of power system information communication network security risks

Even since the "Eleventh Five-Year Plan", the power company has completed the isolation of internal and external networks, and comprehensively built a defense system for hierarchical protection with the "three lines of defense" as the core. The "three lines of defense" effectively protect the core business systems and data security. At the same time, it basically eliminates the possibility of external personnel directly accessing the information intranet and the production control network of the large area. However, the power system security laboratory further analyzed the security risks of network equipment at home and abroad and found that if there are security holes in the device or malicious programs such as backdoors and Trojans are implanted in advance, even in the case of physical isolation, the attack can be performed as follows. The power network diagram is as follows.

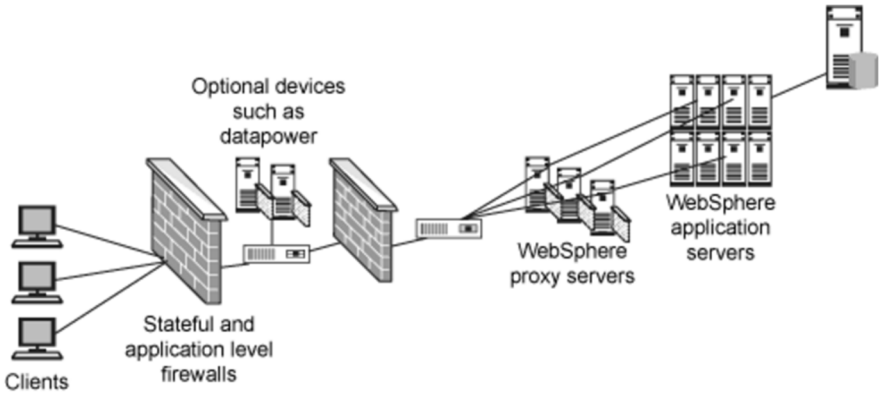


**Fig.1** Power network diagram

Use electromagnetic radiation or radio signals to activate the vulnerability. The attacker uses engineering means to add wake-up programs and instructions to the hardware device in advance, and relax the signal radiation standard of the hardware device so that it can be detected for use at any time, and then the electromagnetic signal transmitted by the device is detected and deciphered. Activate the backdoor with a wireless radiation virus. The attacker deposits the virus into the mobile storage medium or the mobile terminal. When the mobile storage medium or the mobile terminal communicates with the internal network, the virus uses the network device vulnerability to inject into the internal network[4].

### 3.2 Analysis of internal network security risks in power systems

The intranet of the production control area in the power system and the information intranet in the management information area constitute two "offline" internal networks separated from the Internet. From this analysis, it can be seen that “offline attack” may pose a threat to the internal network of the power system, and there are mainly the following risks:

There are a large number of foreign network devices, mobile storage media and mobile terminals in the information intranet, and there is a risk of being implanted in the back door. The attacker initiates an attack by injecting a virus or a control device by activating the back door.There is a large amount of "electromagnetic radiation" in the information intranet, and there is a risk of "radiation attack". The attacker launches an attack by receiving radiation from various types of devices to activate the back door or injecting a virus.In the intranet of the information, there is a wireless network for internal communication, that is, "wireless communication", and the attacker directly attacks the device and the system by means of wireless communication.

## 4 Power system information communication network security protection measures

### 4.1 Localization of network equipment

The purpose of localization of network equipment is to avoid the uncontrollability of security risks of foreign network equipment and to ensure that the power system network equipment is controllable, controllable and under control. The power companies can jointly carry out the localization transformation and testing of various domestic network equipment resources by the manufacturers within the United Nations. In accordance with the principle of “being easy after the first, then the external network and the internal network”, under the premise of ensuring the normal operation of the power system, further Promote the localization process[4].The proportion of power network equipment is as follows.

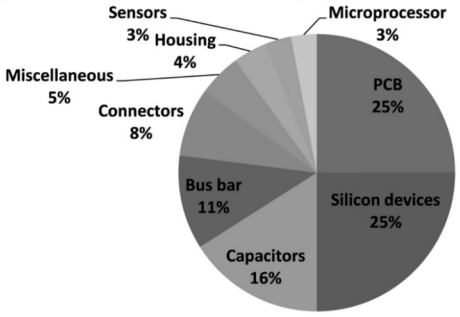


**Fig.2** Proportion of power network equipment

### 4.2 Network equipment procurement security control

The network equipment procurement security management mainly regulates the requirements of network equipment in qualification review, equipment selection, and security access, ensuring that the purchased network equipment meets the security requirements. Establish a sound security access mechanism for information network equipment resources before purchasing products; review the network equipment supplier enterprise security qualifications, personnel safety indicators, service quality evaluation, and network equipment qualification access conditions in the equipment selection process. Key equipment to carry out pre-selection and comprehensive safety inspection of products, timely discover various potential security backdoors, strategic configuration and malicious code risks; specify bidding security technical requirements for network equipment in the bidding procurement process, and clearly identify the confidentiality of the manufacturer in the procurement contract Terms and security constraints[3].

### 4.3 Network equipment online security control

The online security management of network equipment mainly ensures that the network equipment meets the requirements of information security of the state or company before going online. Before the online service, the internal security professional team conducts security assessment on the network equipment to ensure the security of the network equipment hardware, avoiding security loopholes or being implanted with malicious programs such as backdoors and Trojans. The internal team is implemented to ensure that the network equipment is deployed. Security of configuration and operation, and integrity in identity authentication, access control, and log auditing.

### 4.4 Network equipment operation monitoring security control

Network equipment operation monitoring and security management mainly ensures the safe operation of network equipment by strengthening information system security monitoring and strengthening information security supervision. The power company should cooperate with the National Information Security Evaluation Center and the National Security Technical Team of the General Staff Department to conduct network equipment vulnerability mining and risk warning work, summarize and improve the power company security vulnerability database, and carry out the deepening application of the vulnerability database, vulnerability detection and vulnerability tracking repair work. The power company shall establish a security risk prevention and early warning mechanism for the power company network equipment, optimize and improve the company's internal and external network monitoring system, and monitor various types of network equipment patch vulnerability repair status, abnormal access status, special port usage status, network service status, and equipment performance status[5].

## 5 Summary

As the country further strengthens network security and information management and the advancement of informationization in the power industry, network equipment is the basic unit of power network construction, and its information security is an important part of power system network security. Through the analysis of the security risks of foreign network equipment and the research on the security risks of power systems, this paper shows the necessity of accelerating the localization of power system network equipment and strengthening the security management and control of network equipment[6]. At the same time, this paper combines the actual situation of power system and proposes security protection measures for the power system information communication network. Even so, as the security system requirements for power system information continue to improve, it is still necessary to further strengthen network security and protection measures[7].

## References

1. Amin Akrami,Mohammad Ghaderi,Saeed Ghadi. Synchronous Study of Ferroresonance and Inrush Current Phenomena and their Related Reasons in Ground Power Networks[J]. Scientific Journal of Riga Technical University. Power and Electrical Engineering,2010,27(-1).
2. Hyung Min Kim. Introducing the New Concept of National Power: From the Network Perspective[J]. Peace Economics, Peace Science and Public Policy,2011,15(1).
3. Thomas Otieno Olwal,Karim Djouani,Okuthe P. Kogeda,Barend Jacobus Van Wyk. Joint queue-perturbed and weakly coupled power control for wireless backbone networks[J]. International Journal of Applied Mathematics and Computer Science,2012,22(3).
4. Zbigniew A. Styczynski,Chris O. Heyde,Kurt Rohrig,Krzysztof Rudion. Renewable Generation and Reliability in the Electric Power Network Zuverlässigkeit elektrischer Netze mit Energieerzeugung aus erneuerbaren Energien[J]. Methoden und innovative Anwendungen der Informatik und Informationstechnik,2010,52(2).
5. Fan Liu,Zhaohong Bie,Shiyu Liu,Tao Ding. Day-ahead optimal dispatch for wind integrated power system considering zonal reserve requirements[J]. Applied Energy,2017,188.
6. Hung Tran,Georges Kaddoum,François Gagnon,Louis Sibomana. Cognitive radio network with secrecy and interference constraints[J]. Physical Communication,2017,22.
7. Jonathan D. Fuller,Benjamin W. Ramsey,Mason J. Rice,John M. Pecarina. Misuse-based detection of Z-Wave network attacks[J]. Computers & Security,2017,64.