Research on Key Elements of Safety Problems in Power Automation Communication Network

Li Wenlong  Xiao wei  Ji Zhimin
Chongqing Aerospace Polytechnic 400021

Abstract: This paper briefly introduces the power communication system, expounds the power communication security protection technology, analyzes the security problems existing in the automation communication network, and conducts in-depth research and analysis on the security of the power automation communication network, hoping to secure the power automation communication network. Rationally utilizes the power automation communication network technology, improves the operation safety and stability of the power automation communication network, better meets the needs of the continuous and stable operation of the power automation communication network.

1. Introduction
In the current process of social and economic development, all walks of life show obvious trends of automation and informationization. The power communication network in the power operation system is the core component, which can ensure that the power system is systematically centralized in a wider range and improve power users. Distribute scientific rationality in terms of electrical energy. In the process of information technology development, the status of power communication system in power grids is more critical. New communication equipments are entering the power system. The level of digitization, automation and intelligence of power communication networks has increased significantly. The power communication system must maintain a safe and stable operating state to further ensure the safety of power grids. This paper has carried out research and analysis.

2. Power Communication System
The power communication system is the main component of the power system, which can meet the needs of information transmission in the operation, maintenance and management of the power system. It can significantly improve the scientific and rationality of the power supply and distribution of the power grid and ensure timely information of all types of power grids. Accurate transportation, better meet the needs of power fault handling, etc., providing important support for grid automation and intelligent development. In order to reduce the normal work and life of residents in the area, the operation of the power system must adhere to the principle of continuity, but the operation of the power system is affected by factors such as the complex situation of the power grid, and it involves a wide range of environments, while the environment, society and climate are complex. Many uncontrollable factors are prone to various problems in specific operations, and there are strict requirements in power dispatching communication. At present, the power departments in various regions have established special communication networks to adapt to the operation of power systems and better meet the needs of safe and stable operation of power systems.
3. Power Communication Security Protection

The power system is closely related to the people's life. At the same time, it belongs to the national energy development essential energy. Once the power grid fails, it will be very easy to bring impact and loss to the regional economy. Therefore, the power grid security protection and sufficient attention must be taken. Grid security protection belongs to a systematic project. In specific applications, it is necessary to use the construction process, management technology and corresponding processing methods to achieve effective integration of power communication automation technology. From the theoretical point of view, the application of grid security engineering can be combined with the information security engineering model. When applying the communication network, it must pay sufficient attention to information security, do a good job in analyzing and detecting the security system, and maintain the system alarm equipment, real-time monitoring and other modules. The continuous and stable operation ensures the security of all kinds of data information in the operation of the grid communication system, and encrypts the data of the power information system.

Data information encryption needs to use the corresponding encryption technology to convert plaintext into ciphertext and transmit. The current common data encryption algorithms include RSA "public key algorithm" and DES "data encryption standard algorithm".

3.1 Data Encryption Technology

3.1.1 RSA
RSA is widely used at this stage, and it can effectively resist most password attacks. Among them, PK (public key) and SK (private key), PK is public information, which can be publicly announced. SK belongs to confidential information and must be Specialized storage. There is a very close relationship between PK and SK. In order to ensure the security of the key, it is necessary to ensure that the number of RSK keys is not less than 500 bits. Generally, a 1024-bit RSA key can be used to increase the length and security level of the key. Correspondingly, the amount of calculation has increased significantly.

3.1.2 DES
DES technology is relatively mature in China, and has been widely used in gas stations and toll stations. It can effectively encrypt key data and is widely used in PIN encryption transmission and IC two-line authentication. DES technology has a very high security in practical applications. At this stage, in addition to the exhaustive method, it is difficult to use other convenient methods to decipher and attack it. When using the exhaustive method, a 56-bit key, according to the normal detection speed, takes more than 2,000 years to complete the search of all keys. Therefore, the DES technology is highly secure in practical applications.

3.1.3 Comparison of RSA and DES
DES technology has different methods such as linear analysis, differential analysis, and brute force attack. In the future development of computer technology, its performance will be significantly improved. At the same time, with the application of distributed systems, the DES security level will decline. The security of RAS technology is largely affected by integer factorization. In fact, it is very difficult to decipher RAS by factorization. Many RAS variants have been proved to be difficult to decompose. That is to say, when the power data is encrypted, if the security level of the power data is relatively low, the DES encryption method can be selected, and the ideal encryption effect can be obtained, which is economical and reasonable.

3.2 Key Technology
In the practical application, the data encryption technology must be managed with key to ensure the security and reliability of the key generation, storage and use. When there are problems such as secret key leakage, it is very easy to cause leakage of data information. Therefore, in practical applications,
is necessary to combine the key application environment and network security to analyze the factors and improve the scientific rationality of the key management method.

3.2.1 Key Distribution
In the key distribution mode, the KDC can use the central station to implement the key distribution with the server. This key distribution has a centralized feature and can also meet the central server peer server key distribution needs. Key allocation In practical applications, if the KDC can only meet the needs of a sub-station key distribution, try to choose a centralized distribution key. If a key can be distributed to a larger number of sub-sites at the same time, the peer-to-peer mode can be applied.

3.2.2 Preset Shared Key
Nodes in the network are shared with other nodes in terms of key distribution. Under normal circumstances, if the network has n nodes, each node needs to store a key. The preset shared key has great difficulty in practical applications, mainly because the network itself is large in size, and the preset shared key mode is used to store the node, which is very easy to cause waste of network space and storage resources, and must be selected in the sharing mode. Improve the effectiveness of data encryption based on the goal of network resource conservation.

4. Security Issues in Automated Communication Networks
The automation communication network has a wide range of applications in current power work, enabling real-time transmission, and the development of information transmission work is characterized by automation and high efficiency. In the uplink data, there are telemetry, remote signaling, etc. In the downlink data, there are remote control, remote adjustment, and the like. These numerical control can better support the continuous and stable operation of the power grid, provide important support and reference for power work decision, and have strict requirements on security and real-time. It is necessary to ensure the confidentiality and integrity of data transmission. For non-real-time data, because of its large amount of data, although the timeliness requirements are not very strict, the security requirements are extremely high. In the process of power automation communication work, there are still several problems:

First, network information security, the current network technology is developing rapidly, and the information transmission process is very vulnerable to network viruses and threats. Network intruders can use the virus to perform system configuration without authorization, and change the transmission data. In this case, it will bring serious impacts and threats to network data security and power system stability. Third, system security, information transmission process must pay sufficient attention to system application, no matter what system, more or less There are certain security vulnerabilities. If criminals use this vulnerability to invade the system, it will directly threaten the security of power information. Third, application security, the current power information shows a clear trend of automation, and enterprises present in information transmission. Obvious diversification trends, information dissemination applications, in this part of the operation, it is easy to have information leakage and information integrity is broken. That is to say, the emergence of these problems will bring certain threats and impacts to the security of power data transmission. In order to effectively solve this problem, it is necessary to use power communication security technology to improve data transmission security.

5. Construction of Safety Management System for Power Automation Communication Network
First of all, in the construction of safety management system, it is necessary to fully analyze the economic indicators, network management requirements, communication system scale, structure, etc., the existence of these factors will affect the whole system function more or less, the power sector needs attention When the network management system is built, it is combined with the actual needs of the power communication network. In terms of security management configuration, the higher the level, the better, and the function is not very complete. It only needs to meet the power communication
problem processing needs. For example, in the grid operation process, more attention should be paid to the system real-time monitoring equipment, and the monitoring system should be improved to have comprehensive and real-time characteristics. If the power organization has high requirements in the grid communication and monitoring system, it can be established. A network element management system can achieve comprehensive coverage of power communication systems.

Secondly, China’s power sector has chosen power equipment production and design units for power network design. As a result, its network management system has very limited limitations and fails to fully consider the overall and overall issues. A complete network management system must have different results such as service processing, network element data collection, service management, and network element management. It also covers systems such as data access and collection, which not only meets the needs of a single network element management, but also satisfies Network management needs such as level and superior, carry out data collection, analysis, and processing of power systems to better meet the needs of communication system managers in system operation decision-making and planning. The network management system also needs to use hierarchical distributed management technology, fault intelligent prediction and analysis technology, etc., and can automatically search the entire system network. Clearly identify each node of the network, establish a corresponding physical topology based on the network’s Layer 2 connection relationship, monitor the network operation status in real time, find the security problems and hidden dangers of the system, and analyze and predict the system failure. The staff and management personnel of the power system of the system can be used only in terms of permissions, which can meet the needs of monitoring and management of different angles of the network, and can also regularly check and back up system data. That is to say, the application of the network management system needs to realize the comprehensive coverage of the communication network. The communication network involves a wide range of aspects, and it is necessary to increase management from the network and service aspects to better meet the security and stable operation requirements of the communication network.

Thirdly, optimize the management functions of the communication network management system in terms of fault, configuration, performance and security. In practical applications, the grid communication system needs to analyze the current network environment in combination with its own operating state, and timely discover the abnormal conditions and operations in the network operation process. Realize and accurately record these information, use data analysis and processing related software to achieve comprehensive processing of these information, accurately determine the location of the fault, identify the cause of the fault, explore the nature of the fault and the impact of the fault on the system, and provide rapid and effective prevention. And treatment measures to mitigate and eliminate the potential safety hazards. At the same time, it monitors the performance and parameters of various types of electrical and electronic equipment throughout the operation of the network, determines its operating status, and maintains network stability and security. In addition, physical topologies and logical topologies can be established to effectively adjust and optimize various types of resources, and improve the effectiveness of monitoring system-related performance indicators. Use security measures to prevent unauthorized users from intruding, resulting in the impact and threat of communication network stability and security. At the same time, the operating personnel and maintenance personnel are given the appropriate permissions to better meet their daily work needs.

Finally, information security management in power automation communication technology, power automation communication technology must be done in the application of information security management issues: First, a reasonable choice of encryption algorithm, the introduction of SSL layer at the application layer and network layer, improve data flow Encryption validity, in terms of encrypted content, it needs to include application data and transmission protocol content, etc., and divide the entire data stream into different data segments to be encrypted accordingly. Second, do a good job in personnel training, improve employee operational norms, and make employees clear information security. Management importance, learn data backup, data encryption and other operations, fundamentally solve information security problems; Third, the security room security management system, pay attention to the computer room inspection every day, limit non-worker access, but also
need to implement humidity, temperature Measures such as fire protection and access control.

6. Conclusion
Power and energy are related to the development of China's social economy. The power communication network belongs to the key component of the power system. Compared with other networks, there is still a certain lag in the utilization and development of China's power communication network, which provides safe and stable operation for the power network. Leaving a large security risk, the power industry must improve the importance of work in this area, enhance the informationization level of the power communication network, and use the network security protection system to better meet the economic and security needs of the power grid.

References
[1] Xiao Naiyi. Research on Internal Communication Network in Substation Automation System [J]. Digital World, 2018, (11): 43.
[2] Diao Yingying, Zheng Xia, Shi Zhuoxin. Research on Automatic Test Platform for Equipment Network Management of Power Communication Network[J]. Science and Informatization, 2018, (27): 14.
[3] Gao Hao. Distribution Automation System Based on Wireless Narrowband Data Communication Network [J]. Automation Application, 2018, (5): 88-89, 98.
[4] Yang Na. Research on internal communication network in substation automation system [J]. Wireless Interconnect Technology, 2017, (20): 7-8.
[5] Fu Ya, Yuan Sannan, Fu Du. Application Design of Telecontrol Communication Gateway in Power Dispatching Automation Channel [J]. Communication Power Technology, 2018, 35(4): 148-149, 151.