Pisco Med Publishing

Original Research Article

Analysis of Information Security Maintenance Countermeasures in Power Automation Communication Technology

Kun Luo*

Zhengzhou Railway Vocational& Technical College, Zhengzhou 451460, Henan, China.

E-mail: ztzylkyx@126.com

Abstract: This article is divided into three parts. The first part is to summarize the current situation of the use of power automation communication systems, information security, and the basic requirements of the current society for the information security of the system. The second part analyzes the current information security problems of power communication technology from human factors, natural factors, and technical loopholes. The third part explores the maintenance countermeasures to improve the information security of power automation communication technology and systems.

Keywords: Power Automation; Communication Technology; Information Security Maintenance

The power grid is an indispensable support system for modern social production and the normal operation of daily life. It is of great significance for promoting social and economic development. As an important part of the power system, the power communication system has the advantages of wide coverage and precise organization, covering power generation, distribution, power transmission, power transformation, power consumption and other subsystems. Its information quality is directly related to power distribution, transportation and other aspects, and its information security is directly related to the safety and stability of the operation of the power system and the user's power consumption and the security of related information. Therefore, in order to ensure stable and safe power communication support for life and production, it is necessary to improve the ability of power grid maintenance from many aspects. Improving information security in power automation communication technology is one of the most important tasks. Power companies need to increase resources invest to improve the information security of the technology and the entire power communication system by optimizing encryption technology, encryption algorithm, and strengthening daily management.

1. The current status of the use of power automation communication systems, the information security situation and its information security requirements in the new era

1.1 Current status of the use of power automation communication systems

The power automation communication system is composed of wireless terminals, base stations, application managers and other parts. Wireless communication is currently a common method of power communication. It has technical advantages such as simple installation and low cost, but the communication capacity is limited by information capacity and equipment distance. Besides, electromagnetic waves and other interference will affect the quality of information transmission. In response to these common problems, power companies often adopt two measures: ① relying on the existing public network to achieve information and communication upgrades through encryption technology, etc.; ② setting up a professional communication network. The two different forms of measures can optimize the information quality and information transmission capacity of the power communication system to a certain extent. It is also required to ensure that the multiple controls and maintenance system is in a long-term stable and healthy communication state.

doi: 10.18282/le.v9i6.1320

1.2 Information security of power automation communication system

Information technology promotes the rapid development of the power industry, and also makes its information security face more complex and diverse challenges. First of all, in the process of power grid operation, due to a large number of participants, there is greater difficulty in information management, and information security problems may cause problems such as unclear responsibilities and difficulty in quick accountability. Secondly, due to the hidden nature of power communication security accidents, related security accidents have emerged in recent years, but related companies have not yet solved them well, so the current power communication security problems are still very serious. In addition, the relevant laws and regulations are not perfect enough to effectively protect the information interests of related enterprises and people.

1.3 Basic requirements for information security of power automation communication systems

The data types of power automation communication systems are diverse, and the process of information transmission and reception is relatively complicated. In order to ensure the security and stable transmission of information, it is necessary to carry out real-time and non-real-time information transmission. Generally speaking, modern society has the following basic requirements for real-time and non-real-time transmission of power communication:

(1) Real-time data transmission requires real-time and accurate information transmission based on relevant information characteristics and technical requirements in accordance with relevant communication protocols. Generally speaking, there is less information adopting real-time transmission in power communication. The real-time data communication is relatively stable, and downlink data is generally stable in transmission to ensure the safety of information transmission, or to realize the transmission of information such as the cloud and the sea. The communication situation has a certain impact on the security and stability of the grid communication. The uplink data during real-time transmission includes new messages, records of emergencies, and telemetry data. This type of data is important data used by enterprises to determine power dispatch and grid operation, and requires high timeliness, security and confidentiality.

(2) Non-real-time data transmission, which has the characteristics of a huge amount of information and complex information, and has no timeliness requirements for information transmission nor high requirements for its transmission speed. A certain degree of transmission delay can be allowed. Non-real-time data mainly includes Information on the use of electric energy, related equipment by end users, and regular maintenance records of grid equipment. This type of information requires relatively high information integrity, security and confidentiality.

2. Analysis of factors affecting the security of power automation communication information

2.1 Human factors

During the operation of the electric power communication system, human factors caused by improper management are a major hidden danger of electric power information security. This is mainly due to the fact that in the management process of the system, some operation permissions are not clear enough, the operation process is not standardized enough, and the staff's operation is highly subjective. It may even be caused by poor professional ethics of the staff, malicious damage or disclosure of confidential information for personal gain.

2.2 Natural factors

In addition to man-made and technical factors, some natural force majeure will also affect the quality of power communication transmission and information security, such as severe weather such as storms, will have a certain impact on related communication equipment, and even disrupt its normal information transmission and reception process. When the equipment is damaged, the power communication system is also more vulnerable to man-made and technical information threats.

2.3 Technical vulnerabilities

The vulnerabilities in power automation communication technology can be divided into two directions: system central station and wireless terminal technology vulnerabilities. The central station of the system is a centralized node for internal data, and the system sends and receives data through this interface. The node is attacked by information, which may not only cause the information of the entire system to be leaked and destroyed, but also cause the operation of the entire power system to malfunction. The central station information protection generally uses firewall technology. The firewall is used as a separator of internal and external information in the central station, or a monitor of the information transmission process. It can monitor and control the flow of data information in real time according to certain technical standards, restrict external operations from entering the central station, avoid providing dangerous services and restrict users' access to risky websites. However, if the internal personnel does not operate properly, the system may be invaded by viruses or hackers.

3. Research on information security maintenance countermeasures of power automation communication technology

3.1 Improve a unified and scientific power communication management system

In order to ensure that the power communication system is supported by effective technology and improve information stability and security, it is necessary to build a sound communication management system to effectively avoid information risks caused by internal personnel operations. To improve the power grid communication management system, it is not only necessary to build a complete and reasonable internal management system for the information and communication departments, but also to effectively cooperate with relevant departments to carry out scientific and unified system management so that the information of various departments of the power grid system can be circulated reasonably. It is also needed to build an intelligent unified management platform to improve the implementation of the system and achieve efficient and high-quality work management.

3.2 Integrate intelligent technology to realize all-round power communication management

In the process of construction and management of electric power communication systems, enterprises should carry out related work in a more scientific and standardized manner in combination with smart technology, use technologies such as the Internet of Things and related smart management platforms to manage all forms of power information in a comprehensive and intelligent manner. The use of high-quality and comprehensive auxiliary information management on smart platforms and other methods can more effectively intercept and deal with hidden power communication hazards such as network viruses. Electric power companies need to strengthen the monitoring of communication networks, reasonably set security passwords and information operation permissions, so as to improve the effectiveness of information management. It should also use advanced information equipment and technology to reduce power consumption, increase transmission speed, and conduct regular and frequent maintenance work, such as regular maintenance of the system, elimination of hidden information hazards, regular upgrades and optimization of anti-virus software and virus databases.

3.3 Optimize technology to improve the quality of information maintenance

In order to ensure security during the normal transmission of power information, automation technologies such as communication encryption should be optimized. First, it should provide users with a strict identity authentication function, improve the security of terminal access, and prevent random access and tracking access. At the same time, it is necessary to optimize encryption technology and algorithm to better maintain power information, such as using link encryption, hybrid encryption and other multi-level encryption methods, to improve the security of power information through hybrid and multiple encryption mechanisms when it is transmitted between adjacent nodes.

4. Conclusion

In summary, improving the information security of the power communication system is very important for the normal operation of the power system and the normal development of people's related activities. However, power communication faces security threats such as internal human factors and external malicious attacks. Enterprises should actively carry out targeted reforms in terms of communication technology and work management, improve the quality of related management, supervision, and maintenance work, and use hybrid encryption and other technologies to better improve the security of the power information transmission process.

References

1. He A, Liu C. Analysis and prevention of information security problems in power automation communication technology. Technology and Market 2019; 26(12): 157-159.
2. Wang H, Li Z, Chen Z. Construction of information security in power automation communication technology. China New Technology and New Products 2019; (05): 143-144.
3. Hu J, Hu Z. Analysis and prevention of information security problems in power automation communication technology. Science and Technology Wind 2018; (35a): 62.