Research on Informatization Construction of Electric Power Communication Network under Smart Grid

Yan Zhuang¹, Jie Xu¹*, Hui Yuan¹, Liang Dong¹, Yue Guo¹, Yintie Zhang²

¹State Grid Hubei Electric Power Information and Communication Company
²Information Systems Integration Branch, NARI Technology Co., Ltd, China

*Corresponding author: xu4901@sgcc.com.cn

Abstract. This article analyzes the current situation and existing problems of the regional power communication network based on the theory of power communication technology, and then realizes the optimization design of the power communication integrated network system, including planning goals, communication cables, power communication transmission network and communication business network construction, and finally comprehensive Analyse the effect of the optimization design of the power communication integrated network system. Through the test of the power communication integrated network system, it is shown that the optimized network system can effectively meet the requirements of the unified construction of the prefectures and counties, and can also improve the reliability of the regional data network and the disaster tolerance system of the existing data network Demand to improve the stability of the system during operation.

1. Introduction
Network security and informatization is an arduous task, because it involves all network equipment, and equipment security is an important aspect of overall network security. At the same time, with the rapid development of power informatization technology, the informatization construction of various units has gradually deepened. Electricity is a basic industry related to people's production and life. Electric power informatization construction is an important manifestation of the safe production and productivity of power enterprises. However, due to the uncontrollability of foreign information and communication network equipment manufacturers and products introduced in the informatization construction, the hidden dangers of the information resources of foreign manufacturers have been continuously exposed, and the information network security issues related to enterprises and countries have become increasingly prominent. In recent years, the state has begun to support domestic manufacturers to explore the localization of information and communication network equipment resources. However, due to the fact that there are still a certain number of foreign network equipment in use in the information and communication system of power companies, and some core technologies and standards of foreign network equipment products have long been used by foreign countries [1]. Manufacturers are in control, so research and analysis on the security of power system information and communication networks is urgent.
2. Optimized design of power communication integrated network system

In order to effectively ensure the feasibility and scientific of the power communication network system design, this paper integrates the construction characteristics and current situation of a certain regional power communication network in the network optimization design process, and comprehensively considers the actual needs, so as to effectively realize the power communication integrated network system Optimize the design.

2.1. How to deploy the system

It can be seen from Figure 1 that in the process of integrated network system design and research, it is necessary to effectively select the headquarters and local city-level power supply companies, and create power communication management systems respectively. This level of management systems can be connected to each other in the role of the data network. Among them, the provincial management system can directly manage the backbone communication network, the prefecture-level management system can manage the city-level power supply company network, and the two-level power communication management system is interactive, which can ensure that the provincial department can the power communication network performs macro management. This hierarchical deployment management method can effectively avoid the impact of power communication failures of power supply companies on other companies, and it is combined with the modern domestic power communication hierarchical operation and maintenance management structure mode, thereby facilitating the development of the work [2].

![Figure 1. The deployment structure of the integrated power network management system](image)

2.2. Creation of communication cable

Based on the existing power communication network optical fibre system, the optical fibre communication network is effectively improved, which mainly includes 10kV optical cable lines, 220kV optical cable lines and 110 optical cable lines. Figure 2 is a 10kV optical cable circuit diagram.
2.3. Integrated network management hardware architecture
In the design of the integrated network management system of the power communication network, effective and unified management at the provincial and municipal levels is required. Therefore, it is necessary to integrate the maintenance terminals, configuration servers and system external equipment of the provincial company and the power supply company at the provincial level with the provincial power communication network. The data networks are connected to each other, and the comprehensive data network is reasonably used to effectively realize the data interconnection between provincial companies and prefecture-level power supply companies, and give full play to the functions of the maintenance terminal and monitoring management of the integrated network management system. The integrated network management system of the electric power communication network belongs to the whole, so the hardware architecture should also be fully expressed in the form of diagrams. Figure 3 shows the hardware architecture of the integrated electric power communication network management system [3].
2.4. Software architecture of integrated network management system

The integrated network management software architecture in the power communication network mainly includes the platform and subsystems. The subsystems mainly include four types of communication operation management, communication integrated monitoring, communication professional management, and communication resource management. Figure 4 shows the software architecture of the integrated network management system. Among them, the network communication integrated monitoring subsystem refers to the subsystem used in the process of designing the integrated network management system, which mainly includes alarm management, alarm configuration and performance information management. The main function of this system is to use the protocol conversion method to comprehensively detect the alarm information of the system's intelligent equipment, which mainly includes power supply, switching and transmission equipment. Using direct mining can comprehensively detect the quality of non-smart device alarms and the environment [4].

![Software architecture of the integrated network management system](image)

Figure 4. Software architecture of the integrated network management system

3. Safety protection measures for power mobile Internet

3.1. Mobile terminal security protection

Configure the security module on the terminal equipment of the slave station, and take security identification and data integrity verification measures for the control commands and parameter setting instructions from the master station system to prevent the master station from attacking the slave station terminal and malicious operation of electrical equipment. You can configure the hard press plate and soft press plate to start and stop the remote command execution on the slave terminal device. The hard pressure plate is a physical switch, which only allows local manual control after being opened, and can accept remote control after being closed; the soft pressure plate is a logical control switch in the terminal system. When the hard pressure plate is closed, the master station starts and Stop the processing and execution of remote-control commands. The terminal equipment of the sub-station shall have physical safety protection measures such as anti-theft, fire prevention, and anti-vandalism.
3.2. Mobile Internet network channel and border security protection

The goal of mobile Internet network security protection is to prevent malicious personnel from attacking business systems through the network, and to prevent malicious personnel from attacking network equipment. For routers, switches, EPON/GPON, wireless devices, firewalls, security gateways and other network equipment, security protection should be carried out in accordance with the national information security level protection requirements, security configuration reinforcement, and unnecessary services should be turned off; at the same time, access control, monitoring and auditing should be adopted, identity authentication, backup and recovery, resource control and other measures to provide security protection in terms of device security access, device security management, device vulnerability scanning, security event audit, configuration file backup, processing capacity assurance, and device link redundancy. Appropriate encryption and decryption measures should be taken during network transmission to ensure that sensitive information is not illegally intercepted when transmitted via the network; digital signatures are used to ensure that the information is not illegally tampered with or deleted. For wireless private networks using WIFI technology, the network security should be ensured from audit, certification and confidentiality, and the following security protection measures should be taken: It is forbidden to use the brand name or model of the router, name, address, company name or project team as its name, and the name is completely It is composed of random letters and numbers or any other string that does not reveal the router model or identity; disable the remote management option provided by the configuration software, disable the SNMP service, and ensure that no one can control the router settings through the Internet; limit the router’s broadcast area to ensure Cannot receive router signals in non-controllable areas; SSID (service device identification) broadcasting should be prohibited; MAC address filtering, use of access control lists; DHCP is disabled; closed network access control is implemented, only WIFI devices that know the network name or SSID Or users can connect; WIFI terminals should be audited, identified and stripped of illegal WIFI terminals from the network, a standardized WIFI terminal audit and management system should be formed, and WIFI devices with fraudulent access behaviours should be restricted from random access to WIFI wireless access; should Use 802.1x authentication and key management methods; use WPA1 or WPA2 protocol encryption mechanism to encrypt data streams for WIFI wireless access [5].

3.3. Safely configure early warning equipment

Regarding the equipment network management subsystem in the power grid communication system, they are distributed in various computer rooms in the form of a network. This type of distribution not only makes the staff unable to detect the potential loopholes in the system in time, but also unable to timely Dealing with them in a timely manner also makes it impossible for network administrators to analyse the operation of the entire network as a whole, to understand the quality of the operation of the entire network, and to make macro-control and scientific evaluation of the entire network. In view of the above situation, the relevant staff of the electric power information communication system should start from the three aspects of the inspection system, the correlation analysis of the alarm information and the application system interface, further analyse the whole network, and adopt the simulation agent method to accurately deal with it [6]. Add barcodes required in the system. At the same time, the system with the context system is formulated, and the filled content is scientifically managed, so that the power evaluation can be suitable for their respective management locations.

3.4. Comprehensive security testing of data

For distributed systems commonly used in power grids, the number of applications of individual subject sensors has increased significantly, which leads to more complicated control programs designed for them. Therefore, in order to improve the accuracy of the detection data, it must be integrated to ensure that the power work can be carried out smoothly in all aspects and levels. Data integration is mainly to prevent the loss of original alarm information, reduce the occurrence of alarms, and improve the rigor of data information obtained by the enterprise. In the process of integrating data, a variety of technologies need to be used, such as interface integration technology, IoT intelligent identification
introduction technology, and real-time monitoring data display technology, which are mainly used to locate communication resources.

4. Conclusion
Information and communication integration have become a current development trend, and has been generally recognized by scientific research institutions, communication operators, IT manufacturers and large enterprises. However, based on different needs and basic conditions, the development and implementation of information and communication integration have their own characteristics. Information and communication integrated operation and maintenance can straighten out the relationship between the power communication network and the information system, meet the needs of smart grids and modern enterprises, and give greater value to information and communication resources. Electric power information and communication network is one of the two physical networks of the power grid. The integrated operation and maintenance of information and communication must be planned and implemented around the goal of safe electric power production and enterprise intensive development. Therefore, the theoretical research and the discussion and practice of its implementation tools are the current problems that must be solved require new theoretical support, and need to break through the traditional architecture and supporting tools.

References
[1] Emmanuel, M. & Rayudu, R. Evolution of dispatchable photovoltaic system integration with the electric power network for smart grid applications: a review. Renewable & Sustainable Energy Reviews, 67(1) (2017) 207-224.
[2] Giustina, D. D. & Rinaldi, S. Hybrid communication network for the smart grid: validation of a field test experience. IEEE Transactions on Power Delivery, 30(6) (2015) 2492-2500.
[3] Carcangiu, S. Fanni, A. & Montisci, A. Optimization of a power line communication system to manage electric vehicle charging stations in a smart grid. Energies, 12(9) (2019) 1767.
[4] Rey, X. R. Halpin, T. J. Hadgekar, S. Miu, K. & Dandekar, K. R. Cybersecurity analysis of an ieee 802.15.4 based wireless sensor network for smart grid power monitoring on a naval vessel. Naval Engineers Journal, 130(3) (2018) 137-144.
[5] Mozafar, M. R. Amini, M. H. & Moradi, M. H. Innovative appraise ment of smart grid operation considering large-scale integration of electric vehicles enabling v2g and g2v systems. Electric Power Systems Research, 154(1) (2018) 245-256.
[6] Romero-Ruiz, J. Perez-Ruiz, J. Martin, S. Aguado, J. A. & De, I. T. S. Probabilistic congestion management using evs in a smart grid with intermittent renewable generation. Electric Power Systems Research, 137(8) (2016) 155-162.