

Information Security Protection Scheme of Multi Meter Integration System

Juan KONG¹, Wen-Juan SHI, Bing YANG, Jun-Quan ZHANG, and Shu-Xian LI
Beijing China-Power Information Technology Co.,LTD., Beijing, China

Abstract. Relying on its mature and complete power consumption information collection system, and in collaboration with other energy service enterprises, State Grid Corporation of China has carried out research and verification of "water, gas, and heat" multi meter integrated information collection technology in multiple provinces and cities across the country in recent years. Due to the fact that the "water, gas, and heat" multi meter integrated reading system requires a large amount of data interaction with external systems through various interfaces, as well as data interaction with water, gas, and heat companies through Internet VPN channels, there is a risk of data leakage caused by external systems illegally intruding into the company's internal systems through the Internet. To this end, with reference to the relevant regulations on information security protection of relevant business systems of the State Grid Corporation of China, the overall security protection architecture and specific security protection measures at various levels of the multi-meter integrated system are designed to maximize the security of relevant data of the multi-meter integrated reading system and the stable and reliable operation of the system.

Keywords. Multi integration system, safety protection, illegal invasion

1. Introduction

The construction of the "water, gas, and heat" multi meter integrated reading and collection system is an important strategy to promote the development of the Internet and national smart cities, and an innovative measure to address system connectivity. The implementation of the "multi meter integration" construction by State Grid Corporation of China is to utilize the existing electricity information collection system platform of power enterprises to achieve remote centralized reading and acquisition of public data resources such as water, electricity, and gas, create a new energy data platform, fully exploit the big data application of the electricity information collection system, create a new energy use business environment, fully support the construction of smart cities, and reduce the duplication of data system platform construction [1]. In short, relying on the "multi meter integration" collection system established by smart meters, it can achieve information resource sharing in the energy field, build a cross industry dynamic data integration platform for energy operation, and achieve comprehensive energy services such as centralized meter reading, charging, and energy management [2].

Fan Qing [3] proposed effective measures to improve the network security of electric power marketing information systems, fundamentally strengthening the stability of

¹ Corresponding author: JUAN KONG, Beijing China-Power Information Technology Co.,LTD., Beijing, China, E-mail: 15032358287@163.com.

electric power system operation and the security of electric power information networks. Cai Guangsong [4] takes comprehensively improving information security awareness as the starting point, fully considering the information needs of users at different levels, and reasonably formulating network security protection measures. Wang Wei et al. [5] analyzed the information security threats and requirements of charging piles, and designed a charging pile background service management center information security protection scheme based on authentication encryption. Su Qi et al. [6] proposed an information security protection system based on terminal security, which is conducive to the data protection of power industry systems and the safe operation of equipment information, and strengthens the construction of the entire power system information security system. Tan Kai et al. [7] proposed a lightweight charging pile key management scheme that can meet the security requirements of charging pile key management.

Due to the fact that the "water, gas, and heat" multi meter integrated reading system requires a large amount of data interaction with customers, water, gas, and heat companies through the Internet VPN channel, there is a risk of data leakage caused by external systems illegally intruding into internal systems through the Internet, and the leakage of sensitive data such as customer files and transaction information may cause serious damage to State Grid companies, social order, public security, and customer personal interests. In order to maximize the stable and reliable operation of the "water, gas, and heat" multi meter integrated reading system and the safe interaction of data, with reference to the relevant regulations on information security protection of the existing relevant business systems of the State Grid Corporation of China, an information security protection scheme for the system has been designed for different application levels of the multi meter integrated reading system.

2. Multi-meter Integrated Reading System

In recent years, relying on existing power acquisition systems, State Grid Corporation of China has successively carried out research and verification of multi-meter integration technology in branches in Beijing, Shandong, Shanghai, Jiangsu, Zhejiang, and other provinces and cities, covering an increasing number of residential users. In terms of economic benefits, the multi-meter integrated reading system has improved the value of the electricity information collection system, achieved the effect of maintaining and increasing the value of state-owned assets, further enhanced the market competitiveness of State Grid Corporation of China, and also improved the service efficiency and profit space of other companies such as water, gas, and heat, ultimately achieving the goal of providing users with more efficient, convenient, and comfortable services[8].

2.1. Application Architecture

"Water, electricity, gas, and heat" multi meter integrated meter reading system integrates with other public utility users such as water, gas, and heat to establish a combined meter reading and charging service that adapts to water, electricity, gas, and heat utilities. It utilizes the company's established data collection channels and electricity fee payment channels to achieve multiple meter combined reading and unified charging. The entire system includes five major functions: file management, joint meter reading, bill

consolidation and release, joint charging, and clearing and settlement. The specific functional modules are shown in Figure 1.

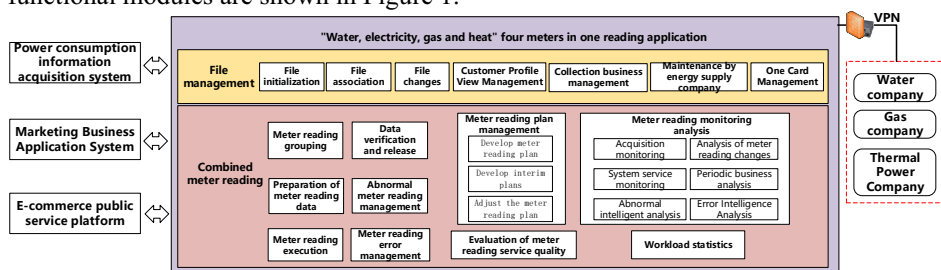


Figure 1. Framework of Multi Meter Integration System

Archives management module: The multi-meter integrated reading system obtains the archive information of water, gas, and heat users from the business system of the water, gas, and heat company, and integrates with the marketing business application system, including four sub functions: file initialization and association, file change management and association, customer archive view management, and acquisition terminal installation and debugging; **Combined meter reading module:** The power consumption information acquisition system (water gas heat meter acquisition module) provides water gas heat meter reading data on a regular basis or as required according to the water gas heat meter reading acquisition requirements, to complete the combined water gas heat meter reading; It includes nine sub functions: meter reading grouping, meter reading plan management, meter reading data preparation, meter reading execution, meter reading exception management, meter reading error management, meter reading monitoring analysis, meter reading service quality evaluation, and workload statistics; **The bill consolidation and release module** obtains power user billing information through integration with the marketing business application system, establishes a unified bill for water, electricity, gas, and heat, and releases it uniformly, including two sub functions: bill management and bill release; **The joint charging module** utilizes existing payment channels to provide services such as sitting, collecting, and withholding for water, electricity, gas, and heat users. Customers can directly pay fees through "one card" cards, achieving unified charging and printing "one ticket"; **In the clearing and settlement module**, after reconciliation with the water, gas, and heat companies, the fees of the water, gas, and heat companies are cleared and paid according to the negotiated settlement principles for the service fees of copying and collecting. It includes four sub functions: reconciliation management, expense clearing, payment settlement, and handling fee settlement.

2.2. Physical Architecture

The multi-meter integrated reading system is designed and developed using a B/S architecture. The system interfaces and integrates with the business information systems of companies such as water, gas, and heat through various interfaces and third-party networks. The third-party network is constructed using two boundary methods.

The network boundary directly formed between the information intranet of the power enterprise and the fixed networks of water, gas, and heat companies through optical fiber dedicated lines. The dual front-end mode is adopted, which means that the power company and the water, gas, and heat parties each build a front-end computer, and

the two front-end computers are connected in real time using optical fiber. Real time transmission of data is ensured through fiber optic dedicated lines.

The network boundary between the external information network of the power enterprise and the fixed networks of the water, gas, and heat companies is directly formed through VPN channels. An external network interface server is established for the information external network of the electric power enterprise and the water, gas, and heat companies, and the two interface servers are connected in real-time through VPN communication. Both interface servers are placed on the other party's information extranet and provide access ports for the other party through firewalls.

3. Information Security Protection Scheme

3.1. Information Security risk Analysis and Protection Objectives

"Water, electricity, gas, and heat" multi meter integrated reading system interacts with marketing business application systems and other business applications on the State Grid Corporation of China's information intranet, and the security risks faced are mainly application level unauthorized access risks; There is interaction with systems related to external businesses of water, heat, and gas companies through VPN networks. Due to the interaction between the company's external network and the water, heat, and gas network, the interactive data mainly includes sensitive data such as customer files and transactions. The security risks faced mainly include network level risks caused by network attacks that cause the overall security of the company's external network, and risks such as sensitive information leakage at the data level.

According to the national and company information security management requirements, combined with the risk analysis faced by the system, the main protection objectives of the system are determined to include: Ensure that the system meets the basic requirements for national information security level protection and company management information system security protection. Strengthen the protection of sensitive information such as user identity information, system configuration information, and business application data (customer archives and transactions) of the "water, gas, and heat" multi meter integrated reading system to ensure its integrity and confidentiality. Strengthen the security management of user accounts, authentication information, and operation permissions at the application and data levels, prevent unauthorized access, sensitive information disclosure, and other risks, and ensure the security of system applications and data. For the safety protection of water, gas, and heat meter reading data, the collection terminal and main collection station are responsible for the water, gas, and heat meter collection module of the power consumption information collection system. The interactive security between the meter reading data and the water, gas, and heat company is responsible for the "water, gas, and heat" multi meter integrated reading system.

3.2. Overall Protection Architecture

The "water, gas, and heat" multi meter integrated reading system is deployed on the information intranet of the State Grid Corporation of China, and interacts with the business systems of the water, gas, and heat companies through the Internet VPN channel.

The overall security protection of the system fully complies with the overall framework system of the company's information security protection, and carries out routine security protection design from eight aspects: physical, boundary, application, data, host, network, terminal, and security management, with a focus on strengthening the security protection of customer files, meter reading data, and billing record storage; Water meters, gas meters, and heat meters are physically isolated from each other, and are physically isolated from each other from electricity meters. During the data acquisition process, water, electricity, gas, and thermal data are transmitted independently. Those who do not meet the requirements of this scheme are not allowed to access the company's network.

3.3. Border Security

The "water, gas, and heat" multi meter integrated reading system is deployed in the information intranet, and the boundaries involved include: third-party boundaries of the information intranet, vertical boundaries of the information intranet, horizontal boundaries of the information intranet, internal and external boundaries of the information intranet, and Internet boundaries. For the third-party boundary of the information intranet, a dedicated encryption isolation gateway has been developed to meet the access requirements of large concurrent data collection in a short time. The security scheme of this device has passed the evaluation of the National Information Technology Security Research Center. Configure security policies such as access control, intrusion detection, logging, and auditing for the internal and external boundaries of information and the vertical boundaries of the internal and external networks of information, using the existing logical strong isolation, hardware firewalls, IDS/IPS, and other border security protection equipment of the company headquarters and various units, to achieve border isolation and security protection; For Internet boundaries, when using VPN channels to access data based on the existing border protection measures of each unit, the security protection of the channel itself is guaranteed by the telecommunications operator.

3.4. Application Security

"Water, electricity, gas, and heat" multi meter integrated reading system is a B/S mode application. The application system functional security is protected and designed from the following 13 aspects: identity authentication, access control, security audit, residual information protection, communication integrity, communication confidentiality, non repudiation, input and output verification, configuration management, session management, parameter operation, exception management, and resource control. The user's identity authentication and authorization are implemented based on the company's unified permission platform. Security functions such as access control, security audit, residual information protection, communication integrity, communication confidentiality, non repudiation, input and output verification, configuration management, session management, parameter operation, exception management, resource control, and application interface security are implemented through system software development. The interface security protection measures are as follows: Perform authentication before establishing a data connection to the web service interface. The authentication method adopts the user name/password method, and pass the user name/password through the Url parameter; Enforce requirements for password length,

complexity, and lifetime, and comply with the following security policies; The minimum password length is 8 characters; Passwords require a mixture of letters, numbers, or special characters; Prohibit passwords from being the same as user names; The periodic password change cycle is 180 days; During the authentication process, password information transmitted through the network is prohibited from being transmitted in clear text, and is implemented through hash (HASH) one-way operations, SSL encryption, SSH encryption, and other methods; By recording interface call logs, the system can provide evidence of data origination or reception to the data originator or recipient in the event of a web services request.

3.5. Data security and Host security

In the process of transmission and storage, the sensitive data of the "water, gas and heat" multi-meter integrated reading system faces the risk of tampering and leakage. The sensitive data involved in the system include: user account password data, system configuration management data, business data, important business data, and business data related to water, gas and heat meter collection. In the process of data interaction, it is necessary to achieve safe and accurate data transmission through transmission encryption, interface authentication, authority control and other processes, and by optimizing the security encryption algorithm.

The server operating system (linux) and database system (relational database) required for the operation of the "water, gas and heat" multi-meter integrated reading system are deployed in the communication room of each province (city) company, which is responsible for the security management and should meet the protection requirements of level 3 protection.

3.6. Network security

The "water, electricity, gas, and heat" multi meter integrated reading system is deployed in the ICT equipment rooms of various provincial (city) companies, mainly utilizing existing network equipment (including security equipment). Each provincial (city) ICT company is responsible for the security management of network equipment (including core switching equipment, access switching equipment, border fire walls, etc.), meeting the level 3 protection requirements for hierarchical protection.

The network channels involved in the "water, gas, and heat" multi meter integrated reading system are mainly the company information intranet vertical channel, the company information intranet and information extranet channel, and the company information extranet and water, gas, and heat network VPN channel. The company's information intranet is operated, maintained, and managed safely by the State Grid Communications Corporation and various provincial (municipal) unit communications companies. When using a VPN channel to transmit data, the security protection of the channel itself is guaranteed by the telecommunications operator.

3.7. Terminal security

"Water, electricity, gas, and heat" multi meter integrated reading system terminal equipment includes: information intranet office machine, acquisition terminal, communication interface converter, and intelligent electricity meter dual mode communication module.

Users and operation and maintenance management personnel of the "water, electricity, gas, and heat" multi meter integrated reading system use the existing information intranet office computer to access the system. Each unit shall conduct unified security protection and management for user terminals according to the company's information intranet office computer management requirements.

In order to ensure the normal operation of the acquisition terminal equipment and avoid safety issues, the following safety protection measures should be taken for the acquisition terminal equipment. As water meters, gas meters, and heat meters are owned by various water, gas, and heat companies, these metering equipment should have their own protective measures such as theft prevention, breakage prevention, and use safety. For water and gas heat meters that require access to the national network information intranet, security modules should also be used to ensure the security of the communication data interface within the system. It is required that the security modules installed in the water and gas heat meters should at least support SM1, SM2, and SM3 encryption algorithms. In principle, for water meters, gas meters, and heat meters that cannot be equipped with a security module, it is required that they cannot be connected to the national network information intranet for the time being. It is necessary for the water, gas, and heat meters to cooperate with the measurement equipment manufacturers of the water, gas, and heat companies to jointly develop and specify a security certification system and data collection format to ensure that the water, gas, and heat meters are connected to the national network information intranet. After development, the security certification method can be accessed only after passing the evaluation by the national security agency.

3.8. *Physical security*

According to the grading situation, the "water, electricity, gas, and heat" multi meter integrated reading system is deployed in the three-level system area of the existing information room on the provincial (municipal) information intranet. The provincial (municipal) telecommunications company is responsible for implementing security protection and management in accordance with the company's computer room management requirements. The system mainly implements the physical security of the system based on the security management of the computer room. Ensure the physical environment security of the network system through computer room monitoring and alarm management. The equipment in the computer room should be equipped with fixed operation and maintenance personnel for maintenance. Non fixed and unauthorized personnel are not allowed to enter. Before system operation and maintenance, physical access control should be used to identify the identity of operation and maintenance personnel, clarify the purpose, and record in detail the name, gender, unit, phone number, ID number, reception unit, time of entry and exit, temporary identification plate number, and belongings. The operation and maintenance personnel are responsible for maintaining the confidentiality of the passwords, core parameters, and business data of the network, host, system software, and application software, and shall not arbitrarily copy and disseminate them. During daily operation and maintenance work, unrelated personnel are not allowed to enter the computer room without the approval of the superior or relevant departments. If permission has been obtained, it is necessary to be accompanied by relevant personnel.

3.9. Safety management

For water, gas, and heat companies accessing the information network through VPN, users of VPN accounts must modify their passwords, which must be no less than six digits in length, and must not be a single column combination of letters or numbers. They must regularly change their passwords. "VPN accounts, passwords, USB-KEY, and hardware gateway devices should be properly stored, operated within the permissions granted, and fully responsible for all operations performed on this account." It is strictly prohibited to lend VPN accounts to others for use. State Grid Communications Corporation has the right to supervise and inspect the behavior of VPN users and conduct necessary processing. When the behavior of VPN users may endanger the system security, China Netcom has the right to first interrupt and terminate the use of VPN users, and then notify relevant personnel.

4. Conclusion

The construction of a multi meter integrated reading system has improved the work efficiency and service quality of energy companies, resulting in economic, management, and social benefits. The normal operation of the system requires a large amount of data interaction between different systems of different companies, involving multiple communication methods. The interactive data mainly includes important sensitive data such as customer archives, transactions, and records. It requires a large amount of data interaction with external systems through various interfaces, and data interaction with water, gas, and heat companies through Internet VPN channels. Therefore, there is a risk of data leakage caused by external systems illegally intruding into the company's internal systems through the Internet. Therefore, the overall security protection architecture and specific security protection measures at various levels of the multi-table integration system are designed. The measures proposed in this article improve the quality of customer sensitive data in the system, provide basic data support for the security of customer data assets, and maximize the security of related data in the multi-meter integrated reading system and the stable and reliable operation of the system.

References

- [1] Liu Yi, Huang Gaoyong, Chen Xinxin, Zhu Meng, You Shalin, et al. Discussion on "multi-meter integration" technology based on power consumption information collection [J] Communication power supply technology, 2019, 36 (11): 165-166.
- [2] Wang Yukun, Kang Yousong, Zhu Xinpo, Jiang Zaiyu, Zhang Yu, Yu Yu, et al. Research and implementation of water, electricity and heat multi-meter integrated reading system [J] Automation application, 2018, 11:84-86.
- [3] Fan Qing Network Security and Protection Measures for Electric Power Marketing Information System [J] Science and Information Technology, 2023 (1): 3.
- [4] Cai Guangsong Research on computer network information security and protection strategies in the era of big data [J] Abstract of Computer Applications, 2023, 39 (1): 3.
- [5] Wang Wei, Xian Zhu Jie, Tian Heping, Chen Zhen, Yuan Xiaoxi Design and Implementation of Information Security Protection Scheme for Electric Vehicle Charging Piles - Background Service Management Center [J] Electric Power Construction, 2019, 040 (005): 55-62.
- [6] Su Qi, Wang Wei, Liu Yin, et al Research on Information Security Protection Schemes in the Power Industry [J] Information Network Security, 2017 (11): 5.

- [7] Tan Kai, Li Zhongwei, Guan Yadong, et al Lightweight Key Management Scheme for Electric Vehicle Charging Piles [J] Electric Power Construction, 2019, 40 (9): 9.
- [8] He Huan, Zhang Qin, Ran Yanchun, et al. Application of power consumption information acquisition system in the construction of multi-meter integration [J]. Automation and Instrumentation, 2019, (2): 142-145.