The Design of Border Security Protection for Master Station of Power User Electric Energy Data Acquisition System Based on Security Domain Division

Wei Huang[1,a], Jun Zhao[1,b], Zhengmin He[2,c,*], Shidong Chen[1], Qi Qian[2], Jianfeng Liu[2], Yu Han[2] and Qiang Zhang[2]

[1]State Grid Hunan Electric Power Co., Ltd., Changsha 410004, China
[2]Beijing KeDong Electric Power Control System Co., Ltd., Beijing 100192, China
a. huangw33@hn.sgcc.com.cn, b. 443102156@qq.com, c. 411799731@qq.com
**Zhengmin He*

Keywords: Power user electric energy data acquisition system, security domain, border security protection.

Abstract: With the rapid development of network and information communication technology, the pertinence, concealment and persistence of network attacks are obviously enhanced. The original security domain division and border protection measures of power user electric energy data acquisition system can't fully meet the current protection requirements. In this paper, the high-voltage user cost control and load control business functions are separated from the other business functions of acquisition system and employed in marketing production control domain to improve the security protection capability. In addition, the security access area for acquisition terminals access to the master station is set up. Based on the new security domain division, a border security protection scheme for the master station of acquisition system by comprehensive utilization of various security protection measures and devices is designed. This scheme can comprehensively improve the protection capability of the acquisition system and have certain reference significance for the further planning and construction of the border security protection for the master station of power user electric energy data acquisition system in the later stage.

1. Introduction

In recent years, with the rapid development of network and information communication technology, the pertinence, concealment and persistence of network attacks have been significantly enhanced, and network security risks and threats have become increasingly prominent. There are some examples in the field of electric power. In November 2010, Iran's nuclear power station suffered from the “seismic network virus” attack launched by Israel and the United States, and the nuclear power station delayed power generation for more than half a year; in December 2015, Ukraine's power grid was attacked by cyber hackers, resulting in a large area of power outage; in June 2017, a highly customized malicious program “Industroyer” for power grid was made public; in March 2019, Venezuela experienced a nationwide power failure incident, it is said to have suffered from

"electromagnetic and cyber attacks" by hostile countries/forces. It can be seen from the above incidents that the attackers adopt advanced attack technology, the viruses are customized according to the network structure and system characteristics of the power production control system, and the destruction and spread paths of the viruses are highly hidden[1-2]. The safe production and operation of electric power are related to national security, national economy and people's livelihood, a sustained national power failure could bring the country to the brink of collapse and chaos.

The network security law of the People's Republic of China was formally implemented on June 1, 2017. As the key information infrastructure of the power industry[3], the power user electric energy data acquisition system should be given a key protection according to the network security law of the People's Republic of China.

Border protection is the focus of information system security protection. At present, border security protection design for the master station of power user electric energy data acquisition system is mainly based on Q/GDW 1377-2013 “technical specification for security protection of power user electric energy data acquisition system” in most of provincial electric power companies. All business functions are deployed in the information intranet of management information area. The protection level of cost control and load control functions of high-voltage users is not high enough. Once be attacked, it will cause serious consequences. In addition, there is no security access area for acquisition terminals access to the master station, so the application area of acquisition system is easy to be attacked. Furthermore, with the continuous expansion of Internet plus new business of the State Grid Corporation, new business terminals access and new technology applications are increasingly widespread, and new network borders are constantly emerging[4-5]. The prevention and control of personal privacy and data security is becoming more and more difficult, and relevant new protection measures need to be implemented simultaneously.

Therefore, there is an urgent need to optimize and improve the existing border security protection measures of the master station of power user electric energy data acquisition system. It is necessary to strengthen the border protection ability of the acquisition system according to the network structure characteristics of the power user electric energy data acquisition system, so that it can fully meet the security requirements of the State Grid information system.

2. Security Domain Division and Border Security Risks Analysis

2.1.Division of Security Domain

According to different security levels, business types, networking methods and other classification standards, the network can be divided into different areas, and the network borders are produced: the border between a network and other networks[6]. The first problem to be solved in border protection is to divide the security domain of the system and determine the borders of the security domain, and then take corresponding technical measures according to the characteristics of the system[7].

The power user electric energy data acquisition system not only involves data acquisition business and parameters setting business, but also involves high-voltage user cost control, load control business and low-voltage user cost control business. It belongs to the scope of power monitoring system, but it is not the traditional power monitoring system. Therefore, its security domain division is more complex. At present, the security protection guidance scheme of power monitoring system is composed of “provisions on the security protection of electric power monitoring systems” (National Development and Reform Commission Order 2014 No. 14) and “the general security protection scheme of power monitoring system” (National Energy Bureau Security 2015 No. 36)[8].Referring to the requirements of the guidance scheme, the power user electric

energy data acquisition system is finally divided into four security domains and five borders by adding the marketing security access area (the security buffer area for acquisition terminals access to the master station) and the marketing production control domain (where high-voltage user cost control and load control business are deployed). The four domains/areas are level-3 domain acquisition system, communication channel area, marketing security access area and marketing production control domain. The five borders are as follows:

I1: border between marketing security access area and communication channel area

I2: border between marketing security access area and marketing production control domain

I3: border between level-3 domain acquisition system and other business systems in information Intranet

I4: border between marketing production control domain and management information area

I5: border between superior and subordinate units in information intranet

The security area of the master station is divided as shown in Figure 1.

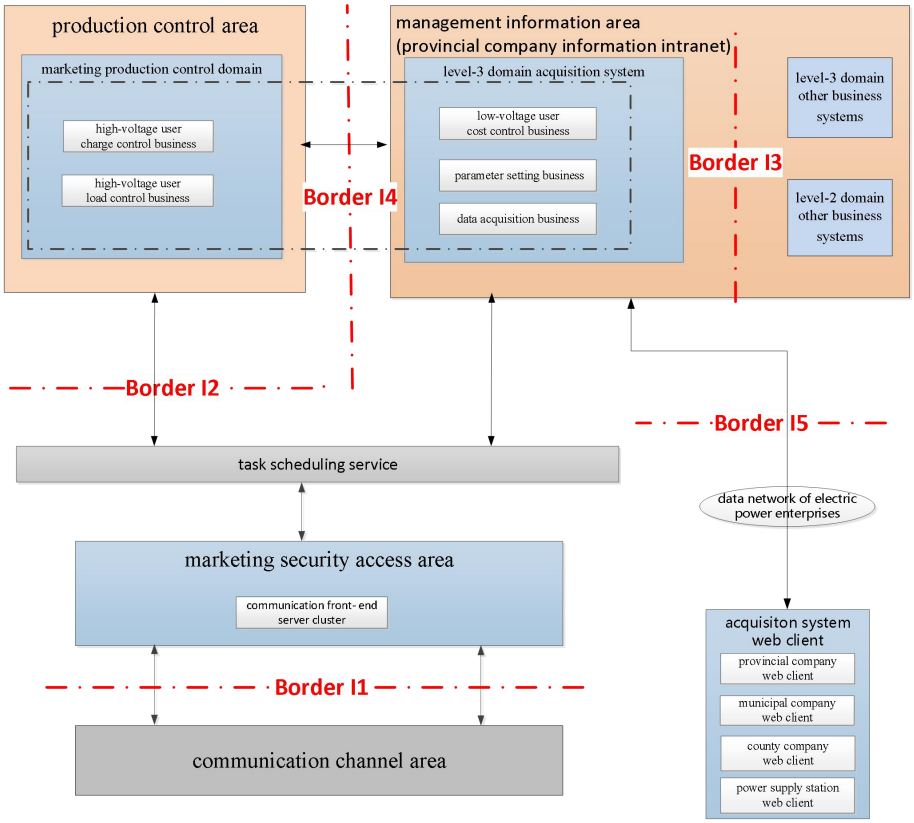

Figure 1: The borders of the master station of electric energy data acquisition system.

2.2.Border Security Risks

For each border, the existing security risks are as follows.

2.2.1. Vertical borders I1 and I2

The existing risks include: falsifying acquisition terminals access; tampering, forging, and replaying terminal uplink messages; suffering from denial of service attacks; port scanning; Trojan horses, viruses, and malicious code attacks[9-11].

The harms caused includes: access to the master station and launching subsequent attacks; affecting the development of system business; consuming system resources; obtaining system information; the system is maliciously controlled or destroyed.

2.2.2. Horizontal borders I3 and I4

The existing risk is that the data is forged or tampered.

The harm is that the sensitive data transmitted is forged or tampered, which affects the normal business development.

2.2.3. Information Intranet Vertical Border I5

The existing risks include: cross infection of Trojan horse, virus and malicious code; scattered and uncontrollable users; unauthorized access and operation.

The harms caused include: the system is maliciously controlled or destroyed; the system is operated by impersonating users.

3. Key Protection Devices and Software

3.1.Forward and Reverse Isolation Device

Forward isolation device is used for one-way data transmission from marketing production control domain to level-3 domain acquisition system or marketing security access area. It centrally receives the data sent from the marketing production control domain to the level-3 domain acquisition system or marketing security access area. After the data is processed by signature verification, content filtering, and validity checking, it is forwarded to the receiving program in the level-3 domain acquisition system or marketing security access area. In contrast, the reverse isolation device is used for one-way data transmission from the level-3 domain acquisition system or marketing security access area to the marketing production control domain.

Security isolation device do not establish a “physical path” between two networks. It extracts the application data from one side and ferries it to the other side, and then sends it to the destination through normal communication methods. Illegal information is often hidden in the format information. From the perspective of security, the format information in the ferry data should be reduced as far as possible, and the original data without any format should be the best.

3.2.Security Encryption Isolation Gateway

The security encryption isolation gateway (including type I security access gateway and information security network isolation device) is deployed in the marketing security access area. It works with the key sharing server to realize terminal key negotiation, identity authentication, data encryption and decryption, and protocol message filtering, blocking network attacks based on the security isolation project, disconnecting TCP/IP connections and other functions.

The security encryption isolation gateway is designed with a dedicated security application link layer protocol (SAL protocol for short), which encrypts and decrypts the uplink and downlink application layer data passing through the gateway. When acquisition front-end server sending the message, the original application layer protocol or data plaintext is taken as the data field of SAL protocol and sent to the security encryption isolation gateway. The gateway encrypts the plaintext into ciphertext and sends it to the communication front-end server. The communication front-end server forwards the ciphertext to the terminal, and the terminal decrypts it to data plaintext. When the terminal uploads data to the acquisition front-end server, the terminal encapsulates the original

application layer protocol or data plaintext into the SAL protocol by chip encryption, and then the communication front-end server forwards it to the security encryption isolation gateway. After the gateway decrypts, the application layer protocol or data plaintext is taken as the data field of the SAL protocol and sent to the acquisition front-end server to interpret.

3.3.Key Sharing Service System

The key sharing service system is deployed in the marketing security access area to provide key synchronization services between devices for the security encryption isolation gateway cluster, and realizes the key upload, query and synchronization by the specified protocol. It provides full life cycle security management for stored keys; implements confidentiality and integrity protection for transmitted and stored session key information of terminal; centrally manages the management configuration of the security encryption isolation gateway cluster; manages communication data messages, implements security protection with the national secret algorithm security suite; provides query and detection of the operation status of the dedicated encryption isolation gateway cluster, and the detection content includes equipment status and business status.

3.4.3A Authentication Service System

The 3A authentication service system is deployed in the marketing security access area, and its main function is to provide security access control function based on SIM card for the acquisition terminals accessing to the marketing security access area through the telecom operator's APN network, so as to prevent illegal terminals access. It supports industry standard security authentication protocol; provides account whitelist management function; supports different standard networks of mainstream operators such as Mobile, Telecom, and Unicom.

3.5.Security Authentication Gateway

The security authentication gateway is deployed in the level-3 domain acquisition system. It acts as the front-end device of web application server and forwards the user access requests by proxy. The security authentication gateway can realize dual-factor authentication based on certificate and password, role-based authority management and access control, and high-strength logging and auditing capabilities. The encryption tunnel is established between the client and the web application server based on SSL transmission layer encryption to realize the encrypted transmission of data.

4. Design and Implementation of Border Protection

In this paper, the security domain is re-divided aiming at the existing security risks and protection deficiencies in the current border protection for the master station of acquisition system. The high-voltage user cost control and load control business functions are separated from the other business functions of acquisition system and employed in marketing production control domain to improve the security protection capability. In addition, the security access area for acquisition terminals access to the master station is set up. Based on the new security domain division, by optimizing the existing security measures and security infrastructure, and comprehensively utilizing various security protection means and devices, such as firewall, network isolation, intrusion prevention, key management, encryption and decryption, security authentication, access control, a border security protection scheme for the master station of acquisition system is designed, as shown in Figure 2.

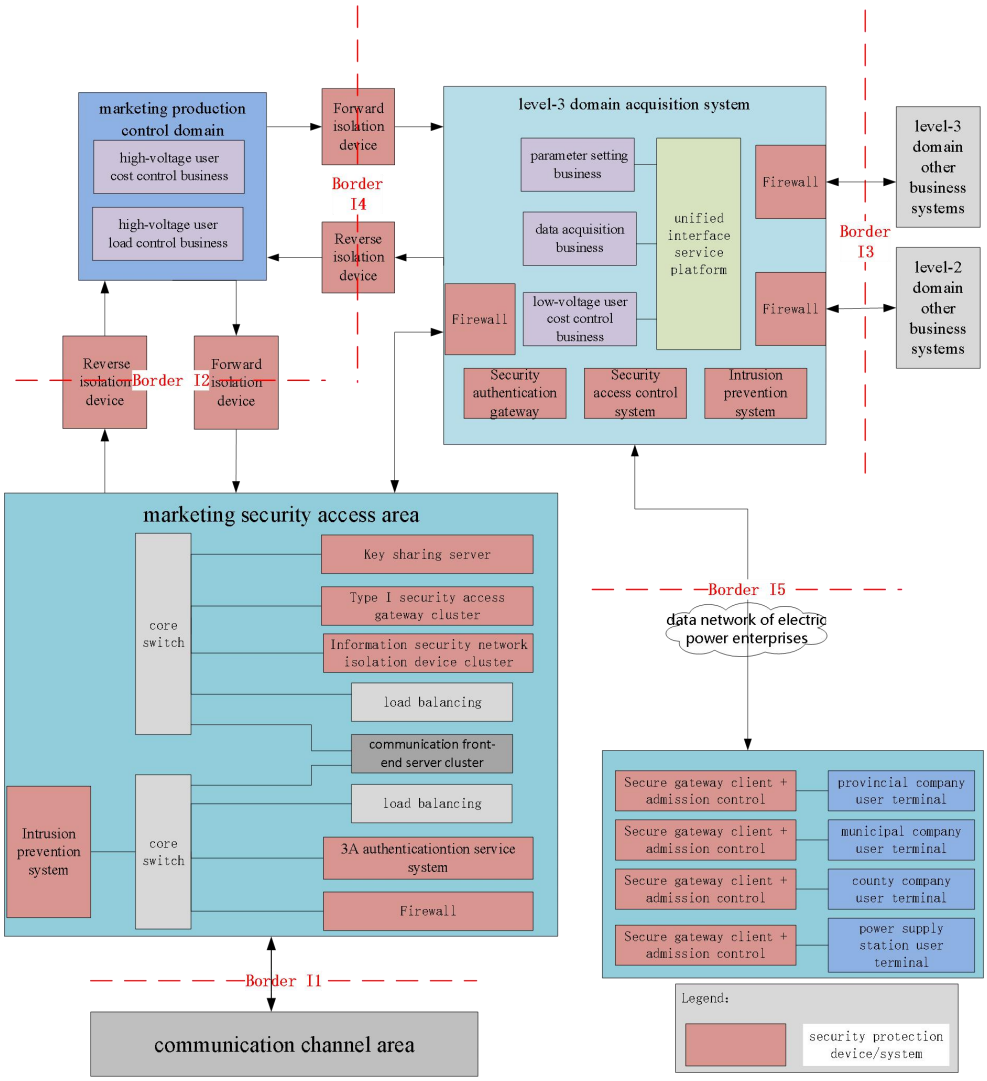

Figure 2: The overall design of border security protection for master station of electric energy data acquisition system.

4.1.Design and Implementation of Border I1 Protection

The marketing security access area, as the DMZ (Demilitarized Zone, referred to as DMZ) where the data acquisition terminals access to the master station, realizes border isolation. It performs authentication, encryption, protocol filtering and data ferrying for acquisition terminals access. Aiming at the security risks at border I1, the protection is designed as follows.

4.1.1. Firewall Configuration

Deploy firewall at the border between the marketing security access area and the communication channel area, and configure reasonable protection strategies for the firewall to limit the number of concurrent connections and control transmission priority. In the same way, deploy firewall at the border between the marketing security access area and the level-3 domain acquisition system, and configure reasonable protection strategies for the firewall.

4.1.2. 3A Authentication Server Deployment

The 3A authentication service software is deployed in the marketing security access area to perform whitelist access authentication for the SIM cards used for wireless public network communication, and only the SIM cards in whitelist are allowed to access.

4.1.3. Intrusion Detection Deployment

Deploy dedicated hardware device or software system inside of the firewall in the marketing security access area to map the data traffic of the border I1 to the switch port where the intrusion prevention system (IPS) probe is located for intrusion detection.

4.1.4. Information Security Network Isolation

Deploy information security network isolation device in the marketing security access area, realize different business support and application layer protection by encapsulating different application layer protocols, and realize protocol isolation and filtering.

4.1.5. Vertical Network Isolation

At the vertical connection between the marketing security access area and the information intranet, type I security access gateway is deployed for physical logic isolation and security isolation.

4.1.6. Protocol Filtering and Data Ferrying

It is required that the communication front-end server must be equipped with dual network cards, and the network card 1 and network card 2 are in different VLANs. The communication front-end server is responsible for maintaining the communication link with the acquisition terminals, checking the format of the data message protocol, and ferrying the data conforming to the protocol format, so as to realize the data transmission between different VLANs.

4.1.7. Inter-VLAN Access Control

Divide the intrusion prevention system, 3A authentication server, communication front-end server network card 1 into the same VLAN, and divide the information security network isolation device, type I security access gateway, and communication front-end server network card 2 into the same VLAN for physical isolation and inter-VLAN access control.

4.1.8. Dedicated Devices

3A authentication server, communication front-end server and other devices located in the marketing security access area must adopt dedicated independent physical equipment, and servers allocated in the resource pool are not allowed to be used.

4.2.Design and Implementation of Border I2 Protection

The high-voltage user cost control and load control business functions are deployed in the marketing production control domain, and the control instructions are vertically distributed from the marketing production control domain to each acquisition terminal through the marketing security access area. Aiming at the security risks at border I2, the protection is designed as follows.

4.2.1. Information Security Network Isolation

Refer to the requirements of the safety protection regulations of the power monitoring system that "the connection between the security access area and other parts of the production control area must be installed with a power horizontal one-way safety isolation device that has been tested and certified by the designated department of the state.", deploy forward and reverse isolation devices at the border of marketing production control domain and marketing security access area to achieve high-strength border isolation capability.

4.2.2. Encrypted Transmission of Key Data

Deploy control cipher machine in the marketing production control domain, and establish an encrypted protection channel between the marketing production control domain and the terminal (ESAM) at the application layer for the control data.

4.3.Design and Implementation of Border I3 Protection

Aiming at the security risks at border I3, the protection is designed as follows.

4.3.1. Firewall Configuration

Deploy dedicated firewall at the border I3, configure reasonable protection strategies to limit the number of concurrent connections and control transmission priority.

4.3.2. Intrusion Detection Deployment

Deploy intrusion prevention system at the border I3 to realize the intrusion prevention on the switch ports where the border server is located, and monitor network intrusion actions.

4.3.3. Signature Verification

Use the signature verification server to sign key data to ensure the reliability of the source data.

4.4.Design and Implementation of Border I4 Protection

Aiming at the security risks at border I4, the protection is designed as follows.

4.4.1. Horizontal Network Isolation

Refer to the requirements in the safety protection regulations of the power monitoring system that “a special horizontal one-way safety isolation device for electric power must be installed between the production control area and the management information area that has been tested and certified by the designated department of the state.”, deploy dedicated forward and reverse isolation device at the border I4 to achieve a high-strength border isolation capability.

4.4.2. Basic Network Optimization

Independent core switches are deployed in the computer room of the master station of acquisition system, and the application area is networked separately. Use security methods such as VLAN division to isolate the application area from the external systems of information intranet.

4.5.Design and Implementation of Border I5 Protection

Aiming at the security risks at border I5, the protection is designed as follows.

4.5.1. System Security Access, Authority Management and Access Control

Deploy security authentication gateway at the border I5. The users of the lower level units (including provincial companies, municipal companies, county companies and power supply stations) use the security authentication gateway client software to establish an encrypted tunnel with the security authentication gateway server. Only these users who passed the authentication can access to the master station of acquisition system. The security authentication gateway can realize role-based rights management and access control.

4.5.2. Equipment Access Control

Centrally deploy network access control system at the border of level-3 domain acquisition system, and use access technology to achieve access to designated clients. The network access control system should be able to specify the client's IP/MAC for admission and the access time, and the IP, port, device type and opening time can be temporarily opened as needed.

4.5.3. Use of Intrusion Detection

Deploy an intrusion prevention system (IPS) at the border I5 to realize intrusion prevention on the switch ports where the border servers of vertical superior and subordinate units are located.

4.5.4. Firewall Configuration

Deploy dedicated firewall at the border I5, configure reasonable protection strategies to limit the number of concurrent connections and control transmission priority.

4.5.5. Inter-VLAN Access Control

Divide the application servers, web interface servers and clients into different VLANs to perform network isolation and inter-VLAN access control.

5. Conclusion and Prospect

This paper designs and constructs a border security protection scheme for the master station of power user electric energy data acquisition system, which can comprehensively improve the border protection capability of the acquisition system, and has certain reference significance for the further planning and construction of the border security protection for the master station of power user electric energy data acquisition system in the later stage. The next step work is to conduct a comprehensive and in-depth study on the security protection of power user electric energy data acquisition system from other aspects, such as application, data, host, network, terminal, physics, security management, in combination with the business procedure and system architecture characteristics of the acquisition system, so as to meet the security protection requirements of State Grid Corporation of China.

References

[1] Ying Huan, Liu Songhua, Han Lifang, et al. Overview of power industry control system security technology. Electric Power ICT, 2018, 16(3): 56-63.

[2] He Tianling. Analysis and research on network security protection scheme in power data communication network. Electric Power ICT, 2020, 18(1): 74-79.

[3] Tong Xiaoyang, Wang Xiaoru. Inference and countermeasure presupposition of network attack in incident on Ukrainian Power Grid. Automation of Electric Power Systems, 2016, 40(7): 150-154.

[4] Cao Xiang, Hu Shaoqian, Zhang Yang, et al. Design and implementation of power universal security access zone based on dual isolation. Electric Power Engineering Technology, 2019, 38(2): 152-158.

[5] Guo Bao，Xiang Wei, Luo Liming, et al. Security access protection of power grid data acquisition terminal based on internet plus mode. Computer Applications and Software, 2018, 35(12): 32-324.

[6] Wang Xiao. Network border security situation prediction based on time-varying Markov model. Master's thesis, Nanjing University of technology, 2017.

[7] Gong Minghao, Wang Xiaoyan, Liang Jinchun. Research on border protection method of TV Station Broadcasting System based on security domain division. Proceedings of 2015 Annual Conference of China Association of Press Technicians. Hefei, China: CAPT, 2015, 172-176.

[8] Hu Zhaohui, Wang Fangli. Research on communication security technology of electric power monitoring system. Application of Electronic Technique, 2017, 43(3):21-24.

[9] Zhang Jing, Xu Xinhua, Cui Rentao. Technology and application of electricity information acquisition system of smart power grid. Beijing: China electric power press, 2012: 226-264.

[10] Zhang Shengjie, Gu Haomin, Li Zhiqi, et al. The information security risk analysis and response plan for power industry control system. Electric Power Information and Communication Technology, 2017, 15(4): 96-102.

[11] Long Zhenyue, Qian Yang, Zou Hong, et al. Threat to network information security and study on new defense technologies in power grid enterprises. Modern Electronics Technique, 2015, 38(21): 100-104.