Construction of security protection system based on online security monitoring technology of acquisition terminal

ZhiMeng Shu*, YongGuang Liu¹, HuiNan Wang², ChaoLiang Sun¹, Lin Lv³

¹, XJ Group Corporation, Xuchang City, Henan Province, 416000, China
² State Grid Shanxi Marketing Service Center, Taiyuan, Shanxi Province, 030001, China
³ State Grid Shandong Electric Power Company Gaomi Power Supply Company, Weifang, Shandong Province, 261505, China

*Corresponding author’s e-mail: shuzhimeng@xjge.sgcc.com.cn; 22045600@qq.com

Abstract. With the completion of the construction goal of "full coverage, full collection and full cost control" of the power consumption information acquisition system, the power consumption field of power grid has been fully transferred into the operation and maintenance period. In the process of security detection and sampling of the acquisition terminal, it is found that there are security risks in the field operation of the acquisition terminal, lack of online security protection processing mechanism for network risks and their own vulnerabilities, and there is a risk of being vulnerable to large-scale malicious attacks. Therefore, it is urgent to study the online security monitoring technology of the acquisition terminal and strengthen the construction of online security protection system of the acquisition terminal Design. In this paper, through the construction of the security protection system based on the online security monitoring technology of the acquisition terminal, the online security monitoring system of the acquisition terminal is built to collect and analyze the security data information of the acquisition terminal in real time, and monitor the acquisition terminal uniformly, so as to realize the security situation awareness of the acquisition terminal and the region; through the security analysis, the security risks in the operation environment of the acquisition terminal are found in time, so as to realize the security Threat identification and attack traceability, improve the level of terminal security operation protection. Through the construction of the security protection system based on the online security monitoring technology of the acquisition terminal, it can effectively support the security monitoring of all kinds of terminal equipment in the power Internet of things.

1. Introduction
As the key information infrastructure of power industry, power consumption information acquisition system should be protected. In March 2018, the company's marketing department issued the "technical scheme for safety optimization of power consumption information acquisition system", proposing to carry out transformation from the acquisition terminal, network, master station and other aspects, so as to improve the overall safety of power consumption information acquisition system[1].

As an important part of power information acquisition system, the information security of acquisition terminal is the key to the construction of power Internet of things security system. The total number of collection terminals reaches tens of millions, and there is a risk of large-scale malicious attacks. With the continuous upgrading of network attacks, relying solely on the collection terminal's own security design can not completely prevent malicious attacks, and the collection terminal has become a potential
risk point for external intrusion into the company's intranet. According to the investigation, the following risks exist in the acquisition terminal[2-3], as shown in Table 1.

Table 1. Current risks of acquisition terminal

| Risk name                                | Risk description                                                                                                                                                                                                                                                                 |
|------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Weak password login on LCD screen        | If the password is leaked or broken, the attacker can steal or tamper with the data of the acquisition terminal.                                                                                                                                                                     |
| Remote service port weak password login  | The login password of remote service port (Telnet, SSH, FTP) has weak password. If the password is broken, the attacker can access the terminal through GPRS port and Ethernet port, realize malicious control of the operating system of the acquisition terminal, steal and tamper with the data of the acquisition terminal, and upload illegal files arbitrarily. |
| Communication interface open access      | The acquisition terminal RS232, RS485, infrared port, GPRS port and Ethernet port are open to access, and the unauthorized and untrusted devices can read the terminal parameters and data information through the access interface, which has security risks.                                                  |
| Console weak password access             | At present, there are weak passwords in the login console password of the operating system of the acquisition terminal. If the password is leaked or broken, the attacker can access the console of the operating system of the acquisition terminal through RS-232 interface, maliciously control the operating system of the acquisition terminal, steal and tamper with the data of the acquisition terminal. |
| USB open access                          | The USB port of the acquisition terminal lacks the trusted authentication of the access device. The attacker can download all the files of the terminal, upload any illegal files, control the operating system of the acquisition terminal maliciously, steal and tamper with the data of the acquisition terminal by accessing the USB port. |
| Illegal SIM card access                  | At present, there is no unique binding between the acquisition terminal and the SIM card, so any SIM card can be recognized and used by the acquisition terminal. The attacker can use the security vulnerability of SIM card to access the acquisition terminal and realize the illegal intrusion and control of the acquisition terminal. |
| ESAM not open                            | In the process of using the terminal, if ESAM authentication is not turned on as required, it is easy to lead to the risk of random parameter change, data tampering and so on.                                                                                                               |
| Caused by parameter change               | The misoperation of the technical personnel of the manufacturer or the change of the terminal parameters by the attacker lead to security risks. For example, the terminal heartbeat is set to 1 second, causing network congestion.                                                                 |
| Signal leakage and interference          | Through the Trojan horse, the terminal can be set up, the terminal can be set up, the fake information can be injected, the terminal can be set up, the terminal can be dropped, and so on.                                                                                                     |
Malicious code attack

Due to the security threat caused by the vulnerability of terminal operating system or application software, it is attacked by Trojan horse, virus and junk information.

Data leakage

When the terminal is used as the server mode (Jiangsu), there is a risk of establishing a client to connect to the terminal and controlling the terminal.

2. Technical study

2.1. Functional architecture

According to the status analysis results, combined with the online security monitoring business process of the acquisition terminal, the security protection system based on the online security monitoring technology of the acquisition terminal should at least include security monitoring, situation awareness, security portrait, security analysis, security control and other functions[4], as shown in Figure 1.

(1) Safety monitoring

According to the technical requirements for safety protection and online safety monitoring of acquisition terminal, all safety incidents specified in the technical requirements shall be reported and monitored. For the terminal not upgraded, the potential security risk and security vulnerability of the terminal are found by analyzing the total data of the acquisition terminal at a regular time.

(2) Situational awareness

By analyzing, evaluating and presenting the situation of regional security and terminal security, and providing uniform display pages for users at different levels, users at all levels can realize the three-dimensional and comprehensive perception of the regional security situation from the vertical, horizontal and time dimensions.

(3) Safety portrait

The model of terminal safety portrait is established, and the terminal safety portrait is regularly carried out to realize the rolling evaluation of terminal security status. Based on the terminal safety portrait, the regional safety portrait and the manufacturer safety portrait are realized.

(4) Safety analysis

Through the full flow analysis technology, the complete security attack tracing evidence collection is realized, and the security personnel can take targeted response measures. Through clustering analysis of security events, the root cause of the security events is located, and the loopholes of terminal security
protection are found, which provides technical support for the improvement of terminal security protection.

(5) Safety control

- Terminal maintenance authorization: all maintenance operations for acquisition terminals are carried out in the authorized state. The maintenance authorization of acquisition terminal can be conducted by two ways: field operation terminal authorization and master station authorization. Authorization includes port authorization and port authorization off.
- Monitoring of dangerous terminal: the terminal with safety risk shall be monitored. In case of any abnormality, the terminal shall be operated on and off the line to realize the isolation between the terminal and the main station, so as to avoid the improper handling, which leads to more security problems.
- Work order closed-loop management: cooperate with the closed-loop system to generate and distribute the work order for safety disposal to maintenance personnel, timely check the root cause of safety risk and eliminate safety hidden dangers[5].

2.2. Overall structure

The overall architecture of security protection system based on online security monitoring technology of acquisition terminal includes data service layer, business logic layer, application service layer and interface service layer[6]. The overall architecture is shown in Figure 2.

![Figure 2. Overall structure](image)

Data service layer provides data access, data cleaning, data storage, data integration, data calculation, data analysis and other services. Data access realizes file data synchronization, security event reporting data, etc., and is closely connected with the interface service layer. Data storage includes relational data storage and massive data storage. Terminal files and other relational data are stored in relational database, and massive historical event data is stored in distributed data warehouse[7]. Real time computing technology is used for data calculation of security event monitoring, and off-line computing technology is used for other businesses with low real-time requirements.

The business logic layer realizes the logic processing of security monitoring, situation awareness, security portrait, security analysis and other businesses. Model and algorithm management of security portrait and security analysis, and timing configuration management of various analysis tasks. Security monitoring includes event monitoring based on active reporting of security events and active monitoring
based on data analysis. Situation awareness includes terminal security situation awareness and regional security situation awareness[8]. Security portrait includes label configuration management, portrait task configuration, terminal security portrait, regional security portrait and manufacturer security portrait. Security analysis includes security analysis algorithm configuration, analysis task management and so on.

Application service layer provides client oriented application functions. It includes situation awareness display, attack traceability analysis results, risk root cause analysis, dangerous terminal monitoring, terminal maintenance authorization, work order closed-loop management and other core functions.

The interface service layer realizes the interface with the user acquisition and closed-loop system. The online safety monitoring system synchronizes the file data from the user acquisition system regularly, receives and processes the safety event data transmitted by the user acquisition system through the user acquisition system issuing instructions such as on-site maintenance authorization of the acquisition terminal, pushes the processing work order to the closed-loop system, and receives the on-site authorization record of the acquisition terminal reported by the closed-loop system[9].

2.3. Technical framework

According to the requirements of State Grid new system, the system adopts sg-uap platform technology architecture to improve the flexibility, scalability, security and concurrent processing ability of the system.

The system scheme can adopt a layered architecture that separates interface control, business logic and data processing, so as to achieve loose coupling within the system, and can flexibly and quickly respond to the needs of business changes for system changes. The system runtime can be logically divided into presentation layer, service interaction layer and persistence layer. The technical architecture is shown in Figure 3.

Figure 3. Technical framework

The presentation layer mainly includes system management, event management, work order management, situation awareness, portrait management, terminal authorization, security statistics, security analysis and other system functions.

The service interaction layer includes the communication client in the running browser and the service access point running on the server. The internal service call of the system mainly supports restful,
operates the server-side resources and realizes the "representation layer state transformation". The server provides Web service support for the integration of the third-party system and the monitoring system[10].

Data persistence layer mainly provides data persistence and data access capability through MySQL and redis. Data sources include: database and memory data; data layer is composed of data mapping and data source. Data mapping completes the access package of data source, and realizes the persistence of MySQL database data objects through data persistence layer framework, mybatis. Redis, as a memory database, has high-performance read-write ability and supports data persistence. It can save the data in memory in disk, and can be loaded again for use when restarting.

2.4. Protection architecture
The protection framework system of the security protection system based on the online security monitoring technology of the acquisition terminal complies with the requirements of the national and company network security. In view of the main security risks faced by the online security monitoring system, the security protection is emphasized from the aspects of Internet boundary and channel security, business application safety function design, and business application interface interaction security. The system safety protection architecture is shown in Figure 4.

![Figure 4. Protection architecture](image)

3. Conclusion
In this paper, through the functional architecture, overall architecture, technical architecture, protection architecture four aspects of the scheme design, and build a security protection system based on the online security monitoring technology of the acquisition terminal, one is to start from the design of the acquisition terminal itself, to upgrade and reduce security vulnerabilities; the other is to build a supporting online security monitoring system to help improve the security protection of the acquisition terminal In order to reduce the existing potential risks, improve the safe operation environment of the acquisition terminal, and enhance the safety protection level of the acquisition terminal. Therefore, the construction of security protection system based on online security monitoring technology of acquisition
terminal can effectively support the security monitoring of all kinds of terminal equipment of power Internet of things.

**Acknowledgements**

Here, I would like to thank the State Grid Corporation of China for its support in the key technology “Research on the cipher application key technologies of client-side terminal based on unified cryptographic infrastructure”. (5700-202055171A-0-0-00)

**References**

[1] Shugang Yin, Zhiqi Li. (2017) Research on security protection technology based on power Internet of things. Application technology and network security, 2017(06):06-09.

[2] Xinzhong Zhao, Zilang Hou, Kangning Luo. (2018) Security protection technology based on power Internet of things. Electronic technology and software engineering, 2018(16):15-17.

[3] Jihui Zhang. (2016) Research on security protection technology based on power Internet of things. Application technology and network security, 2016(06):17-20.

[4] Tianyou Gu. (2019) Thinking of network security protection system based on ubiquitous power Internet of things. China Hi tech Zone, 2019(009):215-218.

[5] Gaofeng Deng,Wei Huang,Ru Xiong,Peng Xia. (2017) Test and Analysis on abnormal fault of power supply board of field special transformer acquisition terminal. Jiangxi electric power, 2017(041):04-07.

[6] Yong Dong,Chi Zhang,Shuiyong Ye,Wenlin Wang. (2018) Risk analysis and control of terminal information security in power enterprises. Electricity and energy, 2018(039):002-006.

[7] Chengqun Hu. (2008) Security risk analysis and Countermeasures of security monitoring and data acquisition system. Power supply and consumption, 2008(025):043-045.

[8] Huailing Shao,Erqiang Xu,Naiguai Yang. (2016) Explore the closed-loop mode of collection and measurement of on-site operation and maintenance work order. Scientist, 2016(004)009-011.

[9] Jingfeng Wang. (2018) Closed loop management of substation tasks based on mobile terminal. China's strategic emerging industries, 2018(000)018-019.

[10] Moxin Ju,Weining Tang,Fanqiang Kong. (2019) Analysis of abnormal acquisition diagnosis based on acquisition operation and maintenance closed loop management module. Jilin Electric Power, 2019(047)004-008.