Analysis and Strategy on Reliability and Security of Intelligent Electric Meter Software

Rui Wang¹, Qiujing Gong², Ke Zhen¹, Xing Zhe Hou², Min He¹ and Ling Yu Wang¹

¹ State Grid Chongqing Electric Power Company Marketing Service Center (Metrology Center), Chong Qing, China
² State Grid Chongqing Electric Power Research Institute (Chongqing Key Laboratory of Energy Internet Advanced Metrology and Measurement Technology), Chong Qing, China
*Corresponding author’s e-mail: wangru18@cq.sgcc.com.cn

Abstract. In recent years, with the rapid development of smart grid, Intelligent Electric Meter is becoming more and more popular. As an important terminal of Intelligent Electric Meter development, its reliability and security play an important role in the development of Intelligent Electric Meter. However, in practical application, Intelligent Electric Meter users and power grid have more testing methods and requirements for Intelligent Electric Meter functionality. The reliability and security of smart meter software have the following problems: the software architecture is not uniform, the software testing involves less penetration testing, and the loopholes in the software testing are not easy to find. In this paper, by analyzing the embedded software architecture of Intelligent Electric Meter, combined with penetration testing method, a set of Intelligent Electric Meter software reliability and security system is established to ensure that the reliability and security test of Intelligent Electric Meter software can be carried out more scientifically.

1. Introduction
In recent years, smart grid is interested in and promoted all over the world. As the terminal of smart grid, smart energy meter has also been promoted and applied in many countries. The intelligent energy meter software is the nerve center of the electric energy meter, and it is the important foundation to realize the functions of electric energy measurement, communication, display, event recording, data freezing storage, cost control, step price and so on. With the gradual deepening of the construction of the power consumption information acquisition system, the smart energy meter has changed from the original power metering based to the metering centered data node, which takes into account the power grid event monitoring, recording and power quality monitoring functions of the power grid. At the same time, it supports two-way communication, such as local area network and wide area network, which is the core power management unit in smart grid. In order to meet the needs of the development of smart grid, more and more requirements are put forward for the functional design of software. In addition to the basic metering, display and communication functions, it also needs to meet the functions of demand measurement, multiple rate, tariff, step price, prepayment, switch on and off control. The scale and complexity of the software have doubled, the complexity of these software function requirements will
inevitably lead to the software design process of watt hour meter becoming more and more complex, and the software code is becoming more and more huge[1].

For Intelligent Electric Meters, in addition to the traditional electrical, electromagnetic, mechanical and environmental impact on product quality, software quality has become an important factor, and gradually become one of the key indicators to distinguish the quality of products. There are the following problems in Intelligent Electric Meter software.

First, the software architecture is not unified. Software architecture is a bridge between software requirements and software design, which focuses on solving the problem of smooth transition from software system structure and requirements to realization. It is the high-level abstraction of software system and can reflect the idea of software design. However, due to the different Intelligent Electric Meter equipment, there is no unified standard for the software architecture designed, and the software testing is various, so as to become a unified system.

Second, software testing involves less penetration testing. In view of the application of Intelligent Electric Meters, the major manufacturers and power grid focus on the functional security issues, whether there are flying words, black screen, power loss and other phenomena. The modification of functions is also based on these indicators to modify the Intelligent Electric Meter software. It is seriously inadequate to consider the aspects of controlling software functions, obtaining important grid data and user information through information security.

Third, software testing vulnerabilities are not easy to find. In the actual use of Intelligent Electric Meters, intelligent Electric Meter users and power grid companies in the actual production and operation process, the problem is often functional failure, hidden in the potential information security vulnerabilities often do not produce functional failure. Its secrecy is high, but once its loopholes are successfully used, its harm and economic loss will sometimes be larger than the damage caused by functional problems[2-3].

2. Analysis of embedded software architecture of Intelligent Electric Meter

The commonly used architectures in embedded software development are as follows: macro kernel structure, hierarchical structure, micro kernel structure, C/S (Client Server), B/S (Browser/Server) structure, etc.

Macro kernel structure is also called overall structure. It regards embedded software as a set of programs (functions), regardless of application software, system software, driver, etc, each function can call any other function as required. The structure is shown in Figure 1. It is the only form of early embedded software, especially suitable for low-end embedded application development.

![Figure 1. macro kernel structure](image)

The advantage of this structure is that the modules call functions directly, and the code execution efficiency is high; the disadvantage is that if there are thousands of functions in the whole software, the complex call relationship will inevitably lead to the difficulty of maintenance. Therefore, portability and scalability are very poor[4].
Figure 2 is a conceptual hierarchical system model. This architecture is one of the most commonly used software architectures. In a hierarchical system, each layer not only provides services for the upper layer of the structure, but also calls the functions of the lower layer as a user. In some layered systems, the inner layer only interacts with the adjacent outer layer and is transparent to other layers. In fact, many embedded operating systems and embedded databases are hierarchical. Because this structure is easy to support software reuse, good portability and replaceability, simple development and maintenance. However, due to the need to provide a set of API interface functions at each level, the efficiency is low and the performance of the system is affected.

![Hierarchical system model](image)

**Figure 2. Hierarchical system model**

Microkernel structure is a common architecture of modern software. It separates most of the functions of the operating system and retains only the most core functional units, such as task scheduling, inter task communication, underlying network communication and interrupt processing interface, and time clock. Therefore, the whole kernel is very small, and the kernel tasks run in a separate address space, which is extremely fast. The microkernel structure is shown in Table 1. The early microkernel architecture is often used for small, efficient and portable operating systems. At present, microkernel mode has become a modern operating infrastructure. It can provide a "plug and play" software environment, which makes the expansion of functions more easily integrated into the core of the system[5-6].

| Table 1. Microkernel structure |
|-------------------------------|
| application                  |
| system service               |
| Task            | Object | RPC | I/O management |
| Task            | Object | RPC | I/O management |
| Microkernel     | VMM    | File| Device driver  |
| Hardware abstraction layer |       |     | The internet   |
| Hardware        |        |     |                |

C/S structure is mainly composed of client and server, as shown in Figure 3. This structure makes full use of the hardware environment at both ends and allocates the tasks to the client and server to achieve the reasonable implementation. The design of this structure can reduce the network communication cost and the server calculation.

![C/S structure](image)

**Figure 3. C/S structure**
Under the B/S structure, the user interface is completely implemented through the web browser, and the main transaction logic is implemented on the server side. The structure is shown in Figure 4.

![B/S structure](image)

**Figure 4. B/S structure**

3. **Software reliability and security test system model of Intelligent Electric Meter**

From the perspective of an attacker, this paper actively analyzes the weaknesses, defects or vulnerabilities in the metering equipment software. To detect design vulnerabilities and software defects in smart meters, this paper evaluates the impact of attacks on metering equipment, including attack modes such as spoofing, replay, tampering, and denial of service. According to the known fault model, the fault is injected into the metering equipment under the operating environment, the behavior of the tested system is analyzed, and qualitative or quantitative test results and verification results are given for its fault tolerance and easy recovery[6-8]. A complete test system is established for vulnerability penetration test. The specific functions are shown in Figure 5.

![Smart meter software reliability and safety test system](image)

**Figure 5. Smart meter software reliability and safety test system**

Intelligent Electric Meter vulnerability test library: the main function is to store specific vulnerability information collected and detected for Intelligent Electric Meters, including vulnerability number, vulnerability name, vulnerability description, vulnerability confidentiality index, vulnerability reliability index, and vulnerability availability index. Vulnerability information acquisition is divided into two parts. First, the vulnerability database is established through known vulnerability information released by well-known mobile phone websites. Second, through the daily detection of vulnerabilities found to establish a self-built vulnerability information database. For the subsequent Intelligent Electric Meter software penetration test to do knowledge reserves.

Intelligent Electric Meter penetration attack module: the existing means of vulnerability penetration is used to test the test object, the test report is imported into the system, and then the vulnerability and...
vulnerability information database are mapped, and the risk assessment value is calculated by using the confidentiality, reliability and availability indexes of vulnerability information, so as to obtain the security risk level of penetration test[9].

Intelligent electricity meter visual report generation module: through penetration test, the vulnerability penetration test visual analysis report is generated from the test object in multi dimensions. The report includes: test object, risk assessment level, confidentiality index value, reliability index value, availability index value, security analysis suggestion, etc.

4. Conclusion
In this paper, through the problems existing in the Intelligent Electric Meter software rack, it clarifies the various aspects of the problem and the importance of vulnerability penetration test. Through the analysis of the embedded software architecture of Intelligent Electric Meter, the location of the vulnerability can be found more effectively, and the subsequent design of the reliability and security test system model of the Intelligent Electric Meter software is more targeted and feasible. Finally, a set of intelligent meter software reliability and security test system model is established, which has good guiding significance and Implementation for the reliability and security test of Intelligent Electric Meter software.

References
[1] Wenjia C, Li L, Wenji Z, A method for automatic detection of LCD cycle display content of intelligent watt hour meter, 2015, Electrical measurement and instrumentation 12 64-67
[2] Bei H, Xiyang O, Xingzhe H, Quality detection method for LCD screen of electric energy meter based on image processing, 2014, Electrical measurement and instrumentation 9 25-28
[3] Jing M, Wei C, Bing Z, A new intelligent electric energy meter test card control system, 2014, Electrical measurement and instrumentation 9 17-20
[4] Wenjing W, Research on field operation management strategy of intelligent watt hour meter, 2014, Electrical measurement and instrumentation 11 23-27
[5] Shijie Z, Shilu Z, Xueming J, Research on contact resistance detection method of smart watt hour meter holder, 2013, Electrical applications 22 77-81
[6] Xiaofei F, Bo W, Yuan T, Development of reliability prediction system for electronic watt hour meters, 2015, Electrical measurement and instrumentation 52 15-19
[7] Shi P, Wu G, Tao W, G-0 vulnerability prediction model based on loss and its improvement, 2015, Telecommunication science 99-105
[8] Jiting J, Design and research of reliability model in software testing, 2014, Computer technology and development 3 110-112, 125
[9] Jingjing Y, Haiwei W, Weixin Z, Research on software reliability test of intelligent watt hour meter, 2017, Electrical measurement and instrumentation 54 7