2022 IEEE International Conference on Advances in Electrical Engineering and Computer Applications (AEECA) | 978-1-6654-8090-1/22/$31.00 ©2022 IEEE | DOI: 10.1109/AEECA55500.2022.9918968

Analysis of Network Security Protection of Smart Energy Meter

Baofeng Li
China Electric Power
Research Institute
Beijing, China
libaofeng@epri.sgcc.com.cn

Feng Zhai
China Electric Power
Research Institute
Beijing, China
zhaifeng@epri.sgcc.com.cn

Yilun Fu
China Electric Power
Research Institute
Beijing, China
fuyilun@epri.sgcc.com.cn

Bin Xu
China Electric Power
Research Institute
Beijing, China
xubin1@epri.sgcc.com.cn

***Abstract*—Design a new generation of smart power meter components, build a smart power network, implement power meter safety protection, and complete smart power meter network security protection. The new generation of smart electric energy meters mainly complete legal measurement, safety fee control, communication, control, calculation, monitoring, etc. The smart power utilization structure network consists of the master station server, front-end processor, cryptographic machine and master station to form a master station management system. Through data collection and analysis, the establishment of intelligent energy dispatching operation, provides effective energy-saving policy algorithms and strategies, and realizes energy-smart electricity use manage. The safety protection architecture of the electric energy meter is designed from the aspects of its own safety, full-scenario application safety, and safety management. Own security protection consists of hardware security protection and software security protection. The full-scene application security protection system includes four parts: boundary security, data security, password security, and security monitoring. Security management mainly provides application security management strategies and security responsibility division strategies. The construction of the intelligent electric energy meter network system lays the foundation for network security protection.**

***Keywords*—smart energy meter, smart power network, network security assurance, smart power management, safety management**

I. Introduction

As an important infrastructure to protect people's livelihood, electric energy meters, collection terminals, and other electric energy measurement equipment are the basis for the settlement of electricity and energy consumption, related to the vital interests of thousands of households, and the foundation of the development of the national economy. Their quality is directly related to the fairness and justice of energy trade settlement. It is related to the fundamental interests of the people.

The measurement accuracy and operational reliability of electric energy meters have always been the focus of attention of power grid companies. Current electric energy meters generally have general problems such as battery under voltage, non-standard wiring, and communication failure. The electric energy meter has a single function, a fixed function configuration, no software upgrade capability, and cannot support the rapid development and ever-changing business needs of the Energy Internet.

In view of the current status of the electric energy meter market, design a new generation of smart electric energy meters, adopting multi-core modular design to ensure the metering function, and enrich the configuration functions of the electric energy meters, making them an important device for the perception layer of the power Internet of Things, supporting the informatization of the power grid, Self-excited and intelligent development to meet the needs of energy Internet business.

II. Modular Design Architecture of Electric Energy Meter

The structure of the new generation of smart energy meters is mainly composed of three parts: measurement module, management module, and expansion module. The metering module is used to implement legal metering functions; the management module is used to implement functions such as security and cost control; the expansion module is for customers to implement communication, control, calculation, and monitoring on the meter according to different business scenarios. The modular design architecture of the electric energy meter is shown in Figure 1.

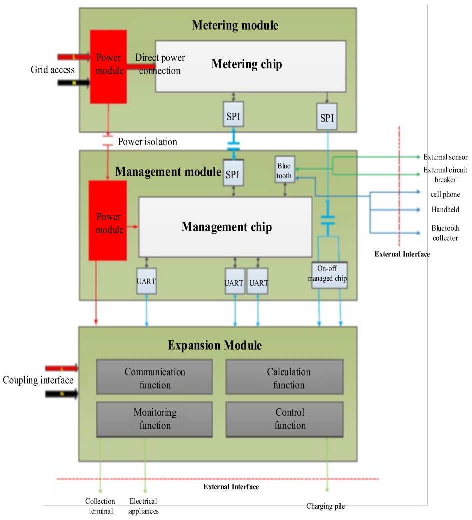

Fig. 1. Architecture diagram of modular design of electric energy meter.

The metering module is connected to 220V/50Hz AC power from the grid, and transformed into the metering chip to provide the required DC power through the power module. The metering chip has functions such as minute freezing and harmonic energy metering, and its battery can be replaced. The metering module communicates with the management module through the SPI communication interface.

The management module provides DC power to the management chip through the power conversion module. The management chip is mainly used to realize functions such as terminal temperature measurement, software upgrade, intelligent display, and active information reporting. The management module communicates with external devices such as mobile phones, handhelds, Bluetooth collectors, and concentrators via Bluetooth. Through the Bluetooth device, the management module can be connected with external sensors and circuit breakers. The management module is linked with the expansion module through the UART communication interface.

The expansion module directly interfaces with 220V AC power supply. The expansion module mainly includes four functional modules: communication function, calculation function, monitoring function and control function. And connect with the collection terminal, user electrical, charging pile, etc. through the external communication interface.

III. Smart power structure network design

The new generation of smart electric energy meters combined with the smart power structure network constitutes an informatized and intelligent energy Internet. The schematic diagram of the smart power utilization structure is shown in Figure 2.

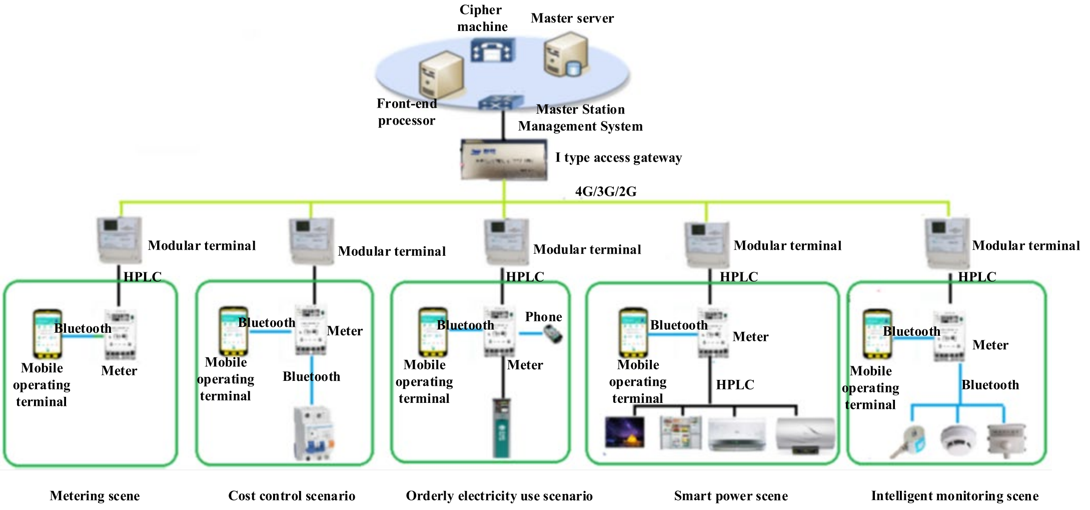

Fig. 2. Schematic diagram of smart power utilization structure.

The intelligent power structure network is composed of the master station server, front-end processor, cryptographic machine, and master station to form a master station management system. The master station management system can complete data mining, energy consumption evaluation, energy saving analysis, energy transformation and energy optimization management services. Through the diagnosis and energy audit of the collected data, we can find the energy waste links, further improve energy process management and energy saving and energy optimization dispatching energy saving, and better serve customers.

The main station management system is connected to the modular terminal through the Type I access gateway, and the modular terminal is connected to the electric energy meter through HPLC. The electric energy meter forms a metering scene, a cost control scene, an orderly electricity consumption scene, and a smart energy consumption scene by connecting different types of equipment.

The smart power utilization system establishes smart energy dispatch operation through data collection and analysis, provides effective energy-saving algorithms and strategies, and remotely controls modular terminals through 4G/3G/2G Internet to realize smart power management.

IV. Energy meter safety protection requirements

The risks faced by smart energy meters are mainly divided into the risk of attacks against the energy meters themselves and the risks of attacks against the business applications of the energy meters.

The attack risk against the electric energy meter itself mainly comes from two aspects: hardware and software. Hardware security risks mainly include the risk of the electric meter being stolen or physically damaged; the risk of illegally replacing the metering module module; the risk of illegally replacing the management module module; the risk of illegally replacing the uplink carrier communication module; the risk of illegally replacing the expansion module, etc.

Software security risks mainly include the risk of malicious code implantation; operating system vulnerabilities; application unauthorized access risks; operating system and application management risks.

The attack risk for the business application of electric energy meter mainly comes from two aspects: communication and uncontrolled device access.

The external communication method of the electric energy meter is Bluetooth and carrier wave, so it will face communication security risks during the communication process. Including the risk of the communication channel being occupied or blocked; the risk of data eavesdropping, forgery, and tampering; the security risk of fraudulent use of operating authority; the risk of replay attacks; the risk of loopholes or backdoors in the Bluetooth chip.

The access risk points of uncontrolled equipment include the transmission of wrong information to the electric energy meter to induce the electric energy meter or the main station system to make wrong decisions, causing power outages of customers; the transmission of malicious codes and viruses to the main station system through the electric energy meter, causing the Station failure, etc.

According to the self-attack risk and business application attack risk faced by smart energy meters, the goal of a new generation of smart energy meter security protection schemes is proposed. Resist the attacks and illegal operations of the electric energy meter by hackers and malicious codes in various ways, prevent the system from being paralyzed and out of control, prevent the loss of business data, and prevent the leakage of sensitive information. Ensure the confidentiality, integrity and availability of business data, and meet the requirements of relevant standards and regulations.

V. Safety protection measures for electric energy meters

Combining the safety wind and safety protection goals faced by electric energy meters, the design focuses on its own safety, application safety in all scenarios, and safety management. The overall protection structure of the energy meter safety protection measures is shown in Figure 3.

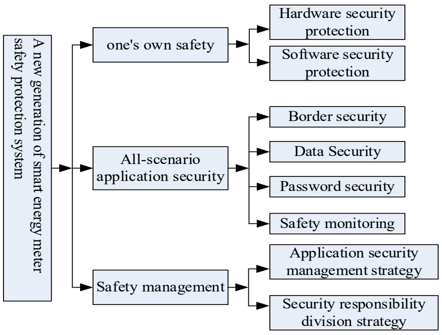
A new generation of smart energy meter safety protection system
one's own safety
Hardware security protection
Software security protection
All-scenario application security
Border security
Data Security
Password security
Safety monitoring
Safety management
Application security management strategy
Security responsibility division strategy

Fig. 3. Overall protection structure of energy meter safety protection measures.

The energy meter safety protection system designed according to the attack risk of the electric energy meter itself and the attack risk of business applications includes two major protections: its own safety and full-scenario application safety, and a safety management part is added. The security management module mainly provides application security management strategies and security responsibility division strategies.

A. Self-safety protection

Since the attack risk of the electric energy meter itself mainly comes from two aspects, hardware and software, its own security protection also includes hardware security protection and software security protection.

1) Hardware security protection

The hardware security protection mainly adopts the electronic seal mode, and different modules are equipped with different security chips to prevent the electric energy meter from being damaged and the modules from being illegally replaced.

Security chip protection means that the smart electric energy meter embeds hardware ESAM security chips or security algorithm modules with different costs and different algorithms in different modules. In this way, the identity authentication, data encryption and decryption, and integrity verification required for the security of various businesses are realized, to ensure legal access to the electric energy meter, and to protect the core data of the intelligent electric energy meter from being stolen and tampered with. The types of security chips and the corresponding cryptographic algorithms are shown in Table I.

TABLE I. Security chip type and corresponding cryptographic algorithm table

Number	Module	Chip type	Cryptographic algorithm
1	Metering module	Low-cost chip	SM1
2	Management module	High performance core	SM1/2/3/4
3	Carrier Module	--	--
4	Expansion module (A)	Low-cost chip	SM1
5	Expansion module (B)	Security algorithm	SM2/3/4

The electronic seal adopts RFID technology and is embedded with SM7 encryption algorithm dedicated to the National Cryptography Administration. Electronic seal protection can realize the safe storage of data information, with self-locking, tamper-proof, and anti-counterfeiting functions. It is used in the factory, verification, and on-site installation and maintenance of electric energy meters to prevent unauthorized persons from illegally opening electric energy metering devices and related equipment. It is a special identification object with legal effect, which can effectively screen out the electric energy meter whose seal has been damaged.

In view of the risk of illegal replacement of each module, the pairing and binding between modules is realized based on cryptographic technology, illegal modules are detected and shielded in time, and the credible identity of the meter itself is constructed together. The module replacement protection strategy mainly includes the pairing and binding of the metering module and the management module, and the pairing of the expansion module and the management module.

2) Software security protection

Software security protection mainly introduces the operating system through the management module to protect the operating system itself, application programs, and interface hardware.

The software protection scheme mainly starts from the reinforcement of the operating system of the smart energy meter, completes the security management and control of applications and interfaces, and prevents attacks on the software system of the energy meter. Software security protection includes operating system security management, application security management, and interface internal management measures.

Operating system security management includes code security management, startup security management, operation security management, upgrade security management, and authority management, six major parts of log management.

(1) Code security management

Code security management is used to strengthen the security management of the source code of the operating system.

(2) Start safety management

Before the operating system is started, the security chip verifies the integrity of the operating system's programs to prevent the operating system from being implanted with malicious code.

(3) Operational safety management

When the operating system is running, the security chip periodically checks the core data of the operating system to ensure that key data is not tampered with, and the operating system is safe and effective.

(4) Upgrade safety management

The operating system upgrade management is realized based on the security chip. The management unit encrypts and signs the upgrade program, and finally sends it to the electric energy meter.

(5) Authority management

The application can only access the underlying device through a standard interface. The operating system realizes the control of the application program through the permission setting, and avoids the unauthorized operation of the application program.

(6) Log management

The operating system records the operations of application programs on key equipment, such as controlling the opening of circuit breakers, and records related logs for easy auditing.

Application security management includes three parts: startup security management, operation security management, and program security management. The protection methods and functions of each part are shown in Figure 4.

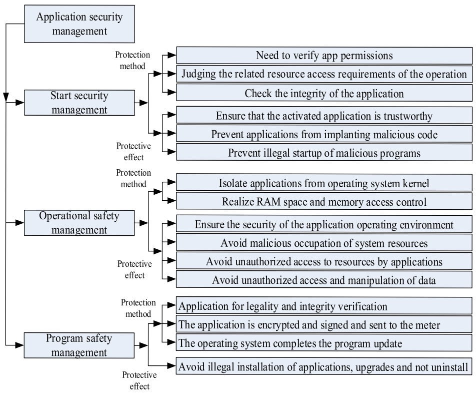
Application security management
Start security management
Protection method
Need to verify app permissions
Judging the related resource access requirements of the operation
Check the integrity of the application
Ensure that the activated application is trustworthy
Prevent applications from implanting malicious code
Prevent illegal startup of malicious programs
Protective effect
Protection method
Operational safety management
Isolate applications from operating system kernel
Realize RAM space and memory access control
Ensure the security of the application operating environment
Avoid malicious occupation of system resources
Avoid unauthorized access to resources by applications
Avoid unauthorized access and manipulation of data
Protective effect
Protection method
Program safety management
Application for legality and integrity verification
The application is encrypted and signed and sent to the meter
The operating system completes the program update
Avoid illegal installation of applications, upgrades and not uninstall
Protective effect

Fig. 4. Application security management protection method and protection function diagram.

Implement interface management measures for the internal and external interfaces of the smart energy meter. Authorization is required to open the internal interface of the smart energy meter, and the unauthorized interface is closed. Control the access rights of the application and prevent illegal operations on the interface. Use a protocol analyzer to filter illegal messages.

The external interface of the smart energy meter is uniformly named and managed by the operating system to the equipment management layer. Based on the permission access attribute of the application, the access permission at runtime is controlled. The device management layer will compare permissions and block access to applications without permissions.

B. Application security protection in all scenarios

The full-scenario application security protection system is mainly aimed at the attack risk of the electric energy meter business application. The protection system includes four parts: boundary security, data security, password security, and security monitoring.

1) Border security protection

The security protection between the metering module, the management module, and the extension module constitutes the boundary security protection, and the security chip is used to securely reinforce the Bluetooth and HPLC communication. The smart electric energy meter is connected with mobile phones, mobile operating terminals, circuit breakers, and sensors through Bluetooth, and connected with modular terminals/master stations and smart home appliances through HPLC. The boundary of the smart energy meter mainly includes the boundary between the northbound and modular terminals and the main station system, and the southbound boundary with sensing equipment, circuit breakers, mobile operating terminals, mobile phones, charging piles, smart home appliances and other equipment. The electric energy meter repackages the legal business data, and uses the session key negotiated with the master station for encryption and integrity protection to complete the boundary security protection function of the smart electric energy meter.

The Bluetooth boundary security protection is to first perform Bluetooth pairing at the beginning of communication, the pairing is successful for user identity authentication, data integrity protection in the form of data encryption, and then data transmission. The blue tooth border security protection scheme is shown in Table II.

TABLE II. BLUETOOTH BORDER SECURITY PROTECTION TABLE

Protection plan	Description	cell phone	breaker	sensor	equipment
Bluetooth pairing	QR code	√	√	√	√
Authentication	SM2	√			
	SM4		√	√	
	SM1				√
data encryption	SM4	√	√	√	
	SM1				√
Integrity protection	SM4		√	√	
	SM1				√
	SM3	√			

HPLC boundary communication also requires data encryption and transmission after identity authentication for boundary security protection. Before the uncontrolled device of the smart electric energy meter is connected, it is necessary to embed a tested security chip or a password soft module, and perform identity authentication when it is connected, and data can be exchanged after passing the authentication.

After the electric energy meter receives the equipment business data, it uses the session key negotiated with it to verify and decrypt the data, and at the same time filter and analyze the information interacted with the external equipment. HPLC boundary security protection is shown in Table III.

TABLE III. HPLC BORDER SECURITY PROTECTION TABLE

Protection plan	Description	Smart Appliances	Charging pile	Modular terminal
Authentication	SM2	√	√	√
data encryption	SM4	√	√	√
Integrity protection	SM4	√	√	√

The boundary protection method is to use the electric energy meter to repackage the legal business data, and use the session key negotiated by the master station for encryption and integrity protection.

2) Data security protection

The data collected and processed by the smart electric energy meter can be encrypted and integrity protected by the security chip for data storage and transmission to enhance data security. Data security protection includes data storage security and data transmission security.

Data storage security means that the new generation of smart electric energy meters use ESAM chips to encrypt important data and store them. For particularly important data, they are directly stored in the ESAM chip, and the symmetric cryptographic algorithm is used to calculate the data MAC to protect the integrity of the stored data.

Data transmission security refers to the use of SM1 or SM4 algorithms to encrypt data during data transmission in the new generation of smart energy meters, and the use of SM1/3/4 algorithms to protect the integrity of the transmitted data, depending on the transmission channel.

3) Password security protection

The control of the electric energy meter needs to be connected with the login control system, so it is necessary to increase the password protection function. The SM1, SM2, SM3, SM4 based on national secrets are used to realize the functions of identity authentication, transmission encryption, integrity verification and other functions to realize password protection.

TABLE IV. PASSWORD SECURITY PROTECTION TABLE

Cryptographic algorithm	type	Key length	application
SM1	Symmetric Algorithm	128 bit	Data encryption
SM2	Asymmetric algorithm	128 bit	Identification
SM3	Hash algorithm	256 bit	Digital signature and verification
SM4	Symmetric Algorithm	128 bit	Data encryption

There are four algorithms used in smart energy meters: National Secret SM1, SM2, SM3, SM4, and different algorithms are used in different scenarios. The designed smart energy meter password security protection table is shown in Table IV.

4) Safety monitoring management

Provide safety monitoring capabilities from the software and hardware of the electric energy meter and the master station system. The security management of smart energy meters includes application security management strategies and security responsibility division strategies, as shown in Figure 5.

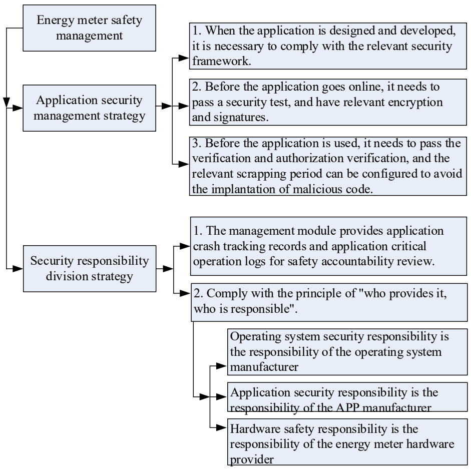
Energy meter safety management
Application security management strategy
1. When the application is designed and developed, it is necessary to comply with the relevant security framework.
2. Before the application goes online, it needs to pass a security test, and have relevant encryption and signatures.
3. Before the application is used, it needs to pass the verification and authorization verification, and the relevant scrapping period can be configured to avoid the implantation of malicious code.
Security responsibility division strategy
1. The management module provides application crash tracking records and application critical operation logs for safety accountability review.
2. Comply with the principle of "who provides it, who is responsible".
Operating system security responsibility is the responsibility of the operating system manufacturer
Application security responsibility is the responsibility of the APP manufacturer
Hardware safety responsibility is the responsibility of the energy meter hardware provider

Fig. 5. Safety monitoring management strategy diagram.

The application security management strategy has a complete application life cycle security management strategy, and the security responsibility division strategy has a clear principle of responsibility division.

VI. CONCLUSION

The measurement accuracy, operational reliability and safety of the electric energy meter are the key to the design of a new generation of smart electric energy meters. And according to its own attack risk and business application attack risk, the safety protection system of the electric energy meter is designed, and safety management is added to realize a safe and intelligent electric energy meter network system.

ACKNOWLEDGMENT

This article is supported by the Science and Technology Project of the State Grid Corporation of China (5400-202155393A-0-0-00).

REFERENCES

[1] Liang Jie. Research on data encryption system of electric energy meter based on elliptic curve encryption [J]. Industrial Instrumentation and Automation, 2018, 22(5): 112-114.

[2] Liang Jie, Li Gang. Research on the function test of the automatic function test system of the metering terminal [J]. Electrical Application, 2017, 36(3): 83-87.

[3] Yan Mei. Research on SSH secure remote login based on Linux platform [J]. Network Security Technology and Application, 2018(9): 17-19.

[4] Li Chengyu, Qi Yudong, Wang Xiaohong, et al. DDoS offensive and defensive confrontation evaluation based on offensive and defensive games and stochastic Petri nets[J]. Computer System Applications, 2019, 28(1): 27-33.

[5] Li Chengyu, Qi Yudong, Wang Xiaohong, et al. DDoS offensive and defensive confrontation evaluation based on offensive and defensive games and stochastic Petri nets[J]. Computer System Applications, 2019, 28(1): 27-33.

[6] Long Guishan, Liu Lei. Research on the fully automated verification and intelligent storage integrated system of electric energy meters[J]. Guizhou Electric Power Technology. 2013, 15(7), 31-35.