# Research on the security system of power system automation network

Song Li[1], Cong Peixian[2], Cai Dongfei[1], Zhang Shiyu[1]

1,State Grid Liaoyang Electric Power Supply Company, Liaoning, China

2,State Grid Liaoning Electric Power Company

**Keywords:** measurement automation system; safe protection system; border security protection; communication channel; terminal equipment

**Abstract.** In the light of the characteristics of electricity measurement automation system in Power Company, the safe protection system is researched from the three perspectives:master station,communication channel and terminal equipment. As for master station,the safe protection system is formulated in accordance with four levels of safety protective measures-boundary, network, host and application. As for communication channel, safe protection system is made in accordance with the scheduling data networks and wireless public network. As for measurement terminal equipment,a set of hardware encryption security mechanism is established.

## 1 Introduction

Measurement automation system widely used in demand side management, electricity energy settlement, sting monitoring and power supply service and application benefit is apparent. In order to meet the requirements of safety protection for the two system, protect the safety of the system, ensure the safety of the load control, reduce the complexity and cost of the safety protection, and try to meet the needs of the system production and operation, need to study the safety protection scheme of the measurement automation system, and put forward the safety protection system[1].

System security is generally in the power supply bureau of information management in the III area or control zone II area under the unified management. But there are some problems to be solved in the current measurement automation system: the master station of the system security is not comprehensive[2]; The remote maintenance are factory direct inward dialing system maintenance phenomenon, does not meet the safe dialing mechanism; The public side of the lack of effective means of security, it is not practical to the remote control and load management, and lack the security of the prepayment means[3].

## 2 system master station security

### 2.1 boundary protection

Border security is concerned with how to detect and control the data flow in and out of the border. Border security measures can be carried out from the following aspects.

(1) The system information management in large area (III) and third party border security

This part mainly carries on the information network security system protection, the relevant security measures mainly include the following contents.

(2) information security at the border and outside the network

Information inside and outside the network boundary should adopt special logical isolation device for security protection, logical isolation device can from the underlying communication protocol between internal and external network information flow isolation control and only allows to determine the business data flow through, thus preventing security incidents by diffusion network to network or blocked from information network or the Internet of information network server attack[5].

(3)The security of the information network and the lower border security

Information within the network vertically and lower unit boundaries, including the provincial companies and companies or directly under the units, and the network boundary between the city

 

and county units, in addition, if there is information transmission between flat level units, but also in accordance with the security of such boundaries. The main contents of the relevant protection are as follows.

(4) The security at the border between the horizontal and inter domain boundaries

The security protection of the lateral domain boundaries is a security measure to protect the communication data stream transmission. The appropriate security measures should be taken to ensure the security of the exchange data. The main contents are as follows.Network access control. Using firewall or virtual firewall or VLAN access control as a security measure, it is only allowed to open and secure network communications between the network access control devices, and to protect the security of information network.

(5) The system control area (II) and security zone (I) boundary

There is no direct data interface in the system of measurement automation system and the I system, and the system platform is located in the unified security of the dispatching data network. Therefore, this system directly follows the security scheme of the dispatching data network, and is not deployed separately.

(6) The system control area (II) of the upper and lower unit boundaries

The measurement automation system and the vertical lower level system are connected by the III system, and there is no connection between the II and the. Therefore, it is not to do the security deployment.

**2.2 The security of the network environment**

The network environment includes the security device, network infrastructure, and network infrastructure which are introduced by the network to provide the route, the exchange equipment and the safety protection system. The specific content of the network environment security has the following several aspects.

(1) The secure access control

This can ensure that the security area is not unauthorized access, to ensure that the access security measures are not required to access the desktop host can not access the network[9].

(2) The equipment safety management

Using the security protocol for remote management, only the user name / password authentication through the authentication of the user to configure the device, persons who do not have permission are not operate the equipment.

(3) The equipment safety reinforcement

This part mainly through the software for all network equipment and routers to reinforce, guarantee the network equipment configuration and its transmission number according to the security.

(3) The security vulnerability scanning

By using the vulnerability scanning system, the scanning strategy for all network equipment configuration can be realized, and the function of the network equipment and operating system, database and application software can be realized effectively.

(4) The security event audit

Using log management analysis system, it is configured to collect core network, security device event R and event analysis in Syslog or Snmp.

(5) The network intrusion detection

By the intrusion detection console for centralized management of Sensor IDS, it can effectively detect viruses, worms, hacker attacks, malicious code attacks, denial of service attacks and other threats, and in the event of an alarm.

**2.3 The host system security**

Host system security includes the security of the server and desktop terminal. The server comprises a business application server, a network server, a WEB server, a file and a communication, etc. the desktop terminal comprises a desktop computer and a notebook computer as a terminal user workstation.

### 2.4 application security

Application of security protection, including the protection of the main station application system itself, the user interface security, system data interface between the security, the security of the system data interface. The goal of security protection is to ensure the security of the application system by taking the identity authentication, access control and other security measures to ensure the security of the application system.

## 3 communication channel security

### 3.1 scheduling data network

In the internal network can take some necessary safety measures, such as in the access layer implementation access and flow control, disable the default password login, avoid using a default route, using security enhanced SNMP V3 version of the network management system, internal network division different segments, in key points of internal network set vulnerability scanning, intrusion monitoring safety facilities, the establishment of network virus protection facilities. At the same time, we must adopt strict access control measures to ensure that the access of the business system is credible, and only the authorized nodes can access the data network, and use the data network to carry on the wide area network communication.

### 3.2 wireless public network channel

For dedicated APN, power companies can build 1 Radius authentication server, the power company for the terminal to assign the account and password. When the terminal connect enterprise network, through the Radius certification and confirm the identity of the user, to assign IP addresses. Typical wireless public network channel such as China mobile gprs APN line. In this scheme, the data communication between GPRS terminal equipment and the main station acquisition server /Radius authentication server not through the Internet network, data communication security. Therefore, in wireless public network channel construction should be through the line makes the master computer system radius authentication server and GPRS network GGSN is connected and capture server inside the enterprise network, the only terminal can access to the collection server. Also, to access the network resources of the GPRS terminal, must be the first of its Radius server authentication. So when the authentication is passed, the collection server establishes a connection with the GPRS terminal, so that the data can be collected or downloaded.

## 4 The terminal equipment security encryption

### 4.1 Encryption mode

The application layer encryption system can be used to combine the symmetric key algorithm and asymmetric key algorithm. The symmetric key is fast, which is mainly used in data encryption and decryption; the asymmetric key algorithm is fast and easy to be used, which is mainly applied to the distribution of key and the issuing of broadcast commands. Application layer of the data encryption and decryption of the implementation should be used in the way of hardware encryption, do not allow the use of encryption and decryption software. The proposed algorithm or 3DES algorithm is adopted.

### 4.2 encryption mechanism

The master station system in the measurement automation system should be equipped with the password machine equipment which has the State Password Administration Bureau. Front machine through the application layer function code (AFN) to determine what data needs to be encrypted, the need to add password encryption, password encryption and encrypted data to the length of the encrypted data and the encrypted data packet, and then the encrypted data will be packaged, the data will be packaged and sent without a password. Figure 1 as the main station system packet encryption process.

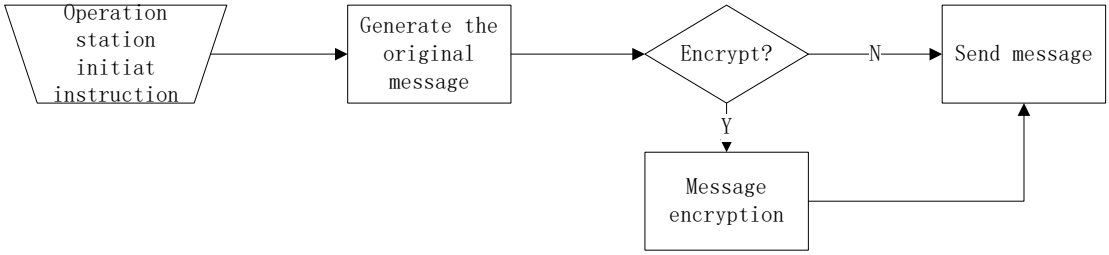


Fig. 1 The message encryption process of master station system

The process of encryption security module: plaintext data sent safe mode block, the security module of ciphertext + MAC operation, returns the ciphertext + MAC packet. The decryption process of the security module: the data packets sent to the +MAC security module, the security module is the first MAC verification, verification of the encrypted data to decrypt the encrypted data, return the effective data and data length.

The encryption and decryption process of the asymmetric key algorithm is shown in Figure 2.

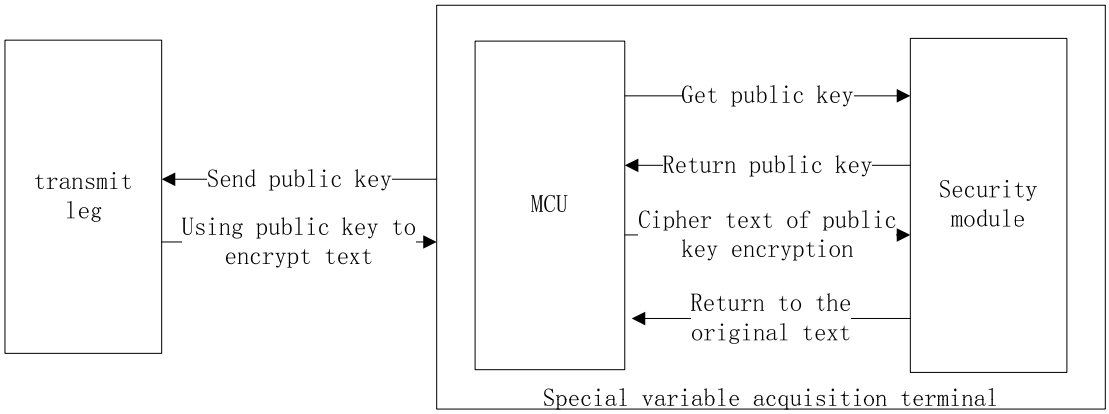


Figure 2 The data encryption and decryption of the asymmetric key algorithm

Load management terminal MCU first gets the public key from the security module, and sends the public key to the sender. The sender by the special transformer data acquisition terminal of the public key to encrypt the plaintext data to be passed, and the encrypted data is sent to the load management terminal. Load management terminal MCU will receive the encrypted message sent to the security module, the security module uses the corresponding private key to decrypt the original text, and sends the original text to the load management terminal MCU.

**4.3 encryption algorithm**

The commonly used algorithms including non symmetric encryption algorithm and symmetric encryption algorithm, hash algorithm.SM1, SM7, SF33, AES and SM7, which are the products of the CPU are non - contact logic encryption card, the security is high. Besides, the security of the, DES, and the key length is 48 bits Mifare. Symmetric cryptography algorithm is only one key, encryption and decryption speed, usually used for data encryption.

Non symmetric cryptography algorithm generally choose the key length is 192, 256, 384 SM2 bit, the key length 192, 256, 384 ECC bit, as well as the key length is 1024 ~ 2048 RSA bit. The security of this algorithm is higher, the product form is CPU card, there are two key, the encryption and decryption speed is slow, and it is usually used for key transfer and digital signature.

## 5 Conclusion

This paper presents the technical requirements of the safety protection system of the measurement automation system in compliance with the two safety of the Liaoyang Grid Co. In master systems, in accordance with the border security measures, network security prevention nursing measures, host security protection measures, application security measures such as four level to develop security system; in the communication system, full foot from the electric power

network and wireless public network communication security; in the terminal equipment, building hardware encryption security mechanism.

## Reference


[1]. Zungeru A M, Kolo J G, Olumide I. A Simple and Reliable Touch Sensitive Security System[J]. International Journal of Network Security & Its Applications, 2012, 4(5).

[2]. Novak T, Treytl A. Functional safety and system security in automation systems[C]// Emerging Technologies and Factory Automation, 2008. ETFA 2008. IEEE International Conference on. IEEE, 2008:311-318.

[3]. Rashid M T A, Yussof S, Yusoff Y, et al. A review of security attacks on IEC61850 substation automation system network[C]// Information Technology and Multimedia (ICIMU), 2014 International Conference on. IEEE, 2014.

[4]. A. Yousefi, T.T. Nguyen, H. Zareipour, O.P. Malik. Congestion management using demand response and FACTS devices. Electr Power Energy Syst, 37 (2012), pp. 78–85.

[5]. Qin Wang, James D. McCalley, Wanning Li. Voltage instability performance of risk-based security constrained optimal power flow. Electric Power Syst Res, 116 (2014), pp. 45–53