Study of information security and protection in integrative design of power systems

Xiaohui Xu[1, a], Ruixiang Fan[2] , Benren Pan[2], Jianbo Xin[2], Danna Wang[3]

[1]China Electric Power Research Institute, Nanjing 210003, China;

[2] Jiangxi Electric Power Research Institute, NanChang 330096, China.

[3] College of Energy and Electrical Engineering, Hohai University, Nanjing 210098, China

[a]57317693@qq.com

Keywords: power systems, integrative design, information security and protection

Abstract. The information security is very important for the secure, stable, economic and superior operation of power system. In the paper, the integrative power system and its features are introduced. The main contents of the integrative information security are explained, including secrecy, integrality and effectiveness. The security techniques such as fire wall, virtual network, authentication center an intrusion detection system are illustrated. The design principle and security strategy of integrative information security and protection are discussed. The proposed scheme is applied in a real power network automation system. And it is verified its effectiveness.

1. Introduction

Integrative power system is a general term for automation system, which include power network dispatching automation system, substation automation system, distribution network automation system, and water dispatching automation system, hydropower cascade dispatching automation system, electric power meter system, and assistant control system for real time electricity market and so on. It has the characteristics of reliability, security, integrality, consistency, timeliness, and so on [1].

2. Integrative Design of Power Systems

2.1 The security of integrative power system.

The security of integrative power system has become an important part of the production, operation and management of electric power enterprises. Combined with the characteristics of electric power industry, to protect the safety of the information, it not only need to implement information security protection, but also need to pay attention to improve the system ability of intrusion detection, the system event reaction ability and the ability to recover quickly after system damage. In addition to encryption[2], identity authentication, access control [3], firewall [4], security routing and other security technology, but also to emphasize the life cycle of defense and recovery throughout the whole information system. The information security of electric power automation system integration is to protection system of information and computing resource will not be unauthorized access and tampering and denial of service attacks, prevent viral invasion, hacking, incorrectly operation of a threat to the system.

2.2 Several kinds of security technology used in design.

There are a lot of popular security products, such as firewall, virtual private network(VPN), the center of authentication(CA) and intrusion detection system[5](IDS), which have their own characteristics. They can be used in Electric power automation network of different network levels and different security level.

(1) Firewall

Firewall is a kind of network security component which is old and has much room to play. It is a barrier between enterprise network and unsafe network. It can prevent illegal access to information

resources. It can use firewall to prevent patent information Illegal output from the company's network. At present, most of the firewall system refers to the hardware firewall, which is composed of the firewall hardware card and the firewall policy server software. At present, most of the firewall system refers to the hardware firewall, which is composed of the firewall hardware card and the firewall policy server software. When the application is required, the hardware card is installed on the server and workstation, and the corresponding firewall policy server software is installed on the server. It configures and manages the firewall in the entire network system through this policy server software. Firewall is suitable for the single network which relatively independent, the way of interconnecting the external network is limited, and the service type are relatively concentrated. It can effectively protect the local area network.

(2)Virtual private network

VPN is a security channel using data transmission capacity of public infrastructure based on public network, with the implementation of security technology and means, which can provide a safe, reliable and controllable secure data communication channel. Specifically, VPN uses the unreliable public Internet as an information transmission medium. To realize the important information security transmission through the additional security tunnel, user authentication and access control technology to achieve a similar security performance with the private network. By introducing VPN into power system, it not only can greatly reduce the power network production input, but also can get rid of some of the heavy network upgrade and maintenance workload. Under the support of VPN, the power network scalability is greatly improved. And it can flexibly adjust the coordination among various departments of power system, provide efficient network support for the power system departments to participate in the handling of some unexpected events, reduce the cost of coordination of office. Tunnel technology is the core of VPN, which is a kind of code based on network layer protocol, which is used to ensure the establishment and removal of data transmission tunnel between two points or two ends. The realization of VPN depends on the network equipment and the control software on the curing network equipment. Now the core device of exchange VPN is VPN switch. It can make interview lead directly to the corresponding tunnel terminal by using tunnel switching, so tha different network users can enter the different segments.

(3) Intrusion detection system IDS

Intrusion detection is a kind of network technology, which is used to detect any damage or attempt to damage the confidentiality, integrity or availability of System. It is a new and rapidly developing field. IDS check the specific attack mode, system configuration, system vulnerabilities, flawed version and system or user behavior patterns and monitor activities related to safety through real-time detection. IDS is composed of network detection agent and data management server. The network detection agent is running on a dedicated host, which monitors all packets flowing through the network and sends the information to the data management server when discovering being attacked. At the same time, the database on the server records information.

3. Design and Application of Integrated Information Security Protection System

3.1 The principle of design.

As the power system integrated the System of Control And Data Acquisition (SCADA), Power System Application Software (PAS), Dispatching Management Information System(DMIS), Tele-Meter Reading System(TMR) and other automation system. It not only include the power grid running real-time control system, power marketing system, but also management information system which support for enterprise management, management, operation. Each application system is different from the requirements of real time and security of data. Integrated design of electric power system must comply with the following principles.

a. All the connections of the real-time control system must be determined to ensure the security of real-time monitoring system. In order to strengthen the real-time control system ,it remove unnecessary connection, consolidate and strengthen the connection reserved of any real-time control system in the network, remove and cancel unnecessary services .

b. Does not rely on a protocol to protect system security. Some SCADA systems use factory specific protocols for communication; obviously system security depends on these protocols. It is obvious that system security depends on these protocols. By this, it cannot rely on the set protection system which factory default. In addition, it also requires manufacturers to report any back door which is likely to threat to the security of system and provide the corresponding protection measures.

c. The characteristics of the execution system provided by the seller of the equipment and system. At present, most SCADA systems do not have any security features. So the seller needs to provide security characteristics in the form of product patches or upgrades, and to set up these characteristics to achieve the maximum system security level.

d. By the realization of the internal and external IDS, it achieve the full day of 24 hours of emergency monitoring. To effectively respond to network intrusion, it is necessary to establish a kind of intrusion detection strategies (including an alert network administrator for a response to an internal or external malicious behavior). The intrusion detection system can be built up by a pager.

e. A physical security review is introduced to assess the safety of all access system networks through evaluate their remote locations; perform power monitoring system equipment and network, and any other technical review of connected network to determine the security relationship involved.

System operation strategy of the whole system should be set up to interactive execute with the strategy of firewall, anti-virus software, Internet Protocol security, intrusion detection and other protective strategies.

With the characteristics and safety level of each application system in electric power system and based on the above design principles, we explore the system security mainly from the design of system architecture and safety management process and policy.

3.2 System design.

According to the different characteristics and safety level of power system, the security of the system is required to improve by means of security grouping. The security groups are grouped according to the different security levels of the system, as shown in table I.

Tab.1 Security group of power system

Security group	Part of system functions	Data real-time requirements	Corresponding production control area
Group I	Part of SCADA	Efficiency	Face the production of real time control area
Group Ⅱ	Part of TMR	Punctuality	Face the production of non real time control area
Group Ⅲ	Part of DMIS	Non real time	Production management area

When set up the hard firewall equipment between the security group I and security group II (in the face of the power grid operation site to establish data communication), it should completely eradicate the direct link with Public communication link outside the network or the Public information channel link within the network. Considering that the MIS system has a Internet exit, the physical isolation device must be established between the safety group Ⅲ and safety group I / II. The DMIS in safety group Ⅲ should completely eradicate the direct link with Public communication link outside the network or the Public information channel link within the network. From the perspective of network structure security, the security group I and group II are considered as integrated systems and the security group is treated as an outside network. IDS system is both set up in the internal network and external network to prevent intrusion and virus from the internal and external intrusion. The overall system security configuration is shown in figure I

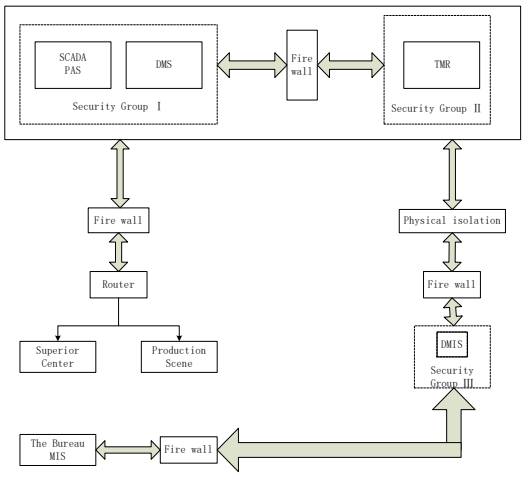

Fig.1 System-wide security protection configuration

3.3 The security policy of management.

The security policy of management can manage security strategies mainly through the following aspects.

a.To clear definition of computer security tasks, responsibilities and management, system administrators, the authority of the general user. The security level of the internal object (such as switch) of the automation system is defined by defining the node authority and operator authority, which can achieve that the specific man can manage the operating authority for a specific object at specific nodes. 4 levels are defined for user rights: first level is system maintenance, which is the maintenance of hardware system, network, database, node configuration, second level is maintenance, which is the editing and maintenance of data and graphics , third level is operator, which is the performance of the SCADA operation monitoring control functions, the fourth level is general user, which can only see a variety of pictures and cannot carry out any control operation.

b.The system / function / software tools of the whole system and operation of all personnel entering the system are all need matching registration tool. The security of longitudinal data exchange and operation of power system can be realized by public key technology or certificate technology.

c.To establish a network protection strategy based on the theory of defense in depth. Deep defense must be considered in the design process, to make a comprehensive consideration of any technical and decisive aspects relating to the network and use technology and management control as much as possible to reduce the threat to the network at all levels. In addition, the system of each level must not be affected. For example, in order to prevent internal threats, it need to restrict user only access to the necessary part of resources which is related to his work.

d.To establish effective configuration management process. Configuration management needs to cover the hardware and software configuration, the change of hardware or software may introduce some of the factors that threaten the security of the network. At this time, we must evaluate and control any change.

To establish system backup and disaster recovery plan. The plan must make quick recovery in any emergency situation. System backup is an important part of any security protection system, which is conducive to the rapid reconstruction of the network. All members must be familiar with the disaster recovery plan and make the appropriate adjustments according to the experience and lessons learned in practice.

4. Summary

Because the power system contains many application automation system integration, so its security system should be arranged reasonably in the system network architecture. The core parts of the production consider setting the security level according to the internal network. And the parts of production management consider setting the security level according to the external network.

Through the transverse effective safety isolation of application automation system, various network security technologies are used to ensure the security of the whole power network.

Acknowledgement

The authors would like to give their gratitude to the support of project “Research and demonstration of comprehensive integration technology for smart grid based on the feature of low carbon grid”, which is a 2012 technology project from China state grid, and also a major project (2013BAA01B00) from Eleven the Five national science and technology support program.

References

[1]. WANG Yi-ming, XIN Yao-zhong, XIANG Li, et al. Security and protection of dispatching automation systems and digital neworks. Automation of Electric Power Systems, vol. 24(2001) No. 21, P. 5-8.

[2]. LI Fang, HUANG YU-yu. Application of encryption technique in security login of MIS system. Journal of Engineering Graphics, vol 34(2003), No. 1, p. 37-43.

[3]. WANG Huai-bo, LI Lin, ZHANG Shen-sheng. Security mechanism in common object request broker architecture(CORBA) and its implementation. Journal of Shanghai Jiaotong University, vol.7(2000), No.34, p. 983-986.

[4]. MIN Jun, CONG Jing-ying. Research of technologies about intrusion detection[J]. Computer Application Research, Vol. 24(2002), No.2, p. 1-4.

[5]. DAI Ying-xia, LIAN Yi-feng, WANG Hang. System security and intrusion. Beijing: Tsinghua University press, 2002, p.78-86.