Research on Network Security of Electric Power Dispatching Automation

Jingsong Wang [a], Shaopeng Yan [b], Hui Fang [c], Qun Liu [d]

State Grid Henan Electric Power Company Luoyang Power Supply Company,

Luoyang 471000, China

[a]yshp-yshp@163.com,[b]1015903240@qq.com

Keywords: SCADA, network security

Abstract. Real-time SCADA system bears, near real-time control of the business and management information services, high data reliability requirements, SCADA systems also need to be connected with higher-level automation systems, office MIS systems, and high network utilization, there is a many security risks. Dispatching automation network if they can establish a more comprehensive security mechanism to properly configure the security system will make full use of the Internet age to bring efficient and convenient, greatly accelerate the development of power enterprises, but also to the dispatch maintenance personnel with to great convenience. In this paper, according to the network security system level and network security system design criteria, a method to build SCADA network security implementation, and from the firewall physical isolation in-depth analysis, we proposed the establishment of power dispatching network security solutions. The article also pointed out that, in addition to technical factors, management systems and personnel are also important factors affect network security.

1. Introduction

With the rapid development of computer network technology, expanding the scale of power systems, power management automation level of continuous improvement, application level grid energy management system continued to deepen, power dispatching automation from traditional SCADA real-time monitoring system to practical use up to grid energy load forecasting management systems, state estimation, dispatcher power flow, safety analysis, voltage and reactive power optimization,, optimal power flow and other practical applications. Access scheduling data network systems, more and more data exchange performed between dispatch centers, power plants, substations, users, etc. more and more frequent, which power monitoring system and data network security, reliability and timeliness. It presents new challenges. As the existing power monitoring systems and data networks in the original design of the construction of the security problem seriously enough, the system there are a variety of security risks. Meanwhile, with the power to establish the quality of customer service standards, electricity reliability, security, we have higher requirements than before, dispatching automation system as the electricity production, transmission, distribution and consumption integrated monitoring, system control, its greater reliability and security requirements is to improve the power quality of customer service an important guarantee. However, open information system must has many potential security risks, hackers and anti-hacking, destruction and the fight against the destruction will continue. In such a struggle, security technology as a unique global network builders more and more areas of concern. Based on the experience in implementing parts of the country grid secondary power system security engineering, this paper explores the implementation of the main methods , architecture and key technologies of security engineering under current conditions.

Ensure the security of information has become particularly important, there is a need to establish dispatching automation system based on the different characteristics of various applications to optimize power dispatching data network, the establishment of security system dispatching automation system to improve the security situation of power enterprises.

2. Network Architecture

Currently the main power dispatching automation complete SCADA functions (telemetry received from the plant stand, remote data is sent to the plant stand remote control, remote adjustment of command), PAS (network modeling, network topology, state estimation, dispatcher power flow, load forecasting, static security analysis, reactive power / voltage optimization control), system interface (large screen, the simulation screen, scheduling data network), WEB services and DTS function (control Center model module, power system model module and faculty system modules, respectively, to achieve power system simulation operations, structural simulation grid simulation results simulation process control and test) and so on.

In a network environment, network security system depends on the security of the network in each host system, and the safety of the host system is the operating system's security by the decision, there is no security of supported operating systems, network security also there is no foundation at all, "but the computer operating system has historically been dominated by a number of large US companies, these operating systems are not open source, there are many loopholes and pitfalls in security. computer hackers can easily from 0 0 backdoor into the system, to obtain control of the system and endanger important computer data processing or storage, "the operating system we do not have a better choice, the ground control station is generally used to reconcile mainframe UNIX operating system, of course, there are some choice WINDOWS operating machines system. UNIX system is superior in terms of security WINDOWS operating system, partly because the UNIX operating system than the WINDOWS operating system difficult to learn, partly because of strong dedicated UNIX operating system, such as TRU64 only run on ALPHA machine, SOLARIS only It runs on Sun machines.

Security system is based on network systems, secure network architecture is the underlying security system successfully established. In terms of security of the entire network structure, the main consideration optimizes network structure, systems and routing. Establish a network structure to consider the environment, equipment configuration and applications, remote networking, estimate traffic, network maintenance and management, network applications and business orientation and other factors. Mature network structure should be open, standardized, reliable, advanced and practical, and should have a structured design, full use of existing resources, with the ease of operation and management, improve the security system. Network structure using a layered architecture, is conducive to maintenance and management and better security control and business development.

3. Implement Network Application Layer

Firewall is an internal network and external network separate approach. You can limit conducted between the protected network and external network access, transfer operation, can be used as entrance information between different networks, according to information flow corporate security policies control access to the network, and itself have a strong anti-attack capability. Logically, a firewall is a separator, a limiter, is a parser to effectively control any activities between the internal network and external networks to ensure the security of internal networks. The firewall is to provide information security services, network and information security infrastructure. In the process of building a SCADA network, the firewall as the first line of defense, more and more be concerned.

In order to more efficiently deal with the various attacks on the network, the firewall also send separate the several defense architecture. According to physical characteristics, a firewall is divided into two categories, namely hardware and software firewalls. Software firewall is a special program on the gateway server is responsible for internal and external network switch or stand-alone personal computer being installed. It is the logical form of a firewall program to follow the system startup ring0 level by running a special driver module is inserted between the defense mechanisms for dealing with part of the network and the network interface device driver system, form a logical defense system.

Dispatching Automation has two sinks in the use of firewalls, located on the lower level

scheduling a private network, the main task is to send and receive data over the data received from the subordinate forwarding, and forward it to the superior scheduling data; another is located at MIS network access SCADA network WEB server, its main task is to MIS network to provide WEB services, only MIS network computers access WEB server, WEB server does not access the MIS network. Two firewalls location is not the same, not the same functionality provided, the configuration is also different. Many firewall features, each manufacturer is also vastly different firewall configuration, configuration rules is not possible, only the rational allocation of the firewall, in order to better protect network security.

4. Security Management and Network Maintenance

Faced with the fragility of computer network security, in addition to increasing the security services on the network design and improve system security measures, but also must make great efforts to strengthen safety management, because a lot of insecurity precisely reflected in organizational management. Data show that 70% of network insecurity comes from imperfect management. Network security management is the most important part. Rights and responsibilities unclear, chaotic management, security management system is not perfect, and lack of maneuverability so may lead to security risk management. Rights and responsibilities unclear, chaotic management, makes some casual employee or administrator to make some non-local employees even foreign workers enter the room powerhouse, or employee intentionally or unintentionally leak important information they know, but the management did not have the system to restrain. When the network is subject to attack or some other network security threats (illegal operations such as internal staff, etc.), cannot be real-time detection, monitoring, reporting and early warning. Meanwhile, when the accident occurred, it cannot provide clues to track hacker attacks and solve the case basis, that the lack of network controllability and audit ability. This requires us to visit the site of the multi-level activity records, to detect illegal intrusion. To establish a new network security mechanisms, a deep understanding of the network and must be able to provide immediate solutions, so the most feasible approach is to develop management systems and strengthen security management.

5. Application Security Management

Scheduling staff scheduling software should be used from a security point of view, the rational use of scheduling automation software.

(l) Classification authority

System administrators, maintenance personnel, operators, supervisors should have different permissions. The system administrator has the highest authority, you can set other personnel accounts, passwords and permissions features. In general, system administrators and maintenance personnel should not have remote control, remote adjustment authority, they should have to modify the parameters of the matter, drawing the wiring diagram, drawing rights report; operator due remote control, remote adjustment, set the number of artificial, permissions listed, print reports, etc., in addition to permission supervisors have operator, but also for the operator to supervise when making remote control.

(2) Remote Security

The current scheduling automation software can meet the safety remote control, you can take a double operation, duplex operation, but falsely accused accident happens every year. One reason is that the parameters set incorrectly, the remote control switch remote control number incorrectly, and did not do well and put into operation before the test; two remote protection reasons not to do it, do not allow remote control of the soft switch plate should place: three operating Reasons , supervisors did not press the remote control procedure. So operator, supervisor at the time of switch disconnections remote control must do to comply with the safety regulations remote control, it must first be operated votes rehearsal, non-negative Hera knife, error breaker, closing with a grounding wire with an electrical ground line, mistakenly charged interval operation. The operator should be

canceled leave for a long time operation panel currently used account.

6. Summary

In this paper, power dispatching automation system under the security situation in the network environment is analyzed, according to the practice of project implementation, from system security planning and safety equipment, such as the practical application of firewalls, physical isolation to improve safety management and other aspects of power dispatching automation system network security situation will be explained. It also proposes to protect and improve system security methods and measures, which has some practical significance.

7. Reference

[1]Deng Y, Cheng J. Research on intelligent architecture of real-time dispatching automation for power systems[C] Intelligent Control and Automation, 2002. Proceedings of the 4th World Congress on. IEEE, 2002:1092 - 1096.

[2]Hao Z P, Xiao-Wen Q I, University Z. Research on Electric Power Dispatching Automation System in Coal Enterprises[J]. Coal Technology, 2013.

[3]Wang B Y, Qiu S G, Zhang S M. Research on Authentication Algorithm Based on Double Factor in Power Dispatching Automation System[J]. Lecture Notes in Electrical Engineering, 2012.

[4]Wang B Y, Qiu S G, Zhang S M. Research on Authentication Algorithm Based on Double Factor in Power Dispatching Automation System[J]. Lecture Notes in Electrical Engineering, 2012.

[5]Fu-Bao W U, Bai Y C, Guo-Fu X I, et al. Electric Power Dispatching Automation System Based on Unix/Windows Associated Platform[J]. Automation of Electric Power Systems, 2005.

[6]Cheng-Qun H U. The Research on Accuracy and Reliability of Telecontrol Used in Dispatching Automation System[J]. Central China Electric Power, 2007.