Network Security Design for Manufacturing Enterprise

Jiangmin He[1, a], Rihuang Yao(Corresponding author)[2, b]

[1]The Fifth Electronics Research Institute of Ministry of Industry and Information Technology, No.110, Dongguanzhuang Road, Guangzhou, Guangdong, China

[2]The Fifth Electronics Research Institute of Ministry of Industry and Information Technology, No.110, Dongguanzhuang Road, Guangzhou, Guangdong, China

[a]hejm@ceprei.com, [b]yao6336@163.com

Keywords: Manufacturing enterprise, Network security, Design, Industrial Ethernet

Abstract. This paper firstly introduces the development of network and informatization, which has brought rapid development to enterprise at the same time also brought information security risk to it. Then combined the enterprise's features, provides a general method of design a security network for manufacturing enterprise. That is divides enterprise's network into three zones: Internet zone, office zone, and production zone; Next, introduces the security design method for each zone according to its respective features; Summary is given at the end.

Introduction

With the development of network and informatization, more and more enterprise increase investment in informatization, enterprises have built their network and deployed many information systems. These information systems bring work efficiency to the enterprises as well as a lot of security problems. The enterprise network and information system are attacked frequently. It lead that the internal data of the enterprise is revealed, and the important production system is damaged. All these above have certainly brought enormous economic losses of the enterprise.

Due to the manufacturing enterprise's features, more challenges are brought in the network security. The life cycle of product includes multiple links, such as design, procurement, manufacturing, sales, service, quality improvement. Therefore, the information system of manufacturing enterprise covers each link of the product life cycle. For example ERP (Enterprise Resource Planning), PDM (Product Data Management), MPM (Manufacturing Process Management), CRM (Customer Relationship Management), SCM (Supply Chain Management), WMS (Warehouse Management System), MES (Manufacturing Execution System), OA (Office Automation system) etc. It shows than manufacturing enterprise has various information system and complex network structure. And compared with the IT company, the technological level of computer and network security of the staff is lower, the information security awareness is weaker. All these above make manufacturing enterprise face a lot of information security problems.

The problem is how to reduce information security risk efficiently? This paper provides a general method of network security design for manufacturing enterprise.

Zone division of network

According to the feature of manufacturing enterprise, the enterprise network can be divided into three zones, as shown in fig. 1.

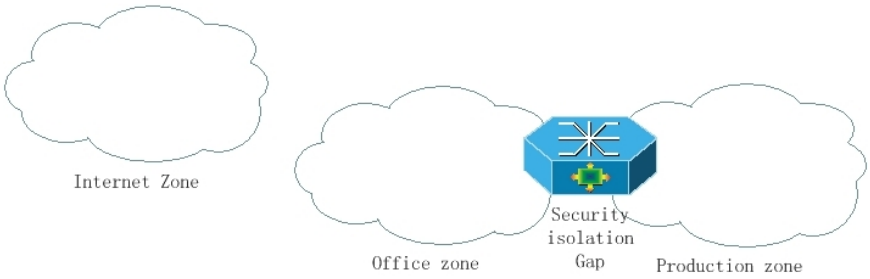

Fig.1 Zone division of network

The enterprise network are divided into Internet zone, office zone and production zone, different zones perform different functions. The benefits of zone division of network is that, it is able to execute key protection for the important zone, and guarantee that the security problem occurred in one zone does not affect the other zones. The functions of the three zones as follows:

The Internet zone is used for internal users of enterprise to access the Internet, deploy the information system for Internet access (such as enterprise website, Email server etc.). Because the main source of network attacks is form the Internet, so the Internet zone, office zone, and production zone are physical isolated; Office zone are used for deploying various of office and management information systems, such as OA, ERP, CRM etc.; The production system is deployed in the production zone, including not only the essential elements such as server and switch, but also various of production devices as machine tool and sensor.

For security reasons, the office zone and production zone are physical isolated with Internet, but there are data interaction between office zone and production zone. For example, office zone needs collect monitoring data from production zone, and send control instructions to production zone, therefore, physical isolation cannot be implemented between office zone and production zone. Because all staffs can access the office zone, the potential security risk cannot naturally be ignored. In order to guarantee the security of production zone, security isolation Gap is deployed between office zone and production zone. Because the security isolation Gap's data exchange unit connects internal and external network are not in the same time, which can realize physical isolation between two network zones. Also the security isolation Gap can take security review of data, therefore, the information security of production network zone is effectively guaranteed.

Security planning of Internet zone

The security planning of Internet zone is shown in fig. 2.

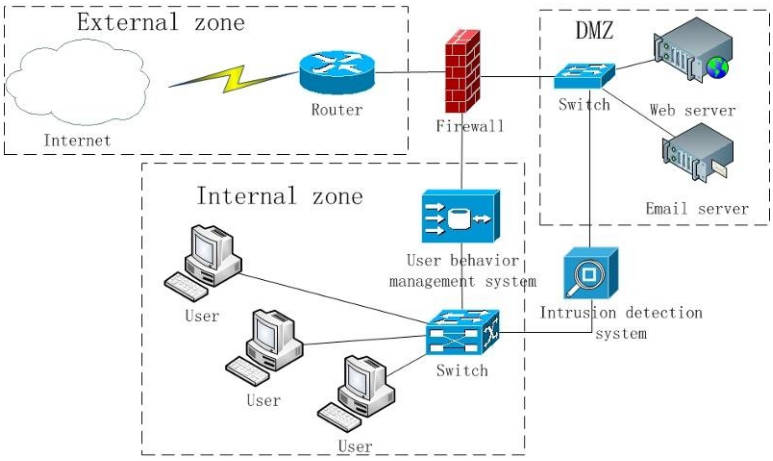

Fig.2 The security planning topological graph of Internet zone

Internet zone is divided into three subzones through the firewall: external zone, internal zone and DMZ (demilitarized zone). External zone connects to Internet, the servers are placed in DMZ, internal network zone is for employees accessing to the Internet. The areas among unused zones are isolated through firewall. On the strategy setting. External zone can only access the specified service in DMZ, internal zone and DMZ can access external zone, but external zone and DMZ are not allowed to access internal zone.

The user behavior management system is deployed in internal zone, which can monitoring employees' online activities. It can not only improve the work efficiency, but also prevent the enterprise information disclosure. The intrusion detection system is connected to the server access switch and user access switch, it detect network intrusion behavior for the first time, so the administrator can take relevant measures to prevent the expansion of intrusion events.

Security planning of office Zone

The security planning of office zone is shown in fig.3.

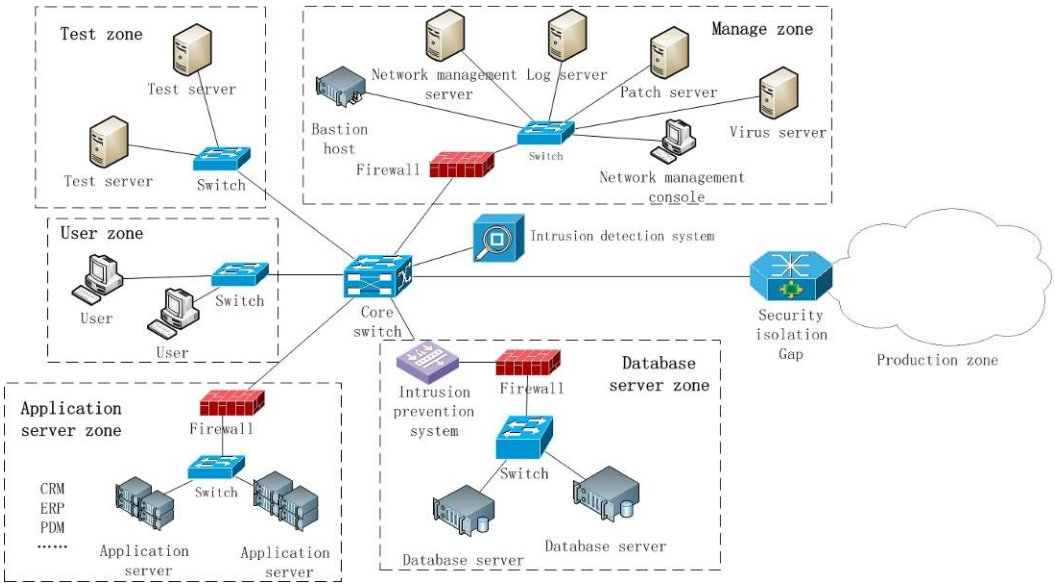

Fig. 3 The security planning topological graph of office zone

The office zone is deployed with many information systems, which is the zone with the most servers and the most complex network topology structure, so it needed to be detailed security planning. According to the different functions, the office area is divided into five sub zones: application server zone, database server zone, manage zone, test zone, user zone. The security measures are different, according to the important degree of each zone. All zones are connected by the core switch.

Information systems for office of manufacturing enterprise are deployed in application server zone, including CRM, ERP, PDM, etc. All these above information systems are peripheral systems except the manufacturing execution system. It's the important support for enterprise's daily work. Firework is deployed in the border of application server zone, protecting of application servers.

Data is the life of enterprise, it's the most important thing that need to be protected in the information system. And based on the demand for defense in depth of security architecture, the database server is divided into a separate zone, it is called database server zone. Similarly, the firewall is deployed in the border of database server zone. In view of the fact that database is very important, the intrusion prevention system (IPS) is added in the border of database server zone. IPS

not only can detect the attacks, but also block the attacks, prevent next Intrusion and guarantee the data security of enterprise.

The network management system, information monitoring system and other supplementary information system are deployed in the manage zone, include log server, network management server, patch server, virus server etc. The servers and network devices in office zone are numerous, it's hard to manage independently and hard to audit manager behavior. Therefore, deploy bastion host to execute unified login, authority division and behavior auditing for all devices. Network management console is only deployed in manage zone, not allowed to manage from user zone.

The test server is deployed in test zone, which is used for the development of information system, patch testing, compatibility testing etc. It is very necessary to build the test zone. Because based on the feature of manufacturing enterprise, system availability is very important, if the patch is not compatible and the system files might be wrongly deleted after upgrading virus database, so the seemingly insignificant modification may cause system crash. All these will cause halt production and bring economic losses. For this reason, any system modification is need to be tested in test zone, and can be deployed only if it have no question.

User zone is used for user terminal access. The employee of enterprise access information systems form it.

Security planning for Production Zone

In traditional industrial control network, a variety of distributed control system based on bus such as RS485，RS232、CAN etc. has definite defects. For instance, poor anti-interference ability, poor encryption ability, slow transfer rate etc. Therefore, the industrial Ethernet based on TCP/IP agreement is adopted for production network. Security planning for production Zone is shown in fig. 4.

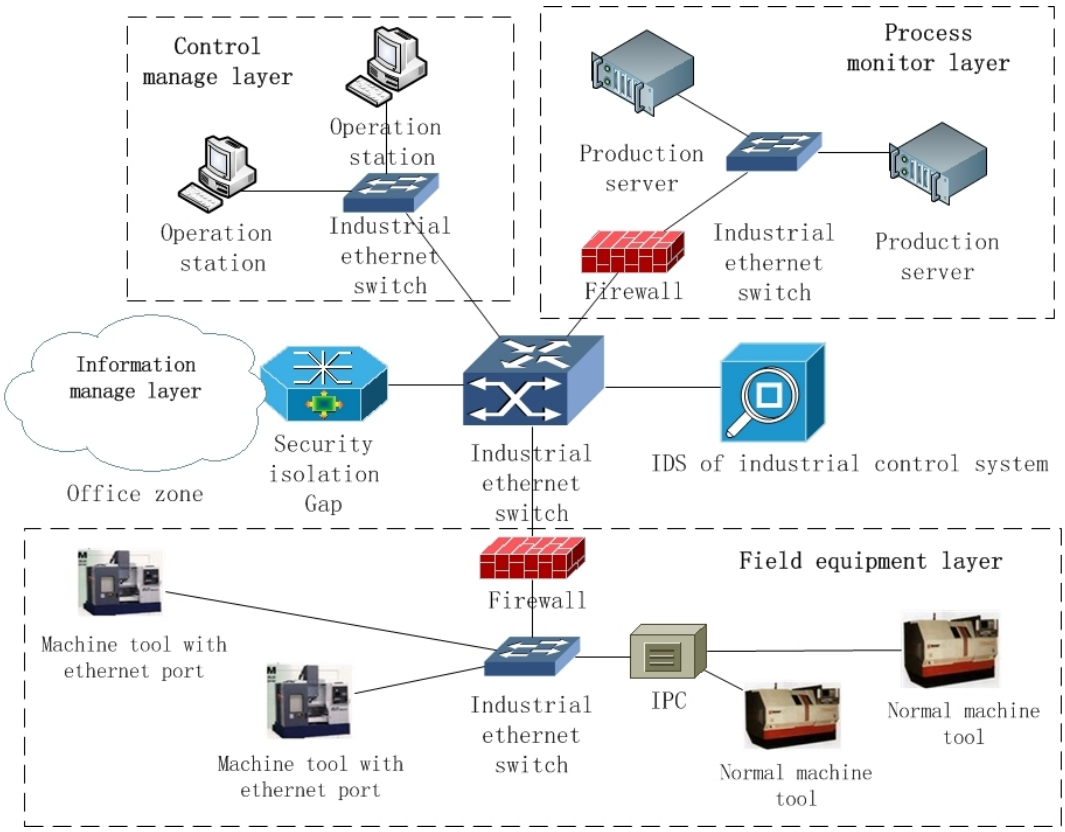

Fig.4 The security planning topological graph for production zone

The traditional industrial automation control network can be divided into three layers: information manage layer, control layer and field equipment layer, this paper divides the control layer into control manage layer and process monitor layer, which formed four layers security architecture system: information manage layer, control manage layer, process monitor layer and filed equipment layer.

The information manage layer is deployed in office zone, which is used for collecting information and monitoring during production process. The office zone and production zone are isolated with security isolation Gap to protect the production zone not be hostile attacked from office zone; Process monitor layer is used for deploying production server which is use for processing production dispatching and real time monitor, fault diagnosis etc. Because the industrial Ethernet connect different layers and up and down network layers use the same protocol with interoperability, only deploying the security isolation Gap in the border of production zone is not enough, therefore deploying firewall to protect in the border of process monitor layer to form multi-level protection structure; Control manage layer deploying operation station, which are used for accessing production server and executing production control operation; Filed equipment layer is composited with various of production devices. They receives the order from control manage layer and process monitor layer and execute production action, returns related information. Similarly, deploying firewall in the border of field equipment layer to protect the internal network.

Due to the higher requirements of real-time, reliability and transmission rate to industrial Ethernet, all of the switches is using industrial Ethernet switch. Each layer is connected to the core switch, and specified intrusion detection system of industrial control system is also connected to the core switch in order to detect and alarm the behaviors such as possible intrusion event, unusual control order and Trojan virus attacks etc.

In view of the physical isolation between production zone and Internet, and the servers are relatively few, regular off-line update of server patch and virus database to reduce risk of Trojan virus spreading is enough.

Summary

This paper provides a general method for security design of manufacturing enterprise network. Dividing the enterprise network into three zones as Internet zone, office zone, production zone. The security isolation between different zones to achieve the purpose of isolating risk data flow. Each zone is also divided into several subzones according to its functions. Different security measures are used for different zones and subzones according to their importance, enterprises can have a definite object in view and protecting the important data.

The network topology listed in this paper is not a physical topology, but a logic topology. For example, the switch and firewall listed in the topology are not only just one, might be two or more, but only be seen as one in logically. Manufacturing enterprise has very high requirement for system availability, network and device redundancy should be guaranteed. In addition, the general security measures of information system such as VLAN division, MAC address binding, ACL etc. Enterprises can chose according to the requirements of their own.

References

[1] Yuanyuan Liu, Yazhe Li, Jiankang LIU, Industry and Mine Automation, Issue 7, pp. 109-111, 2010 In Chinese

[2] Jie Peng, Qijia Ying, Chinese Journal of Scientific Instrument, Vol.25，Issue 4, Supplement, pp.516-517, 2004 In Chinese

[3] Zhifeng Liang, Xiang Xie, Xiaoqi Tang, Modern Manufacturing Engineering, Issue 1, pp. 38-40, 2006 In Chinese

[4] Dongru Ruan, Dongguang Xie, Control Engineering, Vol.13, Supplement, pp.112-114, 2006 In Chinese

[5] Information on http://baike.baidu.com/