CHEMICAL ENGINEERING TRANSACTIONS
VOL. 66, 2018
A publication of AIDIC
The Italian Association of Chemical Engineering
Online at www.aidic.it/cet
Guest Editors: Songying Zhao, Yougang Sun, Ye Zhou

ISBN 978-88-95608-63-1; **ISSN** 2283-9216
DOI: 10.3303/CET1866237

Chemical Enterprise Network Construction and Network Security Solution

Hong Zhang, Pei Li, Jie Zhang

Shanxi Conservancy Technical Institute, Yuncheng 044004, China
syzhlp@126.com

With the informatization process of the chemical industry deepening and the scale of chemical enterprise network gradually expanding, it has brought about the problems of network and information security in chemical enterprises. In order to protect the information security and the network equipment security, and further promote the construction of their network informatization construction and ensure their safe operation of chemical enterprises, this paper analyses the network security configuration and the solutions to network security in terms of the network features of chemical enterprises. Firstly, the network environment background of chemical enterprises was introduced. Based on this, the design requirements of network security were also proposed. Then, the topology structure of chemical enterprise network was designed, the network security and management mechanism of chemical enterprises were analysed, and the related scheme security policy deployment was proposed. Finally, the results of network security application in chemical enterprises were summarized. This study provides constructive guidance for the construction of network security for chemical enterprises, which is of great significance for ensuring the management and operation of chemical enterprises' network security.

1. Introduction

The application of computer networks in all walks of life has become more and more extensive, and the dependence of enterprise management on networks is also increasing. However, with the age of big data developing, data interaction and frequent information exchange have brought great challenges to the management operation of information networks and network information security (Mao and Liu, 2010). The industrial network virus Stuxnet (computer worm) that broke out in Iran in 2010 was the first industrial virus in the field of industrial control, and its target of attack even included the important industrial facilities such as nuclear power plants etc. The era of industrial viruses has come (Dzemyda and Petkus, 2001).

In order to prevent industrial virus attacks, some scholars have discussed the enterprise's industrial control network security technology and established a targeted security protection system (Minoli and James, 2015); some scholars, from the perspective of enterprise host systems and network design, made safety configuration to provide the enterprises with network hazard resistance ability. Therefore, to adapt to the rapid development of network technology and economy, and to further improve the information management level and network security protection capabilities of China's chemical enterprises, this paper conducts analysis about the network security solution for chemical enterprises (Celina et al., 2011).

This paper is mainly divided into four parts: the network background, network design requirements, topological structure of network design, the network security and management mechanisms, and the results of network research of chemical enterprises. It focuses on the security policy deployment of chemical enterprises networks, setting up VLANs, firewalls, and VPNs, and filtering of chemical enterprises' data packet transmissions, so as to greatly reduce the chance of virus infection. This study not only guarantees the real-time of data and information transmission for chemical enterprises, but also provides effective protection for the security of the chemical enterprise network system.

Please cite this article as: Zhang H., Li P., Zhang J., 2018, Chemical enterprise network construction and network security solution, Chemical Engineering Transactions, 66, 1417-1422 DOI:10.3303/CET1866237

2. Current situation and development demands of chemical enterprise network environment

2.1 Background of network environment

The construction of enterprise informatization office platform makes the office and management of the enterprise more and more dependent on the computer network. The remote OA office of the enterprise, the normal operation of the enterprise's normal management and decision network platform, and the data security of the enterprise network environment are crucial to the development of the enterprise. (Aras and Ümit, 2018). Chemical enterprises have the features such as great distance between the functional department, chemical plant, and chemical equipment, etc., large data transmission volume of complicated chemical product manufacturing process flow, and independent regional office networks, which affect the interconnection of the entire enterprise's network data. In order to speed up the informatization construction, chemical enterprises are exploring ways to build an enterprise-class network that combines office automation, remote OA operations, integrated business management, unattended monitoring of remote production sites, remote communications, and information dissemination and querying (Krajnovic, 2009).

The security of the network environment has received extensive attention since the 1970s. After more than 30 years of development, network information security has been formulated in related standards. It have achieved substantial results in basic theoretical research, security product development, defense system construction, personnel training, and safety awareness education. The connotation of network information security evolved from the public key cryptosystem of the 1970s to the integrity, controllability, availability, and non-repudiation of network information, and further developed into "attack" and "defense". The infrastructure and implementation strategies for the areas of measurement, detection, control, management, assessment, and so on. With the popularity of the Internet, the continuous integration of mobile, Internet, and telecommunication services, and the protection and management of network security have received extensive attention from various companies. Building enterprise networks into truly secure and reliable networks has become one of the most important issues that every enterprise and security researcher needs to solve.

2.2 Design requirement analysis of chemical enterprise network

2.2.1 Design objective and requirements

Arranging optical fibres at the site of chemical enterprises' office buildings and chemical production facilities, and connecting them through twisted-pair cables within departmental offices are the common methods for the construction of network infrastructure for chemical enterprises (Ronald and Ballou, 2001). In order to achieve the requirements such as enterprise-class ERP system and enterprise automation office management system etc., the chemical enterprise network design needs to meet the characteristics and specific requirements as shown in Table 1:

Table 1: Requirement of chemical company network design

Characteristic	Specific requirements
Real-time data transmission, data transmission security	Provide WWW Web Service
Realize office automation in all departments within the chemical group	Business Post Office Service
Synchronize the information of each branch company	FTP and information sharing services
Resource sharing, product information sharing, real-time news release	Remote monitoring service
Real-time monitoring of hazardous workplaces	Domain Control Service
Realize centralized ERP system and enterprise operation management monitoring system	Network safety

2.2.2 Demand analysis for chemical enterprise network construction

The chemical enterprise network is interconnected in the manner of the primary network and secondary network. The network security is protected by hierarchical structure, and each level is transited by routing (Sherali and Smith, 1997) (Fig.1).

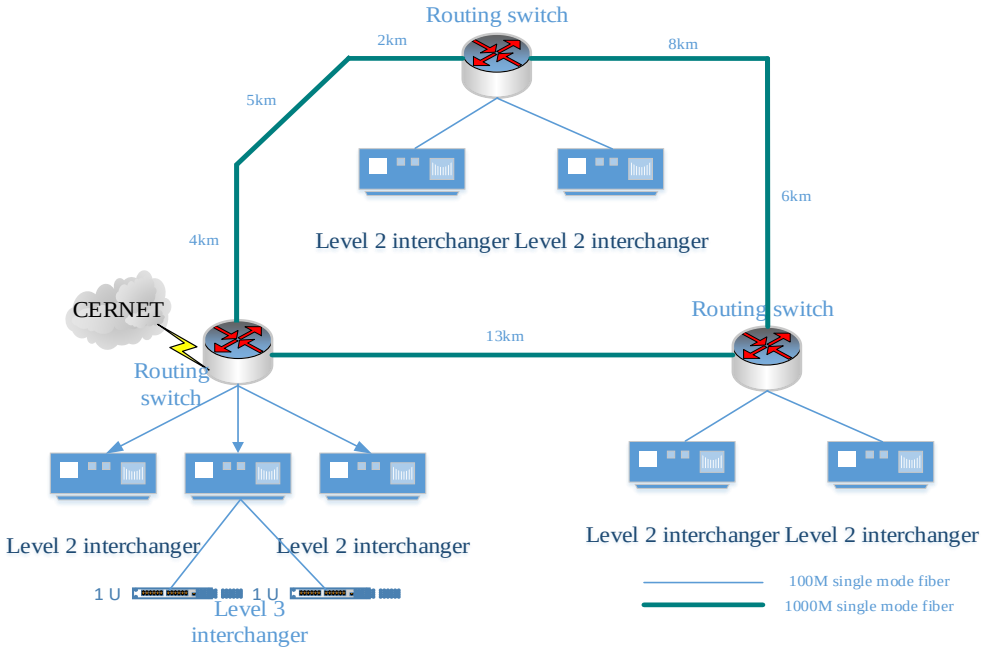

Figure 1: Chemical enterprise network backbone topology

2.2.3 System requirements and user demands for network construction of chemical enterprises

1) System requirements
The stability and reliability of the system: Window 10 operating system and SQL2010 database are selected.
System security: on the one hand, VLANs are used to divide the entire enterprise network; on the other hand, firewalls are used to set the enterprise network.
System expandability, compatibility, and manageability: the network system needs to guarantee the ability of chemical enterprises to manage their operations in the next few years. At the same time, the system should be easy to manage centrally, enabling the management costs of the enterprise network to be reduced as much as possible.
2) User demands
The fluency of transmission communications and the high speed of data processing are challenges faced by chemical enterprises. The chemical network management information management platform should be user-friendly and easy to operate; it can implement WAN integration functions and use three-tier data exchange; the network requires good security policies to avoid external malicious attacks (Randall et al., 2002).

2.2.4 Introduction to chemical network topology

The chemical network topology adopts a “hierarchical” model, which divides the corporate office network into one single layer, the enterprise production shop network into one layer, and the enterprise warehouse management network into one layer. The hierarchical and star-based structure can improve the network’s data processing capability and network maintenance costs (Szeto et al., 2010). The construction of the chemical enterprise network based on multiple levels aims to divide the enterprise network into several subsystems, and the hierarchical management simplifies the management process. Fig.2 shows the hierarchical network topology.

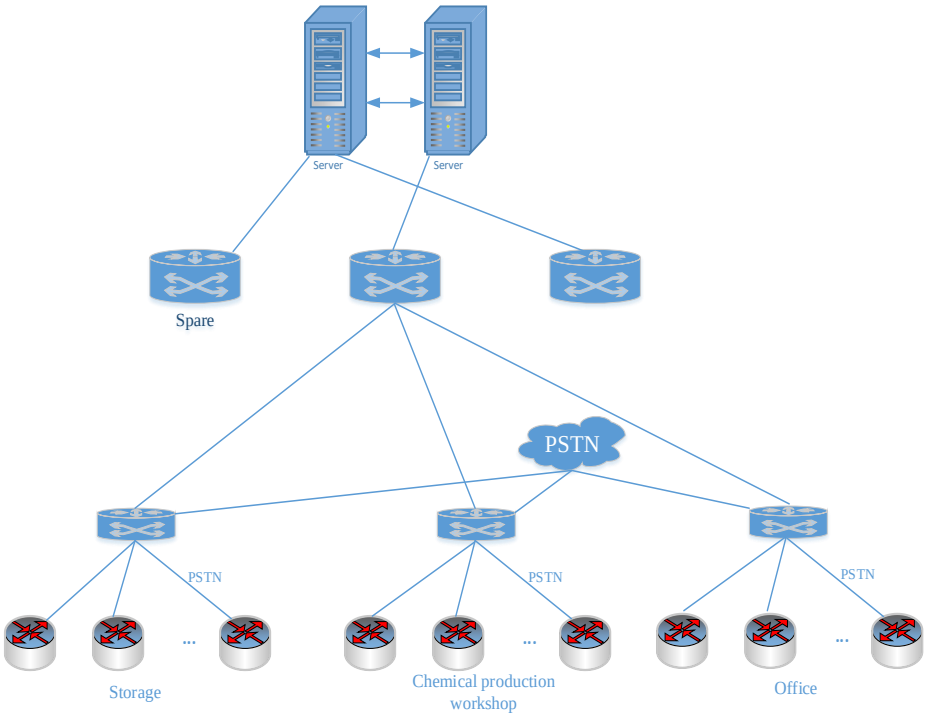

Figure 2: Hierarchical design network topology

3. Chemical enterprise network security and management mechanism

3.1 Chemical enterprise network security

The network security of chemical enterprises can be divided into three parts: enterprise network physical security, enterprise network security itself, and enterprise network information security. The negligence of any one of these three parts can easily lead to an attack on the enterprise network that receives shock wave viruses or malicious operations inside the network. (Mateus and Franqueira, 2000). As shown in Fig.3, it is a schematic diagram of the security of the chemical company network.

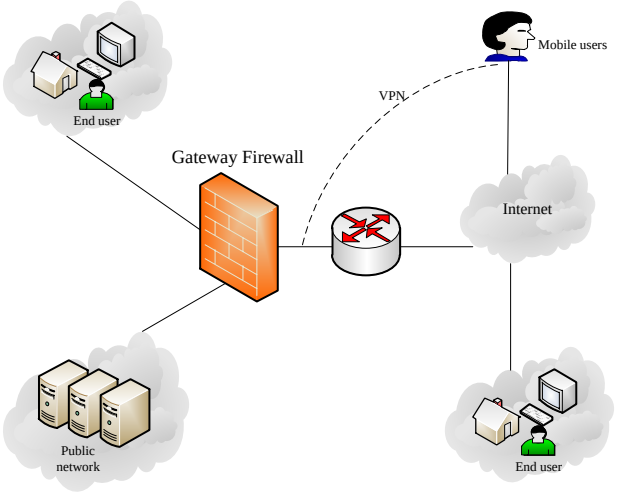

Figure 3: Chemical company network security diagram.

3.1.1 Physical security of chemical enterprise network

Physical security mainly refers to the security of physical equipment in chemical networks. Due to high-risk explosion zoning in the production environment of chemical enterprises, different field network equipment is exposed to fire, flood, earthquake and other risks. Periodic inspection of on-site network equipment plays an

important role in ensuring network physical security. At the same time, the comprehensive network management of chemical enterprises should be well equipped with measures such as waterproofing, lightning protection, and electromagnetic leakage prevention.

3.1.2 Chemical enterprise network security itself

The security vulnerabilities of enterprise-class network are unavoidable, but the system server host and network operating security can be ensured, if regular control is made for the system security vulnerabilities and network access to protect the security of the enterprise network itself.

3.1.3 Information security in the enterprise network

The information security is ensured by ensuring the awareness of internal personnel data protection in chemical enterprises, and also improving the security of information transmission during the operation of enterprise data. In addition, information authorization and authentication storage are the key to protecting database resources.

3.2 Chemical enterprise security policy deployment

3.2.1 VLAN settings

The VLAN exists in the LAN network of the entire chemical enterprise as a kind of local broadcast domain, and the LAN is divided into multiple logical VLANs through VLAN settings. VLAN and LAN network have the same communication method, but different VLAN settings are different. The data in a VLAN can only be in this VLAN, which greatly improves the security of internal information in LAN (Shimizu, 2010).
VLAN settings can effectively prevent unauthorized access between various departments and ensure the security of sensitive information within chemical enterprises. Each VLAN can also implement point-to-point data exchange through the encapsulation technology of trunk link (Chan and Beg, 2002).

3.2.2 Firewall Settings

The firewall is the main mode of defence against external network attacks. The chemical enterprise network firewall is recommended to use the Cisco PIX firewall. Through the firewall setting, the chemical enterprise network is divided into the internal area network (intranet) and external area network (internet network). The ways such as depth data table processing, IP/URL filtering, TCP/IP termination, and access to network process tracking etc. are used to implement firewall attacks on external network viruses.

3.2.3 VPN Settings

Virtual private networks (VPNs) are specifically designed for corporate executives and employees to access internal data of chemical enterprises when using external networks, and by setting up a special channel to achieve secure transmission of information (Eisenbrand et al., 2007). VPN is the great expansion of intranets in enterprises. By using VPNs, remote access to intranets can be achieved.
VPN services are all based on tunnel technologies. VPN mainly adopts tunnel technology, encryption and decryption technology, key management technology, and user and device identity authentication technology (Hurkens et al., 2004). Fig.4 shows the schematic diagram of the VPN technology.

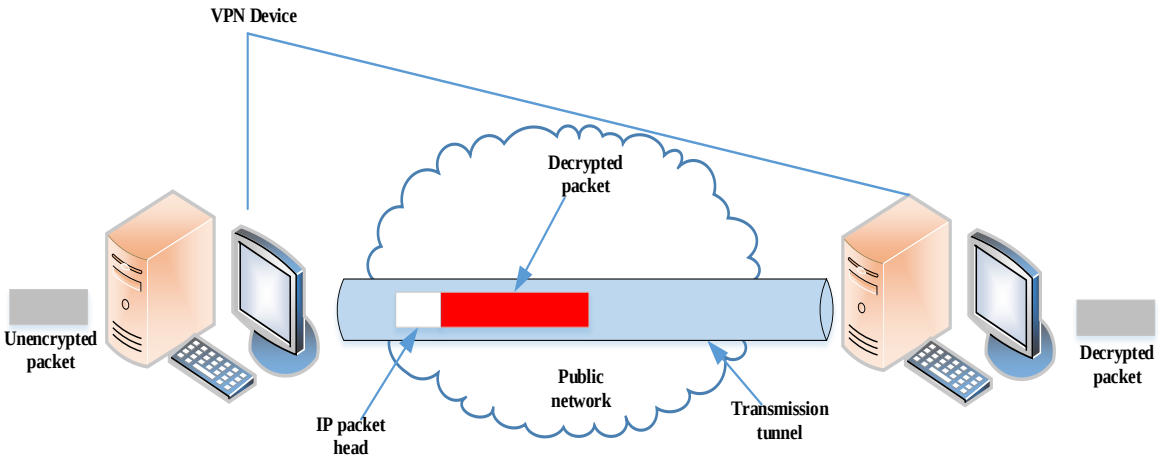

Figure 4: The VPN technology schematic

In the chemical enterprise network solution, the ip-VPN based on IP protocol is used to transmit encrypted data packets through the tunnel. Through the analysis of the network construction and network security policy of chemical enterprise, this paper initially completed the establishment of the local area network of chemical enterprise and brought great convenience to internal data transmission. The internal employees of the chemical enterprise can work in a stable network environment. The amount of data accessed by the internal network is unlimited, and the maximum external network can reach up to FTP accesses. In addition, the data bandwidth and the security in the data transmission process were protected effectively.

4. Conclusions

With the deepening of the network informatization process, enterprise network office systems have provided great help for office management and production management and also improved office efficiency. However, along with the increase of network dependence, network security issues have also attracted more and more attention. In view of the characteristics of chemical enterprise management and production operations, this paper proposes the network solution for chemical enterprises based on demand analysis and analyses the network security solutions. The main conclusions of this paper are as follows:

(1) Based on the characteristics of chemical enterprises, detailed analysis was conducted for the construction needs of the chemical enterprises network; the related network topology was established.

(2) The network security and relevant management mechanism of chemical enterprises were analysed in detail, and the related security policy deployment scheme was put forward.

(3) This study shall provide references for chemical enterprises to establish the secure information exchange and office platform, which is of great significance for safeguarding the management and operation of chemical enterprises' network security.

Acknowledgement

This work was supported by a General Financial Grant from the Research and Extension of Water Conservancy Science and Technology in Shanxi Province (Grant No.201625).

References

Aras N., Ümit B., 2018, Robust supply chain network design with multi-products for a company in the food sector, Applied Mathematical Modelling, 60, 526-539, DOI: 10.1016/j.apm.2018.03.034.

Ballou R.H., 2001, Unresolved issues in supply chain network design, Information Systems Frontiers, 3(4), 417-426, DOI: 10.1023/A:1012872704057.

Dzemyda G., Petkus T., 2001, Application of computer network to solve the complex applied multiple criteria optimization problems, Informatica, 12(1), 45-60.

Krajnovic N., 2009, The design of a highly available enterprise ip telephony network for the power utility of serbia company, IEEE Communications Magazine, 47(4), 118-122, DOI: 10.1109/mcom.2009.4907417.

Leão C.P., Soares F.O., Machado J., Seabra E., 2011, Design and development of an industrial network laboratory, International Journal of Emerging Technologies in Learning, 6(S1), 21-26, DOI: 10.3991/ijet.v6is1.1615.

Mao H., Liu L., 2010, The research and application of pbl didactics in the computer network technology course, IEEE International Conference on Computer & Information Technology, 2239-2243, DOI: 10.1109/cit.2010.386.

Minoli C., James, D., 2015, Industrial network security, Network Security, 4, DOI: /10.1016/s1353-4858(15)30014-3.

Randall M., Mcmahon G., Sugden S., 2002, A simulated annealing approach to communication network design, Journal of Combinatorial Optimization, 6(1), 55-65, DOI: 10.1023/A:1013337324030.

Sherali H.D., Smith E.P., 1997, A global optimization approach to a water distribution network design problem, Journal of Global Optimization, 11(2), 107-132, DOI: 10.1023/A:1008207817095