Research on Oilfield Network Information Security Protection System

Jingshu Wang [1, a *], Xin Wang[1,b] and Xiaolong Wang[2,c]

[1]Department of Information Management, Dalian Neusoft University of Information, Dalian, China

[2]Dalian Cyber Industrial Controls &Security Technologies Co.,Ltd, Dalian ,China

[a.]wangjingshu@neusoft.edu.cn; [b.]wangxin@neusoft.edu.cn; [c.]xiaolong.WANG@CyberICS.tech

* Corresponding author

Keywords: Smart oilfield; Network information security; Oilfield information management

Abstract. In recent years, the state has proposed the network architecture and security requirements for industrial control systems built by smart oilfields. Under the background of this, the paper first describes the importance of information security in the oilfield industrial network in the digital oilfield process. Furthermore, the current situation of industrial control network in SL oilfield is analyzed, and the possible risks are listed. At the same time, the characteristics and shortcomings of existing solutions are analyzed. Then the oilfield network information security protection system is proposed as an optimization solution. The test results show that the proposed system is economically feasible and can be further promoted.

Introduction

With the development of China's social economy, the development of oil companies has played an increasingly important role in the stability of the market economy. Through the interconnection of industrial control networks, the industrial control system of the petroleum industry has become more open and no longer a “network island” in the past. However, the industrial control network environment in which the “smart oil field” is located is also facing increasingly serious threats [1], and the construction of oilfield safety systems has gradually received attention and attention. Sinopec has launched the “four modernization” construction work for ground engineering to replace the traditional construction organization method and management mode [2]. It is “standardized design, standardized procurement, modular construction, and informationization promotion”.

Based on this, in 2012, SL Oilfield carried out a new management mode construction work with “four modernizations” as the main content to improve the refined management level of SL oilfield. Through the informationization upgrade, in the computerized upgrade process, because the dedicated equipment and SCADA system replaced the original large number of manual operations, the entire oil production block was interconnected through the industrial control network and the office network, eliminating the “information island”. This is especially important for the speed and stability of passing information during network transmission. In order to ensure the sustainable and stable production of the “smart oil field”, the protection of the industrial control network of the oil production base should be actively strengthened.

The research start time of China's industrial control system is relatively backward. However, the scale of the industrial control system market has grown rapidly. With the rapid development of industrial automation and information integration, information technology, industrial control, network and communication technologies are gradually being widely used. The inherent vulnerability of the industrial control system's security status, coupled with growing external threats, has already attracted the attention of relevant national departments and even raised to the level of the “national security strategy”. And actively consider policies, standards, technologies, programs and other countermeasures for this issue. In September 2011, the Ministry of Industry and Information Technology issued the “Notice on Strengthening Information Security Management of Industrial Control Systems”. Strengthen the construction of industrial control information security management, security assessment and inspection, and the construction of vulnerability release

Copyright © (2019) Francis Academic Press, UK DOI: 10.25236/icmcs.2019.020

mechanisms in key areas. In May 2012, the State Council passed the “Several Opinions on Promoting Information Development and Safeguarding Information Security”, clearly stating that information security of industrial control systems should be guaranteed [3]. In August 2016, the Ministry of Industry and Information Technology organized the development of 14 standards, such as the “Guide to the Application of Safety Control System for Information Security Technology”. It is used to guide industrial enterprises to establish the safety control ability of industrial control systems; and put forward specific measures to strengthen the safety protection of industrial control systems, which are used to strengthen the safety guarantee capability of construction industrial control systems. Western developed countries are led by the United States, attaches great importance to the safety and protection of industrial control systems, and has implemented a series of coordinated actions[4,5]. In 2003, the US National Cyberspace Security Strategy clearly stated that the protection of industrial control systems was listed as a national priority. In 2006, the US National Infrastructure Protection Program explicitly listed industrial control systems, computer systems, and the Internet as part of the cyberspace infrastructure. In October 2009, the US Department of Homeland Security issued the "Industrial Control System Protection Strategy."

System Analysis and Design

Oilfield Industrial Control Network Status. The oilfield industrial control system has developed a complete industrial control safety protection plan, and divided different safety management areas according to the level according to four different production management levels. According to different levels, establish a security defense strategy, improve the security of industrial control network construction, and finally achieve the goal of improving safety production management level, improving work efficiency and management efficiency. The management of the head office selects the data platform of each oil production plant as the data source, synchronizes the data required by the head office, and establishes the head office management system; Oil plant management, real-time database deployment, receiving management area (work area) data transmission; real-time monitoring, analysis, security management, reporting and equipment management status; Production operation layer, including management area office network and management area production network; Well site layer, mainly based on station and wellhead. The station includes a wired network-based control system; the wellhead is unattended and needs to collect and upload data through the RTU, including wired and wireless networks.

Oilfield industrial control system mainly refers to data collection and real-time monitoring of oil and gas wells and stations. Oil, natural gas, wells and some unattended warehouses have high temperature requirements and harsh environments, often using RTU systems. The booster station, the transfer station and the joint station have high requirements for real-time performance. The logic interlock control is more common, usually using the PLC system; there are many control points in the joint station/booster station, gas injection station, etc. Loop control, so DCS system is often used; and the management level, plant level monitoring and command and dispatch center usually needs to integrate multiple systems, so a SCADA center will be set up for real-time data access of various industrial control systems in the jurisdiction [6].

Risks of Existence. Due to the universality and limitations of network security measures, the industrial control system currently uses a lot of general-purpose hardware and general-purpose software to realize the connection between the office network and the industrial control network through the common protocol. The threat of Trojans and viruses spread to industrial control systems, and controlling the safety of industrial control systems has become an important and urgent matter. Possible risks include: operating system security vulnerabilities; application software security vulnerabilities; limitations of network security devices; cyber attacks and intrusions; vulnerabilities in wireless networks; vulnerabilities in communication protocols and viruses and malicious code.

Design of Protection Plan. The construction and implementation of industrial control network security protection projects will improve the reliability and stability of equipment, systems and networks, and ensure the overall security of industrial networks. Realize vertical border protection

of management area and production area, effectively avoid the threat of information network to production control network security; realize horizontal logical isolation and security protection between production area business systems, prevent unauthorized access, intrusion attacks and illegal access. Security hardening of the upper computer, engineering station and system server system, using the whitelist mechanism to establish a security baseline to prevent damage caused by virus Trojans and malware; intrusion detection and auditing of the entire network, timely detection of violations in the network or system , behavioral strategies and signs of attack.

A gradual security upgrade through existing industrial control systems. Security measures can be divided into three steps. First, we must develop security strategies and processes to ensure that follow-up security measures are followed. Second, we have developed a preliminary defense strategy that is based on key points that are currently easily resolved and urgently needed to be addressed. Finally, establish an industrial control system defense system to ensure oilfield information security and safe and stable production.

System Development

Demand Analysis. The main task of the system requirements analysis phase is to conduct thorough investigation and analysis by developers in the early stage of design to accurately understand the specific requirements of users. The system should meet the following requirements: First, the performance requirements, the system should be re-tested and the corresponding measures should be taken in the design and implementation of the front-end and back-end. The second is to meet the ease of use requirements. The goal of ease of use is user-centric, so that users can find the functions and data information they care about most easily, and learn and use them as easily as possible so that users can more effectively Finish their work. In addition, there is still a need to meet the needs of scalability, maintainability and interface design friendliness.

Development Environment and Architecture. The system adopts MVC architecture mode design idea. The server side adopts SpringBoot, Spring-data-jpa and Freemarker integrated infrastructure. The front end adopts Bootstrap, Jquery, AngularJS and Echart integration framework. The whole system architecture includes five levels: presentation layer, control layer, service layer, DAO layer and physical layer.Throughout the architecture, the Freemarker framework is officially recommended by SpringBoot, and can be used well with Spring MVC to achieve front-to-back separation. The system is designed and developed based on the MVC pattern as a whole, in an effort to reduce the degree of coupling between layers. Use the Bootstrap+Jquery+AngularJs+Echarts framework. In order to achieve system maintenance, only a small amount of code needs to be modified to complete system function expansion, database server modification and so on.

Functional module design. System function design mainly considers the following aspects: support user identification, support user authority division, support network status overview, support "oilfield industrial control network security access unit" security configuration, support strategy batch delivery, support a lot The traffic of the 5000 oilfield industrial control network security access unit supports the secure transmission mechanism of servers and devices, supports peer offline password generation, and supports multi-dimensional alarm mechanism. Its functional module design is shown in Fig. 1.

System implementation. After logging in, the console interface is displayed to provide a series of functions such as system status overview, data access trend analysis, device online status analysis, device access status analysis, and alarm status analysis. The data is presented graphically and the data is refreshed in real time.

System Test

Function Test. The main task of the system requirements analysis phase is to conduct thorough investigation and analysis by developers in the early stage of design to accurately understand the specific requirements of users. The system should meet the following requirements: First, the performance requirements, the system should be re-tested and the corresponding measures should

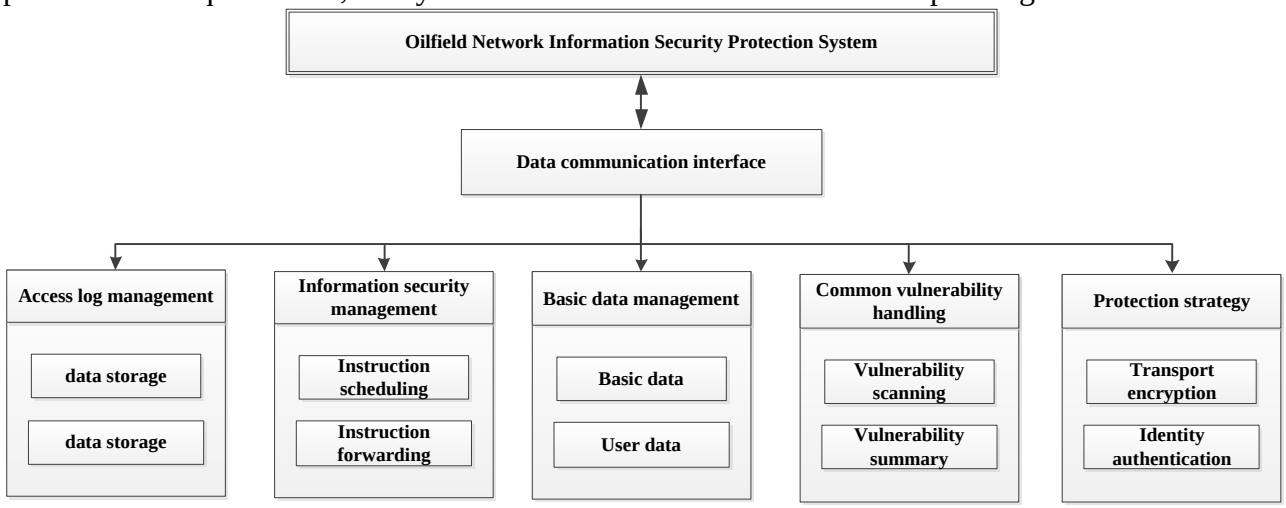

Figure. 1 Functional block diagram of "Oilfield Network Information Security Protection System

be taken in the design and implementation of the front-end and back-end. The second is to meet the ease of use requirements. The goal of ease of use is user-centric, so that users can find the functions and data information they care about most easily, and learn and use them as easily as possible so that users can more effectively finish their work. In addition, there is still a need to meet the needs of scalability, maintainability and interface design friendliness.The results of the testing can be shown in Table1.

Table 1 Equipment testing items and results

Test Items		**Test Results**
User authentication mechanism		Checked
Access guarantee		Checked
Access restriction	User access restrictions	Checked
	Content access restrictions	Checked
Security policy cannot be bypassed		Checked
Compliant encryption operation	Remote management encryption	Checked
	Remote access encryption	Checked
Access control project management	User Management	Checked
	Resource management	Checked
Administrator authentication mechanism		Checked
Administrator privileges		Checked
Log data generation	Use of user authentication mechanism	Checked
Understandable format		Checked
Limit log access	Allow only authorized administrators to access logs	Checked
	Provide tools with the ability to query data	Checked

Hardware Performance Test. Perform hardware performance tests on the system, including Four corner test, temperature test and low temperature cold start test. Among them, the four corner

test links, "oilfield industrial control network security access unit" are respectively powered by -20℃, 231V; -20℃, 209V power supply; 65℃, 231V power supply; 65℃, 209V power supply environment respectively run for 4 hours, the equipment is not There was a crash or restart and there was no interruption in the business. The equipment was cycled at 220V, -40℃~65C in 8h cycle for 48 hours. The equipment did not crash or restart , and the service did not interrupt. The device is powered off and left in the -40℃ environment for 2 hours. It is powered on and can be started successfully. The experiment was carried out 3 times in the same condition, and all of them were successfully started.

Long-term Stability Test. The system protects against RTU, IPC and PLC devices. Turn on the protection policy to run, without any impact on the network function. As of this writing, it has been running for more than 4 months. The data of RTU, IPC and PLC devices in the network are transmitted normally. No interruptions are made. Occasionally, the protection strategy is still in effect, and the risk equipment can be identified normally and content can be blocked.

Self-safety Test. To ensure that the product itself does not introduce new risks to the network, separate hardware and software platforms are tested for security. At the same time, the system visited the network vulnerability scanner and the web application vulnerability scanner, and no risk vulnerability was found in the scan results.

Summary

In view of the network architecture and security requirements of the industrial control system involved in the construction of “smart oil fields”, this paper specifically studies the protection equipment by studying the characteristics of the industrial control network that needs to be protected, combined with the relevant standards and laws and regulations of the industrial safety system proposed by the state. A complete set of oilfield network information security protection system is proposed. In order to complete the above scheme, the demand analysis and overall design of the oilfield industrial control network information security protection system are first carried out. After the requirements analysis and overall design, the system is developed, and finally it has performed functional tests, hardware performance tests and long-term stability tests on the system. The test results show that the proposed solution can solve the existing problems of the oilfield industrial control network, and has certain advantages in terms of functionality, economy and ease of use, which can be further promoted and used.

References

[1] Y. Zhang, D.X. Liu and Q.Y. Tian, et al. Safety Analysis of Industrial Control Network in “Smart Oilfield” [J]. Chemical Engineering Design Communication, 2017, (12): 56-57.

[2] F. Ye. Practice and thinking on the construction of "four modernizations" in oilfield ground engineering [J]. Oil and Gas Field Surface Engineering, 2016, (2): 38-41.

[3] C. Liu. On the construction and achievements of Shengli Oilfield[J].Petrochemical Technology, 2016, (9): 266- 274.

[4] Shore M, Du Y, Zeadally S. A Public‐Private Partnership Model for National Cybersecurity [J]. Policy & Internet, 2012, 3(2):1-23.

[5] Ministry of Industry and Information Technology. Printing and Distributing the Notice on Strengthening Information Security Management of Industrial Control Systems [J]. China Information Security, 2011, (11): 11-16.

[6] W. Li. Improvement of LAN Information Security in Oilfield Production Environment [J]. Silicon Valley, 2014, (12): 156-156, 163.