Information security protection technology of station and depot industrial control system of oil production plant

Tianze Liu

The Sixth Operation Area of the NO.2 Oil Production Plant of Daqing Oilfield Co., LTD. Daqing Heilongjiang 163000, China

Abstract: With the rapid development of Internet technology, as well as the development of informatization and industrialization in oil production enterprises, industrial control system of information security protection technology can make the efficiency improved, but once the invasion by the virus, can cause the control system failure, pressure, temperature, flow, liquid level, such as measuring index will appear problem, chain alarm detection system failure, Or the solenoid valve and power supply of various instruments are not supplied. Once a major hazard source is out of control, it will cause serious accidents and endanger the safety of operators and the ecological environment.

Key words: information security; Industrial control system; Protection technology.

1. Introduction

With the rapid development of industrial information, industrial control system and public network, office network, Internet and other forms of connection, making the industrial control system from a relatively closed, isolated state to the transition of interconnection. As the traditional DCS, PLC, RTU and other industrial control systems are increasingly open, general, standardized, so that the Trojan horse, virus and other security problems in the enterprise's control systems continue to spread. Stuxnet in 2010, Night Dragon in 2011, Duqu, Nitro, and Flame in 2012 all illustrate information security issues in industrial control systems.

2. Current situation and characteristics of information security of industrial control system in oil production plant

2.1 Status quo of information security of station and depot industrial control system of oil production plant

In the early stage, the control system of oil production station is designed for closed special environment, which is only suitable for the production of single machine or process section, and there is no network with the outside world. In the design, implementation and deployment of the system, usability, functionality and real-time as the main indicators, network attack, information security and other aspects are less considered.

With the in-depth combination of computer, network technology, especially information technology and industrialization, industrial control systems increasingly use general protocols, hardware, software, etc., so that their openness is constantly improved, but also under the threat of the following aspects: (1) malware attack; (2) major industrial control processes are destroyed; (3) Improper operation of industrial control data: (4) Illegal access to the function of industrial control system.

At present, most of the industrial control systems used in oil production plants were developed many years ago, and most of them use special software, hardware and communication protocols. They only pay attention to their performance and reliability when designing, but ignore the demand for safety measures. With the application of Internet technology in industrial control system more and more widely. Industrial control systems also have many weaknesses that make them vulnerable to attack. The safety defects of industrial control system and their influencing factors are as follows: the system safety strategy and management system are not perfect; The proliferation of common protocols and applications; No antivirus software is installed on the console of the control system, or the virus library of the antivirus software is not updated in a timely manner. The introduction of general Ethernet technology makes the industrial control network face the threat of Ethernet communication. Many hardware platforms that use Windows PCS as workstations for engineers are as compromised as general PCS.

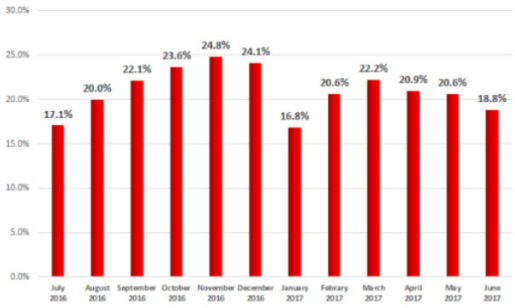

Fig. 1 Safety threat of industrial control system in oil production plant

2.2 Characteristics of station and depot industrial control system of oil production plant

(1) The system has good closure. Industrial control system is an important business subsystem in the management network of oil production enterprises. It involves many important technologies and sensitive information in the production process, so it can only be properly disclosed.
(2) The system needs high ease of use and real-time performance. Industrial control systems must ensure sustainable use. Stability of system access. System characteristics. Safety protection techniques for special industrial control systems. At the same time. Most real-time reaction times are within 1 millisecond [1].
(3) Industrial communication protocol and TCP/IP communication protocol. There are two kinds of protocols in industrial control system, one is industrial control protocol and the other is TCP/IP, when industrial communication protocol and TCP/IP coexist. Some protocols are not designed with security requirements in mind, so security solutions must be targeted.
(4) The safety relationship between the work network and the industrial control system is closely related. With the deep integration of the two industries, more and more information is exchanged between the industrial control production network and the office network, and the interrelation between the two needs higher security.
(5) The system has been maintained for a long time. Industrial control system is closely linked with equipment, production, generally using DCS. DCS. DLL/0 embedded equipment, specifically for site control. In a long-term and stable industrial control system, if there is no certain impact on its normal production, it will not be easily adjusted and changed [2].

3. Demand analysis of industrial control system information security

Information security of industrial control system is a complex system engineering, involving technology, products and systems, but also related to the safety management of enterprises. Compared with traditional IT information security, the information security of industrial control system has its own characteristics. It is mainly reflected in the degree of attention to security. IT security is generally office-specific, starting with confidentiality, integrity, and ease of use.
The goal of safety protection is field DCS, PLC, real-time network communication, industrial control applications, the main features are as follows:
(1) To ensure 24/7/365 availability, continuous operation and access to industrial control systems must be ensured;
(2) Guarantee the operation of the system;
(3) Ensure real-time data transmission;
(4) whether the system and data are complete;
(5) Adopt open standards to achieve tankless communication and functional interaction;
(6) Use common components as the basis for automated solutions;
(7) In order to ensure the real-time monitoring of production, communication between the office network and the production network is not interrupted;
(8) Prevent wrong operation and intentional damage;
(9) Protection of patented technology;
(10) Safety record and change management, etc.
The information security of industrial control system must first ensure the high availability of the system, then the integrity, and then the confidentiality. The main requirements for information security of industrial control systems are as follows:
(1) Improve the design of the project. Construction of the industrial control system is currently underway. In the design of the system, there are also many uncertain security risks, such as: which process equipment needs to be installed separately, which equipment needs to be installed to strengthen the information security of the third party, these are empirical judgments, there is no standard answer.
(2) Improve the design of the whole system. The quality of industrial control system also has advantages and disadvantages. In the early stage of the project, it is necessary to go through a series of design, installation and debugging, which are completed by the supplier. Supplier's technical level and experience. The degree of perfection of the system obtained also varies. The difference in the participation of user engineering designers and related professional and technical personnel will also have a certain impact on the quality of the system and produce certain security risks.
(3) Improve the daily operation and maintenance of equipment. After the completion of the industrial control system, it is necessary to carry out daily maintenance, regular inspection and a series of work to make it continue to play a role. The quality problems of these works will cause the risk of Angin.
(4) Information assurance measures need to be taken. The traditional industrial control system is generally closed, and the function is relatively single. With the advancement of technology. The control system is gradually opening up, making the connection between industrial equipment more convenient. Due to the lack of corresponding security countermeasures against viruses and hackers, it is particularly important to establish systematic information security measures.
(5) New challenges need to be faced. With the acceleration of the two integration process, the emergence of new computer technology and network technology,

industrial control system through a variety of interface technology, the realization of industrial control system network structure. With the new situation of industrial control system information security, it is urgent to formulate industrial control system network planning and specification, in order to ensure the sustainable development of industrial control system.

4. Industrial control system protection strategy construction

4.1 Overall architecture design of defense policies

The protection strategy of the industrial control system of oil production enterprises can be divided into: safety protection of production management, production monitoring and on-site equipment protection; Based on the design ideas of boundary control, host monitoring and internal audit, the multi-level protection of the whole industrial control system is realized. It also unified logs at all levels, analyzed and evaluated the information security situation of the automatic network, realized real-time monitoring of the Internet of Things, and effectively dealt with it [3].

4.2 Security Protection at the Production Management Layer

Three industrial control firewalls are set between the DCS control cabinet and the PC host in three processing stations, and three industrial control firewalls are set between the DCS of three processing stations and the switch of the automation center in the work area. In the SCADA system of the production monitoring center, a set of industrial control firewall is configured, and it is composed of the central control switch. DCS and SCADA systems can be protected in the area to avoid data sensitivity and leakage. By using the whitelist function on the industrial control firewall, you can actively protect the security software or programs in the industrial control network, thus ensuring safety and reliability. The firewall enables abnormal message detection and abnormal traffic detection to implement passive defense and prevent land attacks such as eardrop. ping deah attacks.

4.3 Security Protection on the production monitoring layer

Unified management of all industrial control host protection software clients in the oil production plant, status monitoring of each system, policy allocation and release, collection, summary, update and synchronize the white list data of each independent customer, unified audit of each customer, and data analysis [4].

In industrial control client hosts configured on host protection, and carries on the unification of protection, established a complete set of security maintenance plan, strategy and planning, to strengthen the daily safety training, strict control of process, prevent the internal attack, achieve the purpose of protect the terminal, is not going to solve the technical problem in view of the present, take effective management measures, It effectively improves the safety of the industrial control system. The information security of industrial control system is a dynamic process, it must run through the whole life cycle of industrial control system, and constantly improve and improve.

4.4 Onsite Device layer Security protection

The normal section can be read on a computer without an industrial control system; It can be viewed and used normally only after the host is installed with the industrial control host reinforcement and the corresponding policies are enabled at the same time, so as to achieve "regional exclusivity" [5]. Because of the use of high-density commercial encryption algorithm, it can effectively prevent data leakage. Security USB flash drive and industrial control host enhance the management of mobile storage media and their own security, can effectively prevent Trojan horses, viruses and other intrusions into the artificial control host. To ensure the safety of the industrial control host. Strengthen the management of industrial control medium, it is forbidden to use U disk for data copy and transmission, only use the security U disk for data copy, to prevent the misuse of U disk caused by the virus into the industrial control network and spread, improve the security level.

5. Industrial control system information security protection solutions

Security work of modern industrial control system. Strengthen the construction of the company's security strategy system, strengthen the security awareness of employees, strengthen security protection from different levels, different areas, different functions, different priorities, through the deployment of multifaceted security policies and processes including physical security. Firewalls are configured to protect different security devices. VPN technology is used to enhance communication between devices, patch management, configuration account management, and malware detection and protection to ensure the security of key industrial control processes and applications.

(1) Establish a boundary of physical protection: Physical security is a prerequisite for the information security of the control system. It first ensures that the system is in a controllable physical environment, and then establishes a security isolation system between the enterprise office network and the industrial production network [6].

(2) Safety strategy and procedure: Formulate a complete safety strategy and procedure. Set up the audit system between the industrial control network and the industrial control network, strictly implement the access control of the industrial control network, the operation of the audit engineer workstation,

(3) Set up safety monitoring device. Secure the boundaries of the system; It is divided into different Anjin areas according to its use and communication services, and isolation facilities such as firewalls and security gateways are set up at the junction of Anjin areas.

(4) Use VPN technology for communication protection of each control device: configure VPN in each security device to protect the communication of each unit, ensure the authentication, integrity and confidentiality of the communication, prevent illegal communication.
(5) Strengthening and updating: real-time updating and system strengthening of engineer station and application server. Only vendor-specific protocol data is protected, preventing all communications that do not comply with standards and legal requirements.
(6) Account management: establish industrial control applications, such as DCS, PLC, etc., establish account management, and strengthen the access control of passwords.
(7) Malware protection technology: not only in the industrial control network on the PC host virus monitoring, but also in its entrance to set the antivirus gateway.

6. Conclusion

Industrial control system information security is not only a technical problem, but involves the management process, architecture technology, products and other aspects, the need for management, operators, integrators, component suppliers and other multi-party efforts to improve the information security awareness of all personnel, fully aware of the importance of information security. To ensure the safe operation of industrial control system, it is necessary to continue to improve it.

References

1. Wu Jun, Zhang Xinzheng, Li Jun, et al. Research and application of information security protection technology for station and depot Industrial control System of Oil production Plant [J]. China Management Information Technology,2015,18(19):91-93.
2. YAO Xiangzhen, Zhao Zitong, ZHOU Ruikang, et al. Interpretation of National Standard of Information Security Technology Industrial Control System Information Security Protection Capability Maturity Model [J]. Automation Expo, 222,39(7):48-52.
3. NI Min, Fan Jing, Li Chenguang, et al. Review on Information Security Protection Technology of Industrial Control System [J]. Journal of Yunnan Minzu University (Natural Science Edition),2020,29(6):619-627.
4. TAN Xinzhang. Research on Information Security Protection Technology of Industrial Control System [J]. Computer Programming Skills and Maintenance, 2019(7):145-146,165.
5. LIU Yong. Research on network protection technology of industrial control system information security [J]. Digital User,2019,25(34):53.
6. Zhu Shishun, Huang Yibin, Zhu Yingfei, et al. Research on Key Technologies of Industrial Control System Information Security Protection [J]. Electric Power Information and Communication Technology, 2013,11(11):106-109.