Creative Economy
2024, VOL. 8, NO. 2, 18-26
DOI: 10.47297/wspceWSP2516-251902.20240802

Introduction to the Design of Security Isolation and Protection Program for Industrial Control Network

Siyang Li

Petro-CyberWorks Information Technology Company Limited, Beijing 100007

ABSTRACT
At present, the status of the digital economy in the economy of all countries is increasing, and the acceleration of the digitization process has brought about various hidden concerns. In the industrial field, a variety of information security incidents occur frequently, and the problem of industrial control systems is becoming increasingly prominent. Based on this problem, this paper proposes a set of industrial control security system design program, and introduces the industrial control information security control subsystem mainly composed of industrial control information security control platform, industrial control security digital mining gateway, industrial control firewall three products, in order to the industrial control system related to the national economy and people's livelihood to reduce the network vulnerability, platform vulnerability, management vulnerability to ensure that the industrial control system is healthy and stable operation, and to defend the national security.

KEYWORDS
Industrial control network; security isolation; information security; industrial control security; industrial control firewall

1 Overview

At present, the status of digital economy in the economy of all countries is increasing, and the acceleration of the digitalization process also brings various hidden worries. In the industrial field, various information security incidents occur frequently, and the problem of Industrial Control System (ICS) is becoming more and more prominent. Based on this, the Ministry of Industry and Information Technology (MIIT) issued the Notice on Strengthening the Information Security Management of Industrial Control Systems in September 2011, requiring the effective strengthening of the security management of ICS; the National Development and Reform Commission (NDRC) issued the Notice on Matters Related to the Organization and Implementation of the National Information Security Special Project in 2013 in August 2013, which requires the establishment of a security detection mechanism for industrial control systems in the nationally important fields, reduction of vulnerabilities, enhancement of security protection level.

2 Status quo and problems

Industrial enterprises continue to promote the process of information technology, not only to bring efficient management and convenience, but also bring certain security risks(Sattarov, S. B. , Adilov, F. , & Ivanyan, A. 2015). Among them, industrial control network security is the most

important, but also the focus of this paper. Through the petrochemical enterprise industrial control system network on-site research, the author mainly found the following aspects of the problem need to be resolved:

(1) the lack of border protection technology: in the control network and information network interconnection, due to information systems, information security requirements are far lower than the control system, information systems security will directly affect the safety of the control system, therefore, the border between the two networks to protect the control system has become the focus of the information security defense 2.

(2) A single type of isolation equipment can not guarantee the effective isolation of the border between the two networks: due to the variety of communication services connected to the two networks, the use of a single isolation device can not meet the diverse requirements of network communication and security isolation, and it is difficult to guarantee the effectiveness of network isolation.

(3) The overall information security situation and network communication at the border of the two networks is missing: the two network connections and isolation equipment scattered throughout the plant can not be centralized and unified to show the whole picture of the industrial control network, the monitoring and management of the two network isolation equipment, security policy unification, network communication status monitoring is often missing, and can not grasp the overall information security situation.

3 Program design scope and principles

3.1 Program design basis

According to the relevant national and industry standards, and combined with the actual situation of petrochemical enterprises, this paper proposes the main reference basis for the design of industrial control security programs include: GB-T 26335-2010 Specification for Information Technology Integration Systems in Industrial Enterprises, GB-T 26333-2010 Specification for Security Risk Assessment of Industrial Control Networks, Guidelines for Industrial Control System Security (NIST-SP800 -82), IEC TS 62443-1-1-2009, IEC TR 62443-3-1-2009. In the face of network viruses, malware invasion, illegal access and other potential threats, a single means of network protection is no longer able to effectively deal with the increasingly complex network security situation. Therefore, it is necessary to create a set of defense-in-depth architecture based on multiple security measures for industrial control systems(Kim, S. , et al, 2019). According to Figure 1, it includes the use of firewalls, quarantine zones, and incident response mechanisms so that it can continuously meet the needs of technological development and business development.

3.2 Program design scope

Selecting security isolation equipment with independent intellectual property rights, designing and deploying the industrial control information security control system suitable for the actual needs of enterprises without affecting the operation of industrial control systems, dividing the security area, constructing the security data exchange area, isolating the control system, eliminating the security risks of industrial control systems due to data collection, realizing the security data collection, eliminating the dissemination of information security threats through the network, and guaranteeing the safe and stable operation of the device(Wu, Y. D. , et al. 2016). Safe and stable operation of the device

1) Use industrial control firewall to isolate the control network and management network, divide

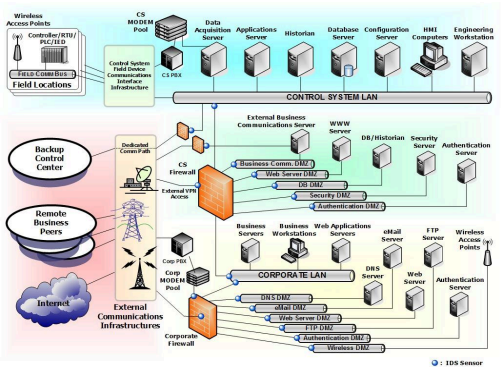

Figure 1 Defense in depth architecture

reasonable security areas, and formulate strict access policies. At the same time, it links with the control platform for control and warning functions.

2) Use the security data collection gateway with independent intellectual property rights to replace the existing buffer machine (ordinary PC) and other collection devices to realize protocol-level security agent and security data collection functions. It protects against industrial control viruses and intrusions, and links with the security control platform for control and warning.

3) Build an all-round industrial control information security control platform to provide services such as device configuration management, real-time monitoring, authorization management, authentication management and log management, effectively monitor operations and warn of illegal behavior. For industrial control system information security events to achieve visualization and control.

3.3 Program Design Ideas

A perfect industrial control system security defense system should include a security management system and technical product system(Zhang, X. , et al, 2019). From the management and technology to strengthen the company's industrial control network security protection level, two-pronged approach to prevent the control system from virus infection, to prevent the control system from being attacked leading to unplanned stopping of production equipment or even casualties and other catastrophic accidents, to ensure that the device is long, stable and excellent operation.

3.4 Program design principles

1) Moderate protection and grasp key defense points. According to the construction requirements of the system, combined with the security requirements of each part of the hardware and software in the system and the deployment scheme of each component in the whole system, the security design will be specifically implemented to the network, hosts, applications, auditing, management and other aspects, to find the key control points at all levels, and to enhance the security of the system construction.

2) Reasonable use of existing resources, saving security construction investment. Maximize the use of the project implementation scope of the enterprise's existing security-related hardware and software and network status quo resources, effective use of existing resources. From the overall consideration of network and application level security protection.

3) While preventing external threats, focus on regulating the behavior of internal personnel and strengthening access control, monitoring and auditing capabilities.

3.5 Program Design Objectives

The security objectives proposed in this paper are: through the analysis of network structure and network security risks, implement industrial control network security construction for the security of data communication between different regions and the overall informatization construction requirements, implement reliable border security equipment and strategies for the key areas of DCS network management, and realize a hierarchical deep security defense strategy to resist various known attack threats.

4 Program Design

4.1 System Design

4.1.1 Industrial control network security program

This program is a four-layer architecture - enterprise management layer, security interaction layer, control network layer and field control layer. Among them, the self-developed security data acquisition gateway can realize protocol-level security agent and security data acquisition, deployed between industrial control information network and enterprise management network for effective security protection; the security isolation gateway divides the DMZ (Demilitarized Zone), formulates strict access control policy, and designs man-machine friendly interface for the control platform to realize security and control visualization. management and control visualization.

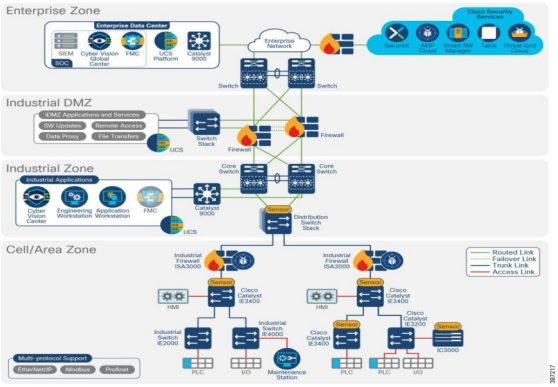

Figure 2 System Architecture Diagram

4.1.2 Access control program

1) The control platform realizes access control by means of permission authentication;

2) The access control between the control platform and the communication platform, and between the communication platform and the secure digital mining gateway is carried out in the way of "deny all, allow specific", which only allows specific IP addresses and specific ports to communicate;

3) Physical isolation is realized between the management network and control network through the secure digital mining gateway, rejecting all attacks or illegal access from the management network to the control network.

4.1.3 System Rights Design

The user authority management design is used for unified management of users accessing the

system, including information such as user's name, phone number, organization to which he/she belongs, and authority to access the system. Unauthorized users cannot log into the system, and different users have different permissions.

l Organization Management

The system administrator creates the corresponding organization structure according to the actual departmental units, and can maintain the organization structure, including new construction, modification and deletion.

l Role Management

The system administrator creates system roles and enters user details, including real name, phone number, and position. Assign one or more roles to users and assign different usage rights. For example, the Chemical Department Operation and Maintenance role is created, which only allows viewing of safety information of the relevant devices in the Chemical Department;

l Permission Assignment and Verification

Users with different roles in the same department have different permissions. Users log in to the information monitoring system using their respective user names and passwords. After logging into the information system, personnel with different identities can only use authorized functions. This restriction of operation authority management ensures that personnel have their own responsibilities and do not interfere with each other.

4.2 Industrial Control Network Security Products

4.2.1 System Function Design

The functional structure of this subsystem is shown in the following figure:

As can be seen from the above figure, this sub-system is mainly composed of three products:

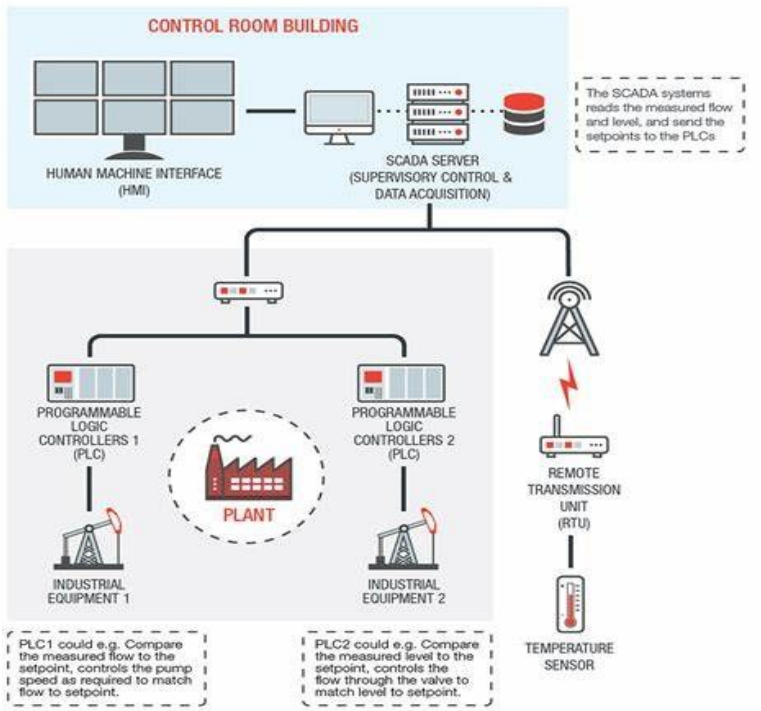

Figure 3 Functional structure of industrial control information security control system

industrial control information security control platform, industrial control security digital mining gateway and industrial control firewall, and the detailed functions of each product are described as follows.

4.2.2 Industrial Control Information Security Control Platform

The main functions of the industrial control information security management and control platform include: general view, assets, policy, monitoring, alarm, log, and seven system modules, as shown in the following figure:

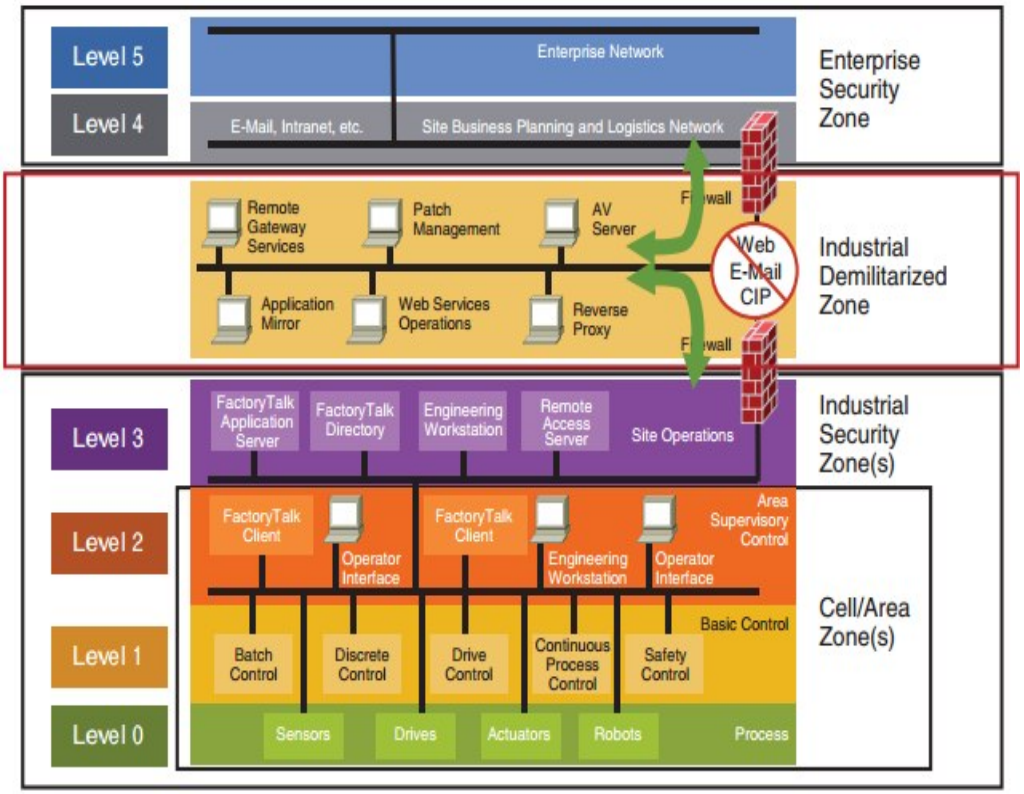

Figure 4 Functional diagram of industrial control information security control platform

4.2.3 Industrial Control Information Security Digital Acquisition Gateway

Secure Digital Mining Gateway is a professional information security equipment used to control system network boundary and carry out application-level information security protection for real-time data collection. By embedding OPC, MODBUS and other industrial control protocol modules to complete the real-time data collection application agent, so as to effectively isolate the management network and control network, so that the information security threats in the management network can not be spread to the control network, to ensure the stable operation of the control system. The hardware of the secure digital mining gateway adopts industrial-grade design, and has the function of automatic recovery from power failure, network disconnection and other abnormal states to ensure the stable and reliable operation of the equipment.

Secure digital mining gateway mainly includes: data acquisition, data caching, data forwarding, status monitoring, clock synchronization, task management, firewall, authentication, hardware

watchdog and other ten major functions. The figure below:

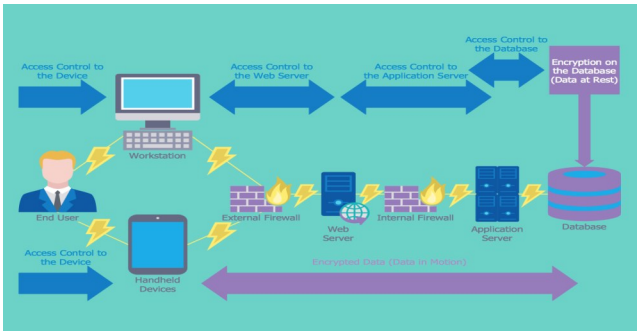

Figure 5 Secure Digital Mining Network Management Function Diagram

4.2.4 Industrial Control Security Firewall

Centralized monitoring of the company's industrial control network security status, comprehensive and centralized information and convenient management, through a platform can monitor the company's industrial control security status. The industrial control security firewall can identify and analyze industrial control protocols, whitelist access control and network attack protection. Secure digital procurement gateway integrates security protection and data collection functions, which can replace the BUFFER machine for data collection and forwarding, and achieve isolation of a single set of production equipment.

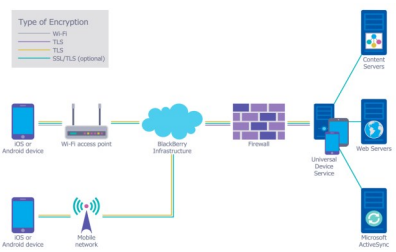

Figure 6 Functional diagram of security isolation gateway

Isolation gateway should be on the basis of packet filtering, through the use of special hardware devices to achieve isolation between host and host, host and network, network and network, with a combination of soft and hard data flow control, connection direction control, three-dimensional control of multi-level access, with a high-intensity defense function, the use of no IP address transparent listening to the work mode, with network address translation function. At the same time, it provides flexible management in GUI mode and rich monitoring tools, which can conveniently configure security policy, user management, real-time monitoring, log collection and other operations on the device, and realize gateway anti-virus, intrusion monitoring and defense (IPS), traffic control (QoS) and other functions, and at the same time, it is able to support industrial control protocol detection and attack defense, and can recognize a variety of industrial control protocols, and can realize both monitoring and blocking operations.

Through the establishment of industrial control security firewall, the physical architecture can realize the safe collection of one-way production data; the formation of longitudinal defense between the enterprise operation and management network and the industrial network; and the comprehensive display and monitoring of viruses, attacks, data traffic and logs at the border of the industrial network.

4.3 Security Design

Industrial control information security is heavier than Mount Tai, there must be necessary initiatives to ensure the smooth and safe operation of the system. In order to prevent the office network virus infection to the control network, we use self-developed security data acquisition gateway as a dedicated data acquisition equipment, security data acquisition gateway using embedded Linux operating system, the system disk is set to write-protected, and port restrictions. Thus, this paper puts forward security measures from three aspects: industrial control protocol detection, security isolation, and authority control, to help enterprises to produce safely:

(1) Industrial Control Protocol Detection

Isolation firewall can recognize a variety of industrial control protocols, including Modbus communication protocol, DNP3, EtherCAT (Ethernet for Control Automation Technology), Elcom and so on. The firewall also has built-in decoders for commonly used industrial control protocols and a variety of vulnerability defense feature libraries to monitor transmission commands and block erroneous commands, in order to defend against attacks brought by these protocols.

2) Security isolation

In view of the fact that malicious programs and viruses can be easily spread through the Internet, the program ensures system security by physically isolating the control network and management network and combining virus firewalls and other measures.

3）Authority control

You must enter the account number and password to log in to the system, and users with different roles in the same department have different permissions. Users use their respective user names and passwords to log in the information monitoring system. Different identities of the personnel in the information system after logging in, can only use the authorized functions, this operation authority management restrictions, to ensure that the personnel of their respective responsibilities, do not interfere with each other. For example, users of methanol plant cannot view the production information of olefin plant.

4.4 Standardization

Although the industrial control security problems faced by each enterprise are similar, the specific implementation process is still very different. In order to efficiently implement and operate and maintain, it is imperative to establish a set of standardized technology and operating procedures. In the implementation process to follow the production enterprise industrial control information security implementation standards, can greatly facilitate the later operation and maintenance and integration with other systems.

(1) Data Acquisition System Technical Standards

The interface of the data acquisition system with the DCS of the device will be designed and developed by adopting the OPC protocol of the international industrial standard, and the timeliness and stability of the interface will be fully considered.

(2) Technical standards of selected products

The design idea and technology of safety data acquisition gateway draws on and absorbs the U.S. SP-800 standard, and strictly abides by the relevant domestic industry standard technology.

(3) System coding standards

In terms of system coding, the standard coding system will be adopted, so that on the one hand, the system coding system can be standardized, and on the other hand, the integration with other systems using standard codes can be well realized. For those that are not covered by the current standard code but can be standardized, they will apply for coding to the standardized coding group.

(4) Quality Management

5 Conclusion

In the increasingly complex international situation, industrial control security issues are becoming more and more prominent(Gaofeng, A. , et al, 2018). By sorting out the current status quo of industrial control network security in China and the main problems that exist, this paper proposes a set of industrial control security system design program and introduces the industrial control information security control subsystem mainly composed of industrial control information security control platform, industrial control security digital mining gateway, industrial control firewalls and three products, in order to reduce the network vulnerability, platform vulnerability, management vulnerability of industrial control systems in the field of national economy and people's livelihoods to ensure the healthy and stable operation of industrial control systems and safeguard the national economy and people's livelihoods. Control system to reduce network vulnerabilities, platform vulnerabilities, management vulnerabilities, to ensure the healthy and stable operation of industrial control systems, to safeguard national security, to achieve independent property rights of industrial control security protection products, technological innovation, protection and high degree of standardization, to achieve the safe collection of unidirectional production data from the physical structure, to form a deep defense at the border of the industrial control network, and to effectively guarantee the isolation of two network boundaries within the petrochemical and the efficient and smooth operation of the industrial digital mining network.

Funding

Implementing project quality management and adopting ISO9000-3 standard for quality management of projects and sub-projects.

References

[1] Gaofeng A. , Changming Z. , Xiaofeng L. , & Yanan L. . (2018). Information security policy and standard system of industrial control system in china. Journal of Information Security Research.

[2] Kim S. , Kim S. M. , Nam K. H. , Kim S. , & Kwon K. H. . (2019). Security Information and Event Management Model Based on Defense-in-Depth Strategy for Vital Digital Assets in Nuclear Facilities. International, Conference on Computer Science and its Applications; International Conference on Ubiquitous Information Technologies and Applications.

[3] Sattarov S. B. , Adilov F. , & Ivanyan A. . (2015). Creation of integrated of industrial security with the use of modern information technology. J. Multim. Inf. Syst., 2, 281-286.

[4] Wu Y. D. , Wang Y. , Li Z. , Jiang Y. , Huang B. , & Chen Q. J. , et al. (2016). Research on high-performance passive optoelectronic materials and devices.

[5] Zhang X. , Cai X. , Wang C. , Han K. , & Zhang S. . (2019). A Dynamic Security Control Architecture for Industrial Cyber-Physical System. 2019 IEEE International Conference on Industrial Internet (ICII). IEEE.