Research on Information Security Protected Scheme for Ship Network System

Feifei Song¹, Jun Zhu², Siyuan Guo³*
¹Kangda College of Nanjing Medical University, Lianyungang, Jiangsu Province, 222000, China
² China Shipbuilding Heavy Industry Information Technology Co., Ltd., Lianyungang, Jiangsu Province, 222000, China
³ College of Science, Inner Mongolia University of Technology, Hohhot HET, Inner Mongolia Autonomous Region, 010000, China
*Corresponding author’s e-mail: m18247178113@163.com

Abstract. Based on the investigation of the current situation of ship automation system construction and ship computer network architecture, the status and requirements of ship computer network information security are studied and analyzed. Ship safety management objectives are set, and the principle of network system security configuration is proposed. Furthermore, the evolution process of network security management is clarified, so as to establish and improve the ship network security management system. Finally, according to all the above analysis and research, the construction plan of information security protected for ship industrial system is determined.

1. Introduction
As an important means of transportation in China, shipping is related to the economic development and foreign trade. Recent years, with the development of China's economy and the improvement of technical level, the overall quality and tonnage of ships have also increased. For crossing vast oceans, more advanced technologies are needed as a guarantee, especially for ship network systems. The shipbuilding industry is an important support for China's implementation of the maritime power and the "One Belt, One Road" strategy. In the transformation and upgrading of the shipbuilding industry, the construction of the industrial Internet is significant, especially to improve the industrial security protected capability. The software and hardware core equipment of the industrial control system in shipping is a little low, and the safety protected capability system has to be perfected[1]. The study of safety protected theory is helpful of technology upgrade and industry development. Therefore, this paper proposed a information security protected construction scheme for computer network system.

2. Construction status of ship industrial control system

2.1. Status of ship automation system construction
With the continuous improvement of ship automation and information, ship computer network systems and their applications have developed rapidly. The traditional navigational fishery resources acoustic monitoring method is inefficient and difficult to expand, so the wireless distributed fishery resource acoustic monitoring system is designed. The system consists of a number of distributed monitoring
The ship management information system database server is connected to the mail server and the crew's mail to synchronize the data of the ship and shore ship database. Information system exchanges data with the shore software to enable clients to use ship management information systems [6]. The ship management uses the ship information system on board. The client/server architecture is used by most shipboard systems to realize ship information management, ocean planning.

2.2. Ship computer network architecture
At present, industrial Ethernet is widely used in ships [5], and a dual-ring fiber backbone network is constructed by using industrial Ethernet and switches. The A and B network of the dual ring network include one three-layer switch and two second-layer switches. The Layer 3 switches of the A network and the B network are interconnected by Gigabit optical cables, and the Layer 2 switches in the network are interconnected by 100M optical cables. When the fiber loop fails, the network can be self-healing within 300 ms, and the real-time data of each subsystem will not be lost. Among them, four important subsystems, such as maneuvering, ship, power, and navigation, use the two-way Gigabit Ethernet interface on the host of each engineering console to access the Gigabit access network of the backbone ring network A and B network in dual-link mode to achieve mutual communication and integration between subsystems, while ensuring the reliability of subsystem services. The information signage is a general system. It uses a 1-way Gigabit Ethernet interface to connect to the 1000M/100M Ethernet port of the A or B network in a single link. The server and device simulator also pass the 2-way Gigabit Ethernet. The interface accesses the backbone network in dual link mode. The subsystems connected to the backbone network are functionally independent of each other and convenient for management, the backbone network is divided into different VLANs, and each subsystem runs in a different VLAN which are interconnected through routing. The IP of the devices in the backbone network can be uniformly planned.

3. Ship computer network information security status and needs analysis
In order to realize ship information management, ocean-going vessels install ship-based software which uses the ship information system on board. The client/server architecture is used by most shipboard software to enable clients to use ship management information systems [6]. The ship management information system exchanges data with the shore-based ship management information system via e-mail to synchronize the data of the ship and shore database.

At present, the security and availability can not meet the basic requirements for operation and use. The ship management information system database server is connected to the mail server and the crew's
office computer, usually on account of the computer virus cannot communicate. Because the ship office computer adopts the Microsoft operating system, neither the patch nor the effective anti-virus measures are taken. Even if some ships install the stand-alone version or the network version of the anti-virus software, they cannot upgrade the anti-virus software and update the virus database in time. Killing new viruses or new variant viruses can cause the anti-virus effect to fail.

On the computer in the ship's local area network, a storage medium such as a CD-ROM with a virus, a USB flash drive, a mobile hard disk, a computer with a virus is connected to a local area network on the ship or a wireless network card installed on a computer in the local area network. Introducing viruses, worms, Trojans, malicious code, etc. through wireless Internet access, these are the starring source of ship computer viruses [7]. Therefore, in order to solve this problem, the commonly adopted solutions are: installing a hard disk protection card on the ship office computer, installing "one button recovery" software on the ship office computer, and installing and deploying a professional security management system in the ship computer network system. Software and network version of anti-virus software, can not fundamentally solve the problem.

The information security requirements of ship computer network systems require strong availability of ship computer networks. No matter the hardware or software, any component of the system fails, and the entire network system is not paralyzed. The hidden layer, it is essential to enhance the reliability, recoverability and maintainability of the ship computer network system. To study and solve the problem of security management, we must consider the actual conditions and implementation cost of the ship computer network system. The solution should be simple, easy to implement, economical, practical, mature, and maintain conveniently.

4. Ship computer network system information security construction

4.1. Ship network system security management objectives

Aiming at the analysis of ship computer network system security problems and availability requirements, it is the cornerstone of ship network system security management to establish a set of effective and feasible ship computer network system management system. Through the development of the ship computer network system security management system, security policy and security management framework, a custom security management system are developed and deployed which suitable for the characteristics of the ship computer network system, to ensure the safe and reliable operation and controlled use of the ship computer network system. Furthermore, the needs of the normal operation, business operation and daily management of the ship management information system can be realized. In general, consider from five aspects:

- For the management-level security, a ship computer network system security management system is established, and the safe operation management and maintenance of the network system are realized through actual implementation and assessment.
- For application-level security, the management of anti-virus and anti-attack of ship computer network are strengthened, backing up related data, encrypting part of data, adopting identity authentication and appropriate security software and hardware, and establishing a sound security protection system [8] [9].
- For the whole system-level security, it is necessary to continuously strengthen the monitoring of the operation for the server, operating system and database, and strengthen the management of the system patch, to ensure the operation of the core system through the form of two systems, and to provide the backup system and recovery in time when a failure occurs.
- For network-level security, to ensure the stable operation of the ship computer network equipment and network lines, the two-way redundancy are provided for the network equipment and lines at the core layer.
- For physical-level security, to ensure the security of the ship computer network system data and timely recovery of the system, the information and data must backup and the management of various software media be strengthened.
4.2. Safety configuration of the ship network system

When the ship network system is safely configured, it should be analyzed and designed according to the actual computer network system. The need is security configuration, but because the system is small, simple, mobile, and lacks professional security managers and professional security managers. Therefore, the safety configuration adopted should ensure the basic operation and ease of management and maintenance under the premise of ensuring the function and performance of the ship computer network system. The threats or risks that the system may encounter should be fully considered, and qualitative and quantitative analysis to develop norms and measures for the balance of needs, risks and costs. Considering the change or expansion of future demand, the ship computer network security management system must be modular, flexible in configuration, good in scalability and adaptable.

Although the ship network system is small in scale, its position is unstable and the number of ships is large. It is a complicated project to safely configure the ship computer network from each level of the network system and every stage of security prevention. It is necessary to consider the realization of technology, as well as to develop specific security measures such as management systems, professional technical measures and administrative laws, and strictly implement and implement them.

In order to expand, upgrade and centralize the safety management system of the ship computer network system, while rationally planning, constructing a new network security system or investing in new network security facilities, the existing network security system should adopt a comprehensive and integrated approach for security configuration standardized and step-by-step. Limited to the historical reasons for the development of computer system security theory and technology and the financial capacity of the enterprise itself, it is necessary to build some overall or regional security technology systems and allocate corresponding facilities to protect investment in different situations.

To establish and improve the ship computer network system security management system, the process method of PDCA should be followed [10] [11]. The management structure should be based on the entire network security management system, from the management level of the system, through the analysis of ship's information assets, risk analysis and evaluation, network security requirements analysis, security strategy development, security system design, standard specification development, and selection of security control. Steps such as measures to propose a security solution.

5. Calculation of network system information security construction plan

For the safety assurance of ship computers and network systems, it is necessary to combine the actual situation with the technical means and the constraints of the system. The development of relevant systems should include the following:

- In order to explain the overall objectives, scope, guidelines, principles, and responsibilities of the organization's safety work, the overall guidelines, policy documents, and security policies for the safety of ship computers and network systems are formulated.
- A safety management system is established for regulating safety management activities and restricting the behavior of personnel.
- In order to require managers or operators to perform routine management operations and prevent operational errors, operational procedures should be established.

In general, a comprehensive information security management system consisting of security policies, security policies, management systems, and operational procedures are formed. The safety management teams regularly organize relevant departments and relevant personnel to verify the rationality and applicability of the safety management system.

This paper establishes a deep safety protection system for the whole life cycle of the industrial control system. Under the premise of ensuring the availability of the industrial control system, the safety control system is constructed for the industrial control system to achieve vertical stratification, horizontal zoning, boundary control and internal monitoring. Vertical stratification is divided into four layers for the vertical direction of the industrial control system: field equipment layer, field control layer, supervisory control layer, and production management. Horizontal partitioning means that the subsystems of each industrial control system should be isolated from the network and in different security zones. Boundary
control is to perform boundary protection and admission control for each subsystem boundary, that is, each operation station, industrial control system connection, wireless network, etc. Internal monitoring is the problem of monitoring network traffic data within the industrial control system to detect intrusions, business anomalies, abnormal access relationships, and abnormal traffic.

The main security threats to the industrial control system of the shipbuilding industry come from hacker attacks, malicious code, unauthorized access, mobile media, weak passwords, operating system vulnerabilities, misuse and business anomalies. Therefore, its security protection should be improved and enhanced in the following aspects: intrusion detection and prevention, malicious code protection, detection of abnormal behavior of internal networks, border access control and system access control strategies, safety of industrial control system development and maintenance, identity and behavioral auditing, account uniqueness and password security, especially the management of administrator accounts and passwords, and the tag, access control, auditing of removable storage media.

The network information security protected system is established, mainly for border security protection and network traffic security audit for each subsystem, and terminal security protection for each operation station. For the ship's fiber ring network to carry out security protection, access control is implemented for the ring network entrance and exit boundary, and abnormal traffics are monitored and audited inside the network. Trojan worm infection are prevented form entering the industrial control network, and network abnormal behaviors are discover in time. The overall security design of the ship computer network system is shown in Figure 1.
Overall Network Safety Design Scheme

| ERP/ME | PDM/CA | CAPP System | DNC System | SCADA System |
|--------|--------|-------------|------------|--------------|
| Order  | Design | Process     | Production | Run          |

Industrial control information security technology system

- **Operation station safety**
  - Access control
  - Data encryption
  - Patch management
  - Baseline configuration
  - Data storage security

- **Application and data security**
  - Data backup and recovery
  - Access control
  - Data confidentiality
  - Software fault tolerance
  - Resource control
  - Data integrity
  - Communication integrity
  - Security audit
  - Identification

- **Industrial network security**
  - Structure safety
  - Security audit
  - Network equipment protection
  - Malicious code prevention

- **Field equipment safety**
  - Machine access control
  - Machine to reinforce
  - Machine isolation

- **Boundary integrity check**

- **Organization and personnel safety management**
  - Operation maintenance management
  - Upgrade management
  - Connection management
  - Configuration management
  - Data security management
  - Data collection
  - Data transfer
  - Data audit

Figure 1. Overall network safety protected design scheme of ship industrial system

6. Conclusion
According to the survey of ship automation system construction, ship computer network architecture and ship computer network information security status, a high-level computer network information security protection scheme is proposed to fully enhance the reliability, recoverability and maintainability of computer network including configuring redundant network devices and building alternate network lines. The information security protection scheme for the computer network system shall be deployed according to the specific status of the ship. For older ships that do not have a computer LAN, it is important to address the anti-virus issues of the ship information system server or stand-alone machine to ensure operating normally.
References

[1] WANG J, ZHU QJ. (2017) Autonomous Controllable Computer Conference Held in Beijing. Computer Engineering and Design, 2017,38(10):289-292.
[2] WANG D, SI JF. (2017) Wireless distributed acoustics monitoring system for fishery resources. Computer Engineering and Design, 2017,38(7):1951-1955.
[3] XU JH, Liu GK, Liu DN. (2018) Application of Ship Management Information System in Crew Management. China Water Transport, 2018(10):33-34
[4] SUN N, LI J. (2017) Analysis of Technology Development Trend and Standard System Framework for Ship Intelligent Manufacturing. China Standardization, 2017(3):44-47
[5] HAO XJ. Analysis of Real-time Communication Technology for Industrial Ethernet. Modern Industrial Economy and Informationization, 2018(12):90-91
[6] JIANG Z, LIU H, XIANG XB. (2015) Wireless Network Monitoring System for Ship Power Station Based on C/S Architecture. Shipbuilding of China, 2015(4):179-187
[7] WANG YM, WU CK, LI DH. (2018) Monitoring method for cross operation system of ship complex LAN. Ship Science and Technology, 2018(10X):25-27
[8] HAN R. (2018) Design of encrypted communication system for naval vessels. Ship Science and Technology, 2018(11X):139-141
[9] LI C, LEI L. (2018) Analysis of patent technology for dynamic password authentication. Technology Innovation and Application, 2018(24):36-37
[10] ZHANG Q. (2017) Application of PDCA in management system. Wireless Internet Technology, 2017(19):125-126
[11] SAI YJ, FENG ZJ. (2018) Information security for industrial control systems. ELECTRONIC TECHNOLOGY & SOFTWARE ENGINEERING, 2018(17)207-209