GUIDANCE NOTES
GD014-2024

CHINA CLASSIFICATION SOCIETY

GUIDELINES FOR SHIP CYBER SECURITY

2024

Effective from 15 July 2024

Beijing

CONTENTS

Chapter 1 General

Section 1 General Provisions

1.1.1 Application

1.1.1.1 The Guidelines for Ship Cyber Security (hereinafter referred to as "the Guidelines") apply to any ship, subject to either requirement or its own intention, applying for ship cyber security class notation of China Classification Society (CCS) and any Computer Based System (CBS) applying for its cyber security assessment, and are provided for reference for offshore installations.

1.1.1.2 The Guidelines specify the cyber security requirements for ships and on-board CBSs.

1.1.1.3 The on-board CBSs to which the requirements herein apply are the on-board Operation Technology (OT) systems using data to monitor or control physical processes of ships and devices that may be vulnerable to cyber incidents and, if compromised, could lead to dangerous situations for human safety, safety of the ship and/or threat to the environment. These CBSs include but are not limited to:

(1) Propulsion system;

(2) Steering system;

(3) Anchoring and mooring system;

(4) Electrical power generation and distribution system;

(5) Fire detection and extinguishing systems;

(6) Bilge and ballast water systems, loading/unloading control systems, loading computer system;

(7) Watertight integrity and flooding detection system;

(8) Lighting (e.g. emergency lighting and low-location lighting and navigation signal systems);

(9) Any other CBS system whose disruption or functional impairment may pose risks to ship operations (e.g. emergency distruption system, cargo safety system, pressure container safety system, gas detection system, etc.);

(10) Navigation system required by the Rules;

(11) Internal and external communication system required by CCS Rules and Regulations.

1.1.1.4 Systems connecting with those refered to in 1.1.1.3 via Internet Protocol (IP)are to meet the requirements of the Guidelines. Such as:

(1) Passenger or visitor servicing and management systems;

(2) Passenger-facing networks;

(3) Office administrative networks;

(4) Crew entertainment systems;

(5) Any other systems connected to OT systems, either permanently or temporarily (e.g. during maintenance).

1.1.1.5 For navigation and radiocommunication systems required by the Rules or CCS requirements, standard such as IEC 61162-460 or other equivalent standards can be used as an alternative to the Guidelines. When such systems are installed and arranged onboard ships, requirements related to SL0 as stipulated in Chapter 4 section 3 of the Guidelines shall be complied.

1.1.1.6 The requirements of the Guidelines may also be available for reference for the CBSs not covered in 1.1.1.3-1.1.1.6.

1.1.1.7 The networks considered in the Guidelines consist of the applicable systems and the networks supporting their stable, secure and reliable operations, including computing, security, storage, communication and network devices.

1.1.2 Basic Cyber Security Requirements for ships and on-board CBSs

1.1.2.1 The following ships under construction contracts entered into on or after 1 July 2024 are required to meet at least the relevant requirements corresponding to SL0 in Section 3 of Chapter 4 of the Guidelines:

(1) Passenger ships engaged in international voyage (including hige-speed passenger ships);

(2) Cargo ships of 500gt and above engaged in international voyage;

(3) High-speed ships of 500gt and above engaged in international voyage;

(4) Offshore mobile drilling platform of 500gt and above;

(5) Other self-navigation offshore mobile platforms (e.g. offshore wind turbines, lifting platforms, drilling support platforms, residential platforms, etc.).

1.1.2.2 In addition to the ships specified in 1.1.2.1, ships engaged in domestic voyage and other ships engaged in international voyage may apply voluntarily to meet the relevant requirements of the Guidelines, such as:

(1) Military ships and troop transport ships;

(2) Cargo ships under 500gt;

(3) Non-motor ships;

(4) Primitive wooden ships;

(5) Passenger yachts (not more than 12 people);

(6) Non-business yacht;

(7) Fishing vessels;

(8) Specific offshore installations (e.g. FPSO, floating oil storage ships etc.).

1.1.2.3 When ships specified in 1.1.2.1 cover the systmes refered to in 1.1.1.3 and the interfaces referred to in 1.1.1.4, the relevant or equivalent requirements corresponding to SL0 in Chaper 2 Section 3 of the Guidelines shall be complied at the least.

1.1.3 Determination of compliance of on-board CBS with cyber security requirements.

1.1.3.1 The process illustrated in Fig. 1.1.3.3 may be followed to determine the compliance of a CBS in a ship network with the relevant requirements of the Guidelines.

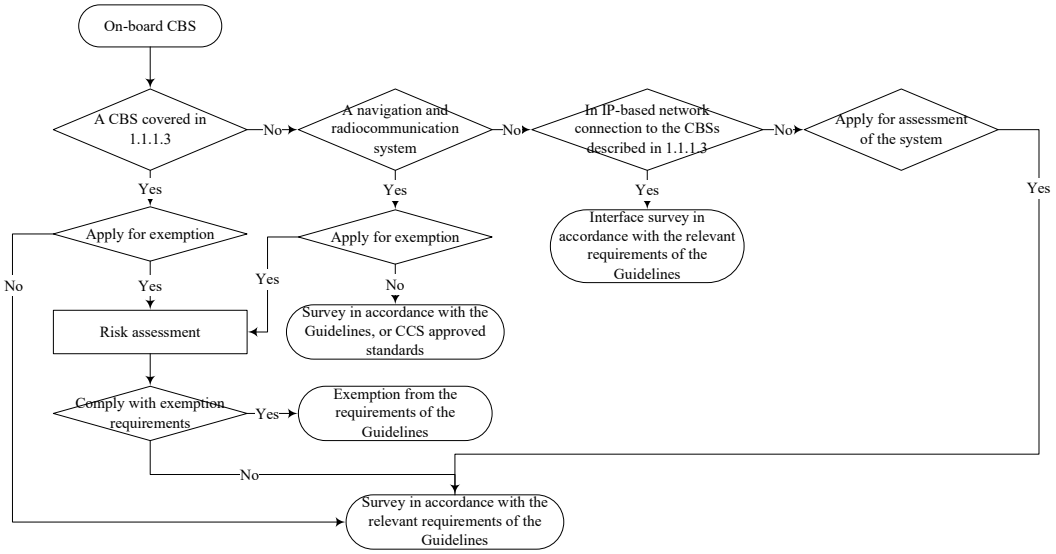

Fig. 1.1.3.3 CBS Security Survey/Assessment Determination Process

Section 2 Terms and Normative References

1.2.1 Terms and definitions

1.2.1.1 **Access Control**: Selective limiting of the ability and means to interact with a system, to use system resources to handle information, to gain information and knowledge the system contains or to control system components and functions.

1.2.1.2 **Attack Surface**: The set of all possible points where an unauthorized user can access a system and extract data. The attack surface comprises two categories: digital and physical. The digital attack surface encompasses all the hardware and software that connect to an organization's network. These include applications, codes, ports, servers and websites. The physical attack surface comprises all endpoint devices that an attacker can gain physical access to, such as desktop computers, hard drives, laptops, mobile phones, removable drives and carelessly discarded hardware.

1.2.1.3 **Authentication**: Provision of assurance that a claimed characteristic of an identity is correct.

1.2.1.4 **Compensating Countermeasure**: An alternate solution to a countermeasure employed in lieu of or in addition to inherent security capabilities to satisfy one or more security requirements.

1.2.1.5 **Computer Based System (CBS)**: A programmable electronic device, or interoperable set of programmable electronic devices, organized to achieve one or more specified purposes such as collection, processing, maintenance, use, sharing, dissemination, or disposition of information. CBS on-board include IT and OT systems. A CBS may be a combination of subsystems connected via network. CBS on-board may be connected directly or via public means of communications (e.g. Internet) to ashore CBSs, other vessels' CBS and/or other facilities.

1.2.1.6 **Computer Network**: A connection between two or more computers for the purpose of communicating data by means of agreed communication protocols.

1.2.1.7 **Cyber Security**: Characteristics of confidentiality, integrity and availability of information stored, transmitted and processed in a cyber environment.

1.2.1.8 **Cyber Attacks**: Any type of offensive operation that targets IT and OT systems, computer networks, and PC devices and attempts to access, compromise or destroy company and/or

ship systems and data.

1.2.1.9 **Cyber Incident**: An act or incident that affects the integrity, availability and/or confidentiality of a system caused by malicious threats in breach of security policies.

1.2.1.10 **Cyber Resilience**: The capability to reduce the occurrence and mitigating the effects of cyber incidents arising from the disruption or impairment of operational technology (OT) used for the safe operation of a ship, which potentially lead to dangerous situations for human safety, safety of the ship and/or threat to the environment.

1.2.1.11 **Defense in Depth**: Information security policy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization.

1.2.1.12 **Demilitarized Zone (DMZ)**: A physical or logical perimeter network segment that contains and exposes an organization's external-facing services to an external network. Its purpose is to enforce the internal network's security policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the internal networks from outside attacks.

1.2.1.13 **Denial of Service (DoS)**: A type of cyber attack designed to prevent legal and authorized users from accessing information typically by means of server buffer overflow. Distributed DoS refers to a DoS through controlling multiple computers and/or servers by a cyber attacker.

1.2.1.14 **Essential System**: CBS contributing to the provision of services essential for propulsion, steering and safety of the ship. Essential services comprise "Primary Essential Services" and "Secondary Essential Services"; Primary Essential Services are those services which need to be in continuous operation to maintain propulsion and steering. Secondary Essential Services are those services which need not necessarily be in continuous operation to maintain propulsion and steering but which are essential for maintaining the ship's safety.

1.2.1.15 **Firewall**: A logical or physical block used to monitor the input and output of network traffic via predefined rules.

1.2.1.16 **Firmware**: Software embedded in electronic devices that provide control, monitoring and data manipulation of engineered products and systems. These are normally self-contained and not accessible to user manipulation.

1.2.1.17 **Hardening**: The practice of reducing a system's vulnerability by reducing its attack surface.

1.2.1.18 **Information Technology (IT)**: Devices, software and associated networking focusing on the use of data as information, as opposed to Operational Technology (OT).

1.2.1.19 **Information Technology System (IT System)**: Mainly a system that uses computer technology, microelectronics technology and electrical means to manage the data and process of ship operation.

1.2.1.20 **Integrated System**: A system combining a number of interacting subsystems and/or equipment organized to achieve one or more specified purposes.

1.2.1.21 **Intrusion Detection System (IDS)**: A device or software application that monitors network or system activities for detection of malicious activities or policy violations and produces reports.

1.2.1.22 Intrusion Prevention System (IPS): A device or software used to identify and block malicious traffic or violations.

1.2.1.23 **Logical Network Segment**: The same as "Network Segment", but two or more logical network segments share the same physical components[①].

1.2.1.24 **Network Segment**: For the purposes of the Guidelines, Layer-2 Ethernet segment (a broadcast domain)[②].

1.2.1.25 **Network Switch (Switch)**: A device that connects devices together on a computer network, by using packet switching to receive, process and forward data to the destination device.

1.2.1.26 **Malware**: Generic term for a variety of software, which may infect computer systems and impair their performance.

1.2.1.27 **Network Transmission Media**: Physical channels bridging senders and receivers in the network, such as coaxial cable, optical fiber and wireless transmission.

1.2.1.28 **Offensive Cyber Manoeuvre**: Actions that result in denial, degradation, disruption, destruction, or manipulation of OT or IT systems.

1.2.1.29 **Operation Technology System**: A computer system used to provide control, alarm, surveillance, security, or internal communication functions.

1.2.1.30 **Operational Technology (OT)**: Devices, sensors, software and associated networking that monitor and control on-board systems. Operational technology systems may be thought of as focusing on the use of data to control or monitor physical processes.

1.2.1.31 **Patch**: Software designed to update installed software or supporting data to address security vulnerabilities and other bugs or improve operating systems or applications.

1.2.1.32 **Physical Network Segment**: The same as "Network Segment", but physical components cannot be shared with other network segments.[③]

1.2.1.33 **Protocol**: A common set of rules and signals that computers on the network use to communicate. Protocols enable data communication, network management and security. On-board networks usually implement protocols based on TCP/IP stacks or various fieldbuses.

1.2.1.34 **Recovery**: Development and implementation of the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cyber security incident. The recovery function supports timely return to normal operations to reduce the impact of a cyber security incident.

1.2.1.35 **Risk Assessment**: The process of collecting data and assigning values to risks for informing priorities, developing courses of action, and informing decisions.

1.2.1.36 **Risk Management**: The process of identifying, analyzing, assessing and communicating risk and accepting, avoiding, transferring or controlling it to an acceptable level considering associated costs and benefits of any actions taken.

① The logical network resides on the same physical network, but is segmented and managed at the data link or network layer (OSI Layer 2 and 3).

② Network address planning is prefixed by its IP address and network mask. Communication between network segments can only be achieved by using routing services at the network layer (OSI layer 3).

③ Segmentation divides the network into multiple physical segments or subnets to control incoming and outgoing packets. Both the network layer (OSI layer 3) and the application layer (OSI Layer 7) allow or block connections and data exchanges. Both traffic management and packet filtering can be managed by a single software or hardware device.

1.2.1.37 **Security Zone**: A collection of CBSs in the scope of application of the Guidelines that require the same access control policy. Each security zone consists of a single interface or a group of interfaces, to which an access control policy is applied.

1.2.1.38 **Shipowner/Company**: The owner of the ship or any other organization or person, such as the manager, agent or bareboat charterer, who has assumed the responsibility for operation of the ship from the shipowner and who on assuming such responsibilities has agreed to take over all the attendant duties and responsibilities. The Shipowner could be the Shipyard or System Integrator (Builder or Shipyard) during initial construction. After ship delivery, the Shipowner may delegate some responsibilities to the ship operating company.

1.2.1.39 **Supplier**: A manufacturer or provider of hardware and/or software products, system components or equipment (hardware or software) comprising of the application, embedded devices, network devices, host devices etc. working together as system or a subsystem. The Supplier is responsible for providing programmable devices, subsystems or systems to the System Integrator.

1.2.1.40 **System**: A combination of interacting programmable devices and/or subsystems organized to achieve one or more specified purposes.

1.2.1.41 **System Category**: System categories defined in IACS UR E22 based on their effects on system functionality, including System Categories I, II and III, as defined in 2.6.3, Chapter 2, Part 7 of CCS *Rules for Classification of Sea-Going Steel Ship*.

1.2.1.42 **Systems Integrator**: The specific person or organization responsible for the integration of systems and products provided by Suppliers into the system invoked by the requirements in the ship specifications and for providing the integrated system. The System Integrator may also be responsible for integration of systems in the ship. This role is to be taken by the Shipyard unless an alternative organization is specifically contracted/assigned this responsibility.

1.2.1.43 **Trusted Platform Module (TPM)**: A chip embedded in a computer to provide trusted roots for the computer.

1.2.1.44 **Untrusted Network**: Any network outside the scope of applicability of the Guidelines.

1.2.1.45 **Virtual Local Area Network (VLAN)**: A network that allows geographically dispersed network nodes communicate as if they were physically on the same network.

1.2.1.46 **Virtual Private Network (VPN)**: A virtual network, built on top of existing physical networks, that provides a secure communications tunnel for data transmitted between networks or devices utilizing tunnelling, security controls and endpoint address translation giving the impression of a dedicated line.

1.2.2 Normative References

The following references are cited in the Guidelines. For dated references, only the edition cited applies. For references not dated, their most updated editions apply to this Guidelines.

1.2.2.1 CCS Rules for Classification of Sea-going Steel Ships and the amendments.

1.2.2.2 IEC 62443-3-3:2013 Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels

Section 3 Ship Cyber Security Levels and Class Notations

1.3.1 Ship Cyber Security Levels

1.3.1.1 There are five ship cyber security levels.

Ship Cyber Security Levels Table 1.3.1.1

S/N	Level	Defensive Capability
1	SL0	Defense capability meeting minimum security requirements (UR E26)
2	SL1	Defense against occasional cyber incidents
3	SL2	Defense against cyber incidents initiated with a small amount of resources
4	SL3	Defense against cyber incidents initiated with a great amount of resources
5	SL4	Defense against well-organized and targeted cyber incidents

1.3.2 Class Notations for Ship Cyber Security

1.3.2.1 For ships, the class notation for cyber security may be granted on application and upon satisfactory plan approval and assessment/survey by CCS:

Cyber Security (M, P/S [SLx])

where: M represents compliance with the requirements of ship cyber risk management, P represents compliance with the minimum requirements of ship cyber security, and S represents compliance with higher requirements of ship cyber security.

(1) For M, the requirements of Section 2, Chapter 4 of the Guidelines are to be met.

(2) For P, the corresponding requirements of SL0 in Section 3, Chapter 4 of the Guidelines are to be met, and the CBS is at least to meet the corresponding requirements of SL0, which is the minimum cyber resilience requirement of the ship.

(3) For S, there are 4 levels (SL1~SL4). SL4 is the highest. The corresponding requirements of SL1~SL4 in Section 3, Chapter 4 of the Guidelines are to be met respectively, and the CBS is at least to meet the corresponding requirements of SL1~SL4 in Section 3, Chapter 2.

(4) Correspondence between Class Notations for Ship Cyber Security and ship/product cyber security level is shown in Table 1.3.2.1.

Table1.3.2.1

	Scope	Requirements	
		Ship-level	Product-level*
M	Applicable systems of the Guidelines	Compliance with cyber risk management requirements	-
P		SL0 (E26)	SL0 (E27)
S		SL1	SL1
		SL2	SL2
		SL3	SL3
		SL4	SL4

*: The security level of CBS shall in principle be not inferior to the security level of the ship.

1.3.2.2 For the application for a ship's cyber security-related class notations, the cyber security level to be achieved may be determined through consultation with CCS based on the cyber security expectations of the ship.

1.3.2.3 The assignment, maintenance, suspension, cancellation and reinstatement of the class notations for ship cyber security are to be in accordance with the relevant requirements of CCS.

1.3.3 Application

1.3.3.1 For the application for ship cyber security survey/assessment of a system and/or ship by CCS, a written application is to be submitted to CCS or its local branch, and an assessment

service contract and/or agreement may be signed if necessary.

Section 4 Application for Exclusion

1.4.1 Application

1.4.1.1 To exclude a CBS, to which the Guidelines apply, from the relevant security requirements, an application is to be submitted to CCS by the supplier or the system integrator/shipyard.

1.4.1.2 The CBS is to be subject to the cyber security risk assessment according to 1.4.2 and meet the cyber risk control requirements of 1.4.3. In addition, the cyber risk assessment report of the relevant CBS is also to be provided as evidence that the system is at an acceptable risk level.

1.4.2 CBS's Cyber Security Risk Assessment

1.4.2.1 The envisaged operational environments for the CBS under examination are to be analyzed in the cyber security risk assessment to discern the likelihood of cyber incidents and their impact on the human safety, the ship safety or the marine environment, taking into account the category of the CBS. The attack surface is to be analyzed, considering the connectivity grade of the CBS, possible interfaces for portable devices, logical access restrictions, etc. In the cyber security risk assessment, factors such as asset vulnerability, threats (both internal and external), and possible impact of cyber incidents are to be considered.

1.4.3 CBS's Cyber Security Requirements Acceptance Criteria

1.4.3.1 A CBS of any one of the following conditions may not be excluded from the cyber security-related requirements

(1) The CBS should not serve ship functions of category III ;

(2) The CBS shall not be an integrated control system serving multiple ship functions as specified in the scope of applicability of the Guidelines.

1.4.3.2 A CBS meeting all of the following criteria may be excluded from the cyber security-related requirements:

(1) The CBS shall be isolated (i.e, have no IP-network connections to other systems or networks) ;

(2) The CBS shall have no accessible physical interface ports. Unused interfaces shall be logically disabled. It shall not be possible to connect unauthorized devices to the CBS;

(3) The CBS must be located in areas to which physical access is controlled.

1.4.4 Approval of Exemption

1.4.4.1 The cyber risk assessment report of the relevant CBS subject to the requirements specified in 1.4.2 and meeting the exemption criteria of 1.4.3 is to be provided.

1.4.4.2 Where a CBS does not fully meet the criteria of 1.4.3.1, but is provied with a rational explanation togenther with evidence, an application may also be submitted to CCS for exemption, and CCS has the right to require additional documents as appropriate.

1.4.4.3 Where the cyber risk assessment can prove that the CBS has no impact on the safety of operations regarding cyber risk, CCS may accept the exemption, and its cyber risk assessment report needs to be approved by CCS plan approval surveyors. In light of ship application scenario, CCS plan approval surveyor shall approve exemptions from relevant requirements for CBS onboard a specific ship.

Chapter 2 Product Cyber Security Requirements

Section 1 General Provisions

2.1.1 General Requirements

2.1.1.1 The cyber security requirements of this chapter are to apply to products including but not limited to:

(1) CBSs covered by 1.1.1.3 as well as systems or devices realizing the interface specified by 1.1.1.4 of the Guidelines;

(2) Network devices as deemed necessary by CCS;

(3) Other systems/devices requested by the applicant.

2.1.1.2 The minimum requirements for the hosts, software programs, embedded devices, network devices, cloud devices, etc. in a CBS are to be determined according to the level of the system they are located.

2.1.1.3 Network devices refer to the dedicated software and hardware systems/devices that interconnect various servers, terminal devices, application terminals and other nodes in the network, including network switching devices (switches, bridges, etc.), network routing devices (routers, etc.), network security devices (firewalls, intrusion detection devices, security audit devices, encryption and decryption devices, etc.), network access devices (network interface cards, wireless access points, etc.) and others. Network equipment used in CBS shall at least meet the requirements of the corresponding security levels of 2.3.1 and 2.3.2 of this Guidelines. Network devices that apply for certification separately should meet the requirements of the Guidelines for such devices, or the equivalent requirements recognized by CCS.

2.1.1.4 The network requirements of marine products are centered on security requirements, and their communication requirements and reliability requirements are based on satisfaction of their business expectations.

2.1.1.5 The focus of product cyber security requirements is the seven elements listed in Table 2.1.1.5, and specific requirements are put forward according to the product cyber security levels.

Elements of Cyber Security Requirements for Marine Products Table 2.1.1.5

S/N	Basic Security Elements	Description
1	Identification and authentication	To identify and authenticate all users (human users, software processes, and devices) before allowing them to access the system.
2	Use control	To assign the privileges for authenticated users (human users, software processes, and devices) to carry out a requested action and also to monitor the use of such privileges assigned to them.
3	System integrity	To ensure the integrity of the system and prevent unauthorized operations.
4	Data confidentiality	To ensure the confidentiality of data in communication channels and storage areas to prevent unauthorized data disclosure.
5	Restricted data flow	To segment the system through areas and pipelines to restrict unnecessary data flows.
6	Timely response to events	To respond to violations against cyber security requirements, notify relevant personnel, report necessary evidence, and ensure that actions are taken in a timely manner.
7	Resource availability	To ensure the availability of the system to prevent critical services from being affected or denial of service.

2.1.2 Basic Security Requirements

2.1.2.1 Security measures are not to adversely affect the essential system functions.

Implementation of security measures are not to lead to the loss of security function, control function and surveillance function.

2.1.2.2 The basic functions of essential systems are not to be affected when the boundary of the security zone is closed due to failure or in island mode.

2.1.2.3 The system is to be adequately designed to ensure the confidentiality, integrity and availability of the data necessary for safety of the ship, its systems, personnel and cargo.

2.1.2.4 Compensating countermeasures may be employed in lieu of or in addition to inherent security capabilities to satisfy one or more security requirements. Compensating countermeasures are to follow these principles:

(1) Compensating countermeasures are to meet the intent and rigor of the original stated requirement. They are also not to be "inferior" to other requirements.

(2) The security capability required to be provided by the system can be provided by other devices or systems. For type approval of a system, the compensating countermeasures are to be implemented in the CBS, i.e., not rely on barriers related to installation on board or operational procedures.

(3) The principles described in the Security Capability Specification document in Section 3.1.3 shall also be followed.

Section 2 Product Cyber Security Levels

2.2.1 Product Cyber Security Levels

2.2.1.1 There are 5 product cyber security levels (SL0~ SL 4), as listed in Table 2.2.1.1.

Cyber Security Levels of Marine Products Table 2.2.1.1

S/N	Level	Corresponding Requirements of the Guidelines	Defensive Capability
1	SL 0	See 2.3-2.4.	Compliance with the minimum cyber security requirements of CBS (UR E27)
2	SL 1		Defense against occasional cyber incidents
3	SL 2		Defense against cyber incidents initiated with a small amount of resources
4	SL 3		Defense against cyber incidents initiated with a great amount of resources
5	SL 4		Defense against well-organized and targeted cyber incidents

Section 3 System Requirements

2.3.1 CBS Security Requirements

2.3.1.1 Identification and Authentication

(1) Human user identification and authentication

No.	Requirements	SL0	SL1	SL2	SL3	SL4
SR1.1	The CBS is to provide the capability to identify and authenticate all human users accessing the system	√	√	√	√	√
SR1.1 RE1	The CBS is to provide the capability to uniquely identify and authenticate all human users			√	√	√
SR1.1 RE2	The CBS is to employ multifactor authentication for human users accessing via an untrusted network.	√*①	√*②	√	√	√
SR1.1 RE3	The CBS is to employ multifactor authentication for all human users.					√

(2) Process and device identification and authentication

No.	Requirements	SL0	SL1	SL2	SL3	SL4
SR1.2	The CBS is to provide the capability to identify and authenticate all processes and devices accessing the system via interfaces.	√*	√*	√	√	√
SR1.2 RE1	The CBS is to provide the capability to uniquely identify and authenticate all software processes and devices.				√	√

(3) Account management

No.	Requirements	SL0	SL1	SL2	SL3	SL4
SR1.3	The CBS is to provide the capability to support the management of all accounts by authorized users, including adding, activating, modifying, disabling and removing account.	√	√	√	√	√
SR1.3 RE1	CBS is to provide the capability to support unified account management.				√	√

(4) Identifier management

No.	Requirements	SL0	SL1	SL2	SL3	SL4
SR1.4	The CBS is to provide the capability to support the management of identifiers by user, group, role or control system interface.	√	√	√	√	√

(5) Authentication management

No.	Requirements	SL0	SL1	SL2	SL3	SL4
SR1.5	The CBS is to provide the capability to: ① Initialize authenticator (token, password, fingerprint, etc.) content; ② Change all default authenticators upon CBS installation; ③ Change/refresh all authenticators; ④ Protect all authenticators from unauthorized disclosure and modification when stored and transmitted.	√	√	√	√	√
SR1.5 RE1	For software and device users, the CBS is to provide the capability to protect the relevant authenticators via hardware mechanisms (e.g. TPM).				√	√

① √indicates applicable.
√* indicates applicable when connected to an untrusted network.
② √*indicates that IEC 62443-3-3 is not applicable at the corresponding level, but it is applicable in the Guidelines in the case of connection to an untrusted network.

(6) Wireless access management

No.	Requirements	SL0	SL1	SL2	SL3	SL4
SR1.6	The CBS is to provide the capability to identify and authenticate all users (human users, software processes or devices) engaged in wireless communication.	√	√	√	√	√
SR1.6 RE1	The CBS is to provide the capability to uniquely identify and authenticate all users (human users, software processes or devices) engaged in wireless communication.			√	√	√

(7) Password strength

No.	Requirements	SL0	SL1	SL2	SL3	SL4
SR1.7	Utilizing password authentication, the CBS is to provide the capability to configure password strength based on minimum length and variety of character types.	√	√	√	√	√
SR1.7 RE1	The CBS is to provide the capability to restrict the use of old password by any human user within a certain password change cycle, and the password minimum and maximum lifetime for human users.				√	√
SR1.7 RE2	The CBS is to provide the capability to restrict the password minimum and maximum lifetime for all users.					√

(8) PKI certificates

No.	Requirements	SL0	SL1	SL2	SL3	SL4
SR1.8	Utilizing PKI technique, the CBS is to provide the capability to operate a PKI according to best practices or obtain public key certificates from an existing PKI.			√	√	√

(9) Strength of public key authentication

No.	Requirements	SL0	SL1	SL2	SL3	SL4
SR1.9	Utilizing public key authentication, the CBS is to provide the capability to: ① Validate certificates by checking the validity of the signature of a given certificate; ② Validate certificates by constructing a certification path to an accepted CA or in the case of self-signed certificates by deploying leaf certificates to all hosts which communicate with the subject to which the certificate is issued; ③ Validate certificates by checking the revocation status of a given certificate; ④ Establish user (human user, software process or device) control of the corresponding private key; ⑤ Map the authenticated identity to a user (human user, software process or device).			√	√	√
SR1.9 RE1	The CBS is to provide the capability to protect the relevant private keys via hardware mechanisms according to commonly accepted security industry practices and recommendations.				√	√

(10) Authentication feedback

No.	Requirements	SL0	SL1	SL2	SL3	SL4
SR1.10	The CBS is to provide the capability to obscure feedback of authentication information during the authentication process.	√	√	√	√	√

(11) Unsuccessful login attempts

No.	Requirements	SL0	SL1	SL2	SL3	SL4
SR1.11	The CBS is to provide the capability to enforce a limit of a configurable number of consecutive invalid access attempts by any user (human user, software process or device), and deny access for a specified period of time or until unlocked by an administrator. For system accounts on behalf of which critical services or servers are run, the CBS is to provide the capability to disallow interactive logins.	√*	√	√	√	√

(12) System use notification

No.	Requirements	SL0	SL1	SL2	SL3	SL4
SR1.12	The CBS is to provide the capability to display a system use notification message before authentication. The system use notification message is to be configurable by authorized personnel.	√*	√	√	√	√

(13) Access via untrusted networks

No.	Requirements	SL0	SL1	SL2	SL3	SL4
SR1.13	The CBS is to provide the capability to monitor and control any access via untrusted networks.	√*	√	√	√	√
SR1.13 RE1	The CBS is to provide the capability to deny access requests via untrusted networks unless approved by the specified role.	√*	√*	√	√	√

2.3.1.2 Use Control

(1) Authorization enforcement

No.	Requirements	SL0	SL1	SL2	SL3	SL4
SR2.1	On all interactive interfaces, the CBS is to provide the capability to assign permissions to all human users to control the use of the system based on the assigned responsibilities and least privilege.	√	√	√	√	√
SR2.1 RE1	On all interfaces, the CBS is to provide the capability to assign permissions to all users (human users, software processes and devices) to control the use of the system based on the assigned responsibilities and least privilege.			√	√	√
SR2.1 RE2	The CBS is to provide the capability to authorize users or roles to define and modify the mapping of all human users or roles to permissions.			√	√	√
SR2.1 RE3	The CBS is to support supervisor manual override of the authorization of the current human user for a configurable time or sequence of events.①				√	√
SR2.1 RE4	The CBS is to support dual approval/confirmation when an action may result in serious impact on the ship safety, e.g. switching of operating modes.					√

① Implementation of a controlled, audited and manual override of automated mechanisms in the event of emergencies or other serious events is often needed. This allows a supervisor to enable the current user to quickly react to unusual conditions without closing the current session and establishing a new session as a higher privilege user.

(2)Wireless use control

No.	Requirements	SL0	SL1	SL2	SL3	SL4
SR2.2	The CBS is to provide the capability to authorize, monitor and enforce use restrictions for wireless connectivity according to commonly accepted security industry practices.	√	√	√	√	√
SR2.2 RE1	The CBS is to provide the capability to identify and report unauthorized wireless devices transmitting in the physical environment of the system.				√	√

(3) Use control for portable and mobile devices

No.	Requirements	SL0	SL1	SL2	SL3	SL4
SR2.3	When the CBS supports use of portable and mobile devices, it is to include the capability to: ① Limit the use of portable and mobile devices only to those permitted by design; ② Restrict code and data transmission to/from portable and mobile devices.②	√	√	√	√	√
SR2.3 RE1	The CBS is to provide the capability to verify that a portable or mobile device attempting to connect to a zone complies with the security requirements of that zone.				√	√

② Port limits/blockers could be accepted for a specific system.

(4)Mobile code

No.	Requirements	SL0	SL1	SL2	SL3	SL4
SR2.4	The CBS is to provide the capability to control the use of mobile code, such as Javascripts, ActiveX and PDF.	√	√	√	√	√
SR2.4 RE1	The CBS is to provide the capability to verify the integrity of mobile code before allowing code execution.				√	√

(5) Session lock

No.	Requirements	SL0	SL1	SL2	SL3	SL4
SR2.5	The CBS is to provide the capability to initiate a session lock automatically or manually after a configurable time period. The session lock will establish access through re-authentication of the human user or other authorized personnel.	√	√	√	√	√

(6) Remote session termination

No.	Requirements	SL0	SL1	SL2	SL3	SL4
SR2.6	The CBS is to provide the capability to terminate a remote session automatically after a configurable time period of inactivity or manually by the user who initiated the session.	√*	√*	√	√	√

(7) Concurrent session control

No.	Requirements	SL0	SL1	SL2	SL3	SL4
SR2.7	The CBS is to provide the capability to limit the number of concurrent sessions per interface to a configurable number of sessions.				√	√

(8) Auditable events

No.	Requirements	SL0	SL1	SL2	SL3	SL4
SR2.8	The CBS is to provide the capability to generate audit records relevant to security at least for the following categories: access control, operating system events, backup and restore events, configuration changes, and communication interruption. Individual audit records are to include the timestamp, source (originating device, software process or human user account), category, type, event ID and event result.	√	√	√	√	√
SR2.8 RE1	The CBS is to provide the capability to centrally manage auditable events and to compile audit records from multiple components through the overall control system into a system-wide (logical or physical) time-correlated audit trail. The control system is to provide the capability to export these audit records in industry standard formats for analysis by standard commercial log analysis tools, for example, Security Information and Event Management (SIEM).				√	√

(9) Audit storage capacity

No.	Requirements	SL0	SL1	SL2	SL3	SL4
SR2.9	The CBS is to allocate sufficient audit record storage capacity according to commonly accepted recommendations for log management and system configuration. The management system is to provide auditing mechanisms to reduce the likelihood of such capacity being exceeded.	√	√	√	√	√
SR2.9 RE1	The CBS is to provide the capability to issue a warning when allocated audit record storage volume reaches a configurable percentage of the maximum audit record storage capacity.				√	√

(10) Response to audit processing failures

No.	Requirements	SL0	SL1	SL2	SL3	SL4
SR2.10	The CBS is to provide the capability to alert personnel and prevent the loss of essential services and functions in the event of an audit processing failure. The CBS is to provide the capability to support appropriate actions in response to an audit processing failure according to commonly accepted industry practices and recommendations.	√	√	√	√	√

(11) Timestamps

No.	Requirements	SL0	SL1	SL2	SL3	SL4
SR2.11	The CBS is to provide the capability to provide timestamps for audit record generation.	√	√	√	√	√
SR2.11 RE1	The CBS is to provide the capability to synchronize internal system clocks at a configurable frequency.				√	√
SR2.11 RE2	The time source is to be protected from unauthorized alteration and is to cause an auditable event upon alteration.					√

(12) Non-repudiation

No.	Requirements	SL0	SL1	SL2	SL3	SL4
SR2.12	The CBS is to provide the capability to determine whether a given human user took a particular action.				√	√
SR2.12 RE1	The CBS is to provide the capability to determine whether a given user (human user, software process or device) took a particular action.					√

2.3.1.3 System Integrity

(1) Communication integrity

No.	Requirements	SL 0	SL1	SL2	SL3	SL4
SR3.1	The CBS is to provide the capability to protect the integrity of transmitted information. Note: Wireless networks should be encrypted.	√	√	√	√	√
SR3.1 RE1	The CBS is to provide the capability to employ cryptographic mechanisms to recognize changes to information during communication.	√*	√*	√*	√	√

(2) Malicious code protection

No.	Requirements	SL 0	SL1	SL2	SL3	SL4
SR3.2	The CBS is to provide the capability to employ protection mechanisms to prevent, detect, report and mitigate the effects of malicious code or unauthorized software, and is to provide the capability to update the protection mechanisms.	√	√	√	√	√
SR3.2 RE1	The CBS is to provide the capability to employ malicious code protection mechanisms at all interfaces			√	√	√
SR3.2 RE2	The CBS is to provide the capability to manage malicious code protection mechanisms.				√	√

(3) Security functionality verification

No.	Requirements	SL0	SL1	SL2	SL3	SL 4
SR3.3	The CBS is to provide the capability to support verification of the intended operation of security functions and report when anomalies are discovered during factory acceptance test (FAT), site acceptance test (SAT) and scheduled maintenance. These security functions are to include all those necessary to support the security requirements specified in the Guidelines.①	√	√	√	√	√
SR3.3 RE1	The CBS is to provide the capability to employ automated mechanisms to support management of security verification during FAT, SAT and scheduled maintenance. Note: automation of verification management methods such as information collection and report generation				√	√
SR3.3 RE2	The CBS is to provide the capability to verify security functions during normal operations.					√

①Verification of security functions includes verification of antivirus software functions, verification of identification, authentication and use control methods, and verification of IDS triggering rules.

(4) Software and information integrity

No.	Requirements	SL0	SL1	SL2	SL3	SL4
SR3.4	The CBS is to provide the capability to detect, record, report and prevent against unauthorized changes to software and information.			√	√	√
SR3.4 RE1	The CBS is to provide the capability to notify particular personnel upon discovering discrepancies during integrity verification.				√	√

(5) Input validation

No.	Requirements	SL0	SL1	SL2	SL3	SL4
SR3.5	The CBS is to validate the syntax and content of any input used to control or directly impact the action of the CBS.	√*	√	√	√	√

(6) Deterministic output

No.	Requirements	SL0	SL1	SL2	SL3	SL4
SR3.6	The CBS is to provide the capability to set outputs or its own state to a predetermined value (unpowered state, last-known value, fixed value) if normal operation cannot be maintained as a result of an attack.	√	√	√	√	√

(7) Error handling

No.	Requirements	SL0	SL1	SL2	SL3	SL4
SR3.7	The CBS is to provide the capability to identify and handle error conditions in a manner such that effective remediation can occur. This is to be done in a manner which does not provide information that could be exploited by adversaries to attack the system unless revealing such information is necessary for the timely troubleshooting of			√	√	√

	problems.					

(8) Session integrity

No.	Requirements	SL0	SL1	SL2	SL3	SL4
SR3.8	The CBS is to provide the capability to protect the integrity of sessions, and is to reject any use of invalid session IDs.	√*	√*	√	√	√
SR3.8 RE1	The CBS is to provide the capability to invalidate session IDs upon user logout or other session termination (including browser sessions).	√*	√*	√*	√	√
SR3.8 RE2	The CBS is to provide the capability to generate a unique session ID for each session and treat all unexpected session IDs as invalid.				√	√
SR3.8 RE3	The CBS is to provide the capability to generate unique session IDs with commonly accepted sources of randomness.					√

(9) Protection of audit information

No.	Requirements	SL0	SL1	SL2	SL3	SL4
SR3.9	The CBS is to provide the capability to protect audit information and audit tools (if any) from unauthorized access, modification and deletion.			√	√	√
SR3.9 RE1	The CBS is to provide the capability to produce audit records on hardware-enforced write-once media.					√

2.3.1.4 Data Confidentiality

(1) Information confidentiality

No.	Requirements	SL0	SL1	SL2	SL3	SL4
SR4.1	The CBS is to provide the capability to protect the confidentiality of information for which explicit read authorization is supported, whether at rest or in transit.	√	√	√	√	√
SR4.1 RE1	The CBS is to provide the capability to protect the confidentiality of information at rest and remote access sessions traversing an untrusted network.			√	√	√
SR4.1 RE2	The CBS is to provide the capability to protect the confidentiality of information traversing any zone boundary.					√

(2) Information persistence

No.	Requirements	SL0	SL1	SL2	SL3	SL4
SR4.2	The CBS is to provide the capability to purge all information for which explicit read authorization is supported from components to be released from active service and/or decommissioned.			√	√	√
SR4.2 RE1	The CBS is to provide the capability to protect against unauthorized and unintended information transfer via volatile shared memory resources.				√	√

(3) Use of cryptography

No.	Requirements	SL0	SL1	SL2	SL3	SL4
SR4.3	If cryptography is required, the CBS is to use cryptographic algorithms, key lengths and mechanisms for key establishment and management according to commonly accepted security industry practices and recommendations.	√	√	√	√	√

2.3.1.5 Restricted data flow

(1) Network segmentation

No.	Requirements	SL0	SL1	SL2	SL3	SL4
SR5.1	The CBS is to provide the capability to logically segment control system networks from non-control system networks, and to logically segment critical control system networks from other control system networks.		√	√	√	√
SR5.1 RE1	The CBS is to provide the capability to physically segment control system networks from non-control system networks, and to physically segment critical control system networks from other control system networks.			√	√	√
SR5.1 RE2	The CBS is to have the capability to provide network services to control system networks, critical or otherwise, without a connection to non-control system networks.				√	√
SR5.1 RE3	The CBS is to provide the capability to logically and physically isolate critical system networks providing primary critical services from critical system networks providing secondary critical services.					√

(2) Zone boundary protection

No.	Requirements	SL0	SL1	SL2	SL3	SL4
SR5.2	The CBS is to provide the capability to monitor and control communications at zone boundaries to enforce the compartmentalization based on the risk.		√	√	√	√
SR5.2 RE1	The CBS is to provide the capability to deny network traffic by default and allow network traffic by exception (also termed deny all, permit by exception).			√	√	√
SR5.2 RE2	The CBS is to provide the capability to prevent any communication through the control system boundary (also termed island mode).				√	√
SR5.2 RE3	The CBS is to provide the capability to prevent any communication through the control system boundary when there is an operational failure of the boundary protection mechanisms (also termed fail close). This "fail close" functionality is to be designed such that it does not affect the operation of security-related functions.				√	√

(3) Out-of-system communication restrictions

No.	Requirements	SL0	SL1	SL2	SL3	SL4
SR5.3	The CBS is to provide the capability to prevent social media, email and other communication messages from being received from users or systems external to the CBS.		√	√	√	√
SR5.3 RE1	The CBS is to provide the capability to prevent social media, email and other communication messages from being transmitted or received.				√	√

(4) Application partitioning

No.	Requirements	SL0	SL1	SL2	SL3	SL4
SR5.4	The CBS is to provide the capability to support partitioning of data, applications and services based on criticality.		√	√	√	√

2.3.1.6 Timely Response to Events

(1) Audit log accessibility

No.	Requirements	SL0	SL1	SL2	SL3	SL4
SR6.1	The CBS is to provide the capability for authorized personnel and/or tools to access audit logs on a read-only basis.	√	√	√	√	√
SR6.1 RE1	The CBS is to provide programmatic access to audit records using an application programming interface (API).				√	√

(2) Continuous monitoring

No.	Requirements	SL0	SL1	SL2	SL3	SL4
SR6.2	The CBS is to provide the capability to continuously monitor all security mechanism performance to detect, characterize and report security vulnerabilities in a timely manner according to commonly accepted security industry practices and recommendations.			√	√	√

2.3.1.7 Resource Availability

(1) Denial of service protection

No.	Requirements	SL0	SL1	SL2	SL3	SL4
SR7.1	The CBS is to provide the capability to maintain important funtions during a DoS event.	√	√	√	√	√
SR7.1 RE1	The CBS is to provide the capability to manage communication loads (such as using rate limiting) to mitigate the effects of DoS events.			√	√	√
SR7.1 RE2	The CBS is to provide the capability to restrict the ability of all users (human users, software processes and devices) to cause DoS events which affect other CBSs or networks.				√	√

①Note：It is acceptable for a computer system to degrade during a DoS event, but it must not fail in a manner that could cause a dangerous situation. DoS events based on overloading should be considered, such as cases where network capacity is attempted to be flooded, and cases where computer resources are attempted to be consumed

(2) Resource management

No.	Requirements	SL0	SL1	SL2	SL3	SL4
SR7.2	The CBS is to provide the capability to limit the use of resources by security functions to prevent resource exhaustion. For example, the CBS is to provide the capability to give priority to allocating system resources to high-priority processes.	√	√	√	√	√

(3) System backup

No.	Requirements	SL0	SL1	SL2	SL3	SL4
SR7.3	The identity and location of critical files and the ability to conduct backups of user-level and system-level information (including system state information) are be supported by the CBS without affecting normal operations. For specific backup requirements, please refer to the incident recovery requirements contained in Section 3, Chapter 4 of the Guidelines.	√	√	√	√	√
SR7.3 RE1	The CBS is to provide the capability to verify the reliability of backup mechanisms.			√	√	√
SR7.3 RE2	The CBS is to provide the capability to automate the backup function based on a configurable frequency.				√	√

(4) Control system recovery and reconstruction

No.	Requirements	SL0	SL1	SL2	SL3	SL4
SR7.4	The CBS is to provide the capability to recover and reconstruct to a known secure state after a disruption or failure.	√	√	√	√	√

(5) Power supply

No.	Requirements	SL0	SL1	SL2	SL3	SL4
SR7.5	The CBS is to provide the capability to switch to and from a power supply without affecting the existing security state or a preset degraded mode.	√	√	√	√	√

(6) Network and security configuration settings

No.	Requirements	SL0	SL1	SL2	SL3	SL4
SR7.6	The CBS is to provide the capability to have its traffic configured according to the network and security configurations recommended by the supplier. The CBS is to provide an interface to the network and security configurations.	√	√	√	√	√
SR7.6 RE1	The CBS is to provide the capability to generate a security configuration report in CSV, JSON, XML and other formats.				√	√

(7) Least functionality

No.	Requirements	SL0	SL1	SL2	SL3	SL4
SR7.7	The CBS is to provide the capability to specifically prohibit and/or restrict the use of unnecessary functions, ports, protocols and/or services.	√	√	√	√	√

(8) Control system component inventory

No.	Requirements	SL0	SL1	SL2	SL3	SL4
SR7.8	The CBS is to provide the capability to report the list of installed components and their associated properties.			√	√	√

2.3.2 Additional Security Requirements for Network Devices

2.3.2.1 Network devices are also to meet the following additional security requirements:

(1) Use of physical diagnostic and test interfaces

No.	Requirements	SL0	SL1	SL2	SL3	SL4
NDR2.13	Network devices are to prevent unauthorized use of the physical factory diagnostic and test interfaces.			√	√	√
NDR2.13 RE1	Network devices are to provide active monitoring of their diagnostic and test interfaces and generate an audit log when access to these interfaces is detected.				√	√

(2) Support for updates

No.	Requirements	SL0	SL1	SL2	SL3	SL4
NDR3.10	Network devices are to support upgrades and updates.		√	√	√	√
NDR3.10 RE1	Network devices are to validate the authenticity and integrity of all software updates and upgrades.			√	√	√

(3) Physical tamper resistance and detection

No.	Requirements	SL0	SL1	SL2	SL3	SL4
NDR3.11	Network devices are to provide tamper resistance and detection mechanisms to protect against unauthorized physical access.			√	√	√
NDR3.11 RE1	Network devices are to be capable of automatically providing notification to the recipient upon delivery of an attempt to make an unauthorized physical access. All notifications of tampering are to be logged as part of the overall audit logging function.				√	√

(4) Provisioning product supplier roots of trust

No.	Requirements	SL0	SL1	SL2	SL3	SL4
NDR3.12	Network devices are to provide the capability to provision and protect the confidentiality, integrity and authenticity of product supplier keys and data to be used as "roots of trust" at the time of manufacture of the device.			√	√	√

(5) Provisioning asset owner roots of trust

No.	Requirements	SL0	SL1	SL2	SL3	SL4
NDR3.13	Network devices are to: ① Provide the capability to provision and protect the confidentiality, integrity and authenticity of asset owner keys and data; and ② Support the capability to provision without reliance on components that may be outside of the security zone of the device.			√	√	√

(6) Integrity of the boot process

No.	Requirements	SL0	SL1	SL2	SL3	SL4
NDR3.14	Network devices are to verify the integrity of the firmware, software and configurable data needed for component's boot process prior to the boot process.		√	√	√	√
NDR3.14 RE1	Network devices are to use the component's product supplier roots of trust to verify the authenticity of the firmware, software and configurable data needed for component's boot process prior to the boot process.			√	√	√

(7) Intrusion prevention

No.	Requirements	SL0	SL1	SL2	SL3	SL4
ADD1	Network devices with intrusion prevention function are to be capable of analyzing the collected information and discovering intrusion events.		√	√	√	√
ADD1 RE1	Network devices with intrusion prevention function are to be capable of taking security measures such as recording events, automatically issuing security warnings or blocking when detecting intrusion events.			√	√	√

(8) Security audit

No.	Requirements	SL0	SL1	SL2	SL3	SL4
ADD2	Network devices with security audit function are to be capable of monitoring and recording the network operational state and cyber security events of the audit target. Note: Different types of dedicated cyber security products have different security audit targets, which usually include hosts, networks, databases, applications, etc.		√	√	√	√
ADD2 RE1	Network devices are to be capable of comparing and analyzing events to discover violations, anomalies, etc.			√	√	√
ADD2 RE2	The network operational state log and cyber security event log are to be stored in non-volatile storage media for at least 6 months for local or outgoing logs.			√	√	√

Section 4 Security Development Lifecycle Requirements

2.4.1.1 Systems/devices are to be developed following the secure development lifecycle process with cyber security factors considered at various stages, including at least the following:

(1) Security requirement analysis, which should clarify the expected security environment and security functions required by the system/equipment, security requirements can be considered from the aspects of security environment, threat model, security requirements audit, etc.;

(2) Security design, the supplier chooses the applicable programming language, architecture, defense mechanism, platform, communication protocol, password and other methods to achieve the system/device security requirements;

(3) Safety implementation, the system/device implementation process meets the safety requirements and safety design requirements. In the process of implementation, attention should be paid to the application of standard coding, the use of code analysis tools, the use of security testing tools, manual review of code safety and other aspects;

(4) Verification, the process of security verification of the system/device to confirm whether the system/device meets the corresponding security level requirements in Article 2.2.1 of this Guidelines. The problems found in the testing process should be recorded, and the safety implementation process should be fed back for remification. The repaired system/device should also be verified, and the security risk should be reduced to a controllable range before release;

(5) Release, before the release of the system/device, all processes/records in the early development process should be reviewed to confirm that all security problems in the security development process have been repaired or mitigated. The product can be released after passing the safety review;

(6) Maintenance, the supplier shall carry out regular security assessment of the product, confirm whether the product has security risks, and update security information such as patches when necessary;

(7) Decommissioning, the system/device is removed from the operating environment, disconnected from any interface in the environment, important information in the system/device should be processed (backup/delete) to ensure that the internal information of the system/device is permanently deleted after decommissioning.

2.4.1.2 The supplier shall document the safety development lifecycle to confirm that the system/device meet the safety development lifecycle requirements, including:

(1) Private key control file to protect the private key used for code signing from unauthorized access or modification (if applicable);

(2) Security update documents, procedures shall be established to ensure that documents about product security update is available to users (such as through the establishment of network security liaison mechanisms or regular update documents accessible to users), including but not limited to:

① version of the product to which the security patch is applied;

② instructions on how to apply approved patches manually and via an automated process;

③ a description of any impacts that installing the patch in the product can have, including restart;

④ instructions on how to verify that an approved patch has been applied; and

⑤ risks of not applying the patch that is not approved or deployed by the asset owner;

(3) Security update documents of the relevant component/operating system to indicate whether the product is compatible with the dependent component or operating system security updates;

(4) Security update delivery procedures, the supplier shall establish a quality assurance (QA) process to provide for the safety testing of product updates prior to release and to ensure that product users can verify the authenticity of security updates applicable to their products and versions;

(5) Product defense in depth policy to describe the product's security defense in depth policy to support installation, operation and maintenance, including:

① The security capabilities provided by the product and its role in the defense in depth policy;

② Threats addressed via the product defense in depth policy;

③ A user mitigation strategy for known security risks associated with the product, including those associated with legacy code.

(6) Defense in depth measures in the expected external environment, describing the product's expected security in depth measures provided by the external environment (such as physical layout, policies, and procedures);

(7) Security hardening guide, hardening guide for product installation and maintenance, including mainly:

① The integration of products (including third-party components) with their security environment;

② Integration of the application programming interface/protocol of the product with the user application programming;

③ Implementation and maintenance of the product defense in depth policy;

④ Configure and use security options/features that support local security policies, and:

a) the function of each security option/feature to the product defense in depth policy;
b) description of the configurable and default values, including how each value affects security and the potential impact of each value on the work;
c) set/change/delete related values;

⑤ Instructions and recommendations for the use of all security-related tools and practical programs that support the management, monitoring, incident handling and evaluation of product security;

⑥ Instructions and recommendations for regular security maintenance;

⑦ Instructions for reporting product security incidents to suppliers;

⑧ Instructions for the best practice of product maintenance and management.

2.4.1.3 The Supplier is to have procedural and technical controls in place and establish a quality assurance process to specify the stages of product safety development process and safety development lifecycle documentation. The procedure documentation and the secure development lifecycle documentation shall be submitted to CCS for review and shall meet the following requirements:

(1) Private key control documents

This requirement applies if the system contains software that digitally signs in order to enable users to verify their authenticity. The supplier shall provide management documentation demonstrating that its policies, procedures, and technical controls are in place to protect the generation, storage, and use of private keys for code signing from unauthorized access. Policies and procedures should define roles, responsibilities, and work processes. Technical controls should include physical access restrictions and cryptographic hardware for storing private keys (such as hardware security modules).

(2) Security update documents

The supplier shall provide management documentation demonstrating that processes are in place within the organization to ensure that security updates are notified to users, and the information provided to users shall include the items listed in 2.4.1.2 (2) of this Guidelines.

(3) Security update documents for related components/operating systems

The supplier shall provide the management documentation required by 2.4.1.2 (3) of this Guidelines to demonstrate that processes are in place within the organization to ensure that users know whether the system is compatible with the updated version of the software on which it relies (new versions, patches to operation system or firmware), and that these notifications shall specify how to manage the risks of not updating.

(4) Security update delivery procedures

The supplier shall provide the management documentation required by 2.4.1.2 (4) of this guidelines, demonstrating that the organization has established processes to ensure that system security updates are provided to users, and describing how users can verify the authenticity of the updated software.

(5) Product depth defense strategy

The supplier shall provide the management documentation required by 2.4.1.2 (5) of this guidelines to demonstrate that the organization has established processes to document defense-in-depth strategies to mitigate security threats to software in CBS during installation, maintenance, and operation. The threat could be the installation of unauthorized software, weaknesses in patches, tampering with the software during ship operation.

(6) Defense-in-depth measures in expected external environment

The supplier shall provide management documentation, as required by 2.4.1.2 (6) of this Guidelines, demonstrating that the organization has established processes to clearly document the defensive measures in depth expected from external environments, such as physical placement, policies, and procedures.

(7) Security Hardening Guide

The supplier shall provide the management documentation required by 2.4.1.2 (7) of this guidelines to demonstrate that the organization has established processes to ensure that hardening guidelines are in place for the system. Such guidelines should specifically describe how to reduce system vulnerability by removing/forbidding/disabling unnecessary software, account, and services.

Chapter 3 Product Inspection/Assessment

Section 1 General Provisions

3.1.1 Survey scope

3.1.1.1 The scope of application of the survey/assessment in this Chapter covers the products specified in 2.1.1.1.

3.1.2 Survey/Assessment Process

3.1.2.1 For the products under the survey scope, applications for surveys shall be submitted to CCS. Among which, applications for the products required by CCS Rules to be approved or subject to voluntary approval can be submitted to CCS combined with the initial product approval, approval alteration and renewal; application for products not required by CCS Rules to be approved can be submitted by combining with product survey.

3.1.2.2 Drawings related to product cyber security shall be submitted in accordance with 3.1.3. Product inspection shall be carried out in accordance with Section 2 of Chapter 3 of this Guidelines. Approval certificate or product certificate shall be issued upon satisfactory completion of the verification.

3.1.2.3 For products of voluntary assessment of cyber security, written application shall be made to CCS. Assessment service contract and /agreement shall be signed when necessary.

3.1.2.4 For products applying for cyber security assessment, drawings shall be submitted in accordance with 3.1.3. Test and assessment shall be carried out in accordance with Section 2, Chapter 3. The product cyber security assessment report shall be issued upon satisfactory completion of CCS plan approval and witnessed test and verification.

3.1.2.5 The supplier shall comply with the security development lifecycle requirements of 2.4 of this Guidelines and undergo field audit and verification.

3.1.2.6 After the cyber security capability of the product is verified satisfactorily, simplified drawings and test data according to Table 3.1.3.1 note 2) shall be submitted.

3.1.2.7 Application for cyber device can be submitted independently or together with those for systems as system components.

3.1.3 Drawings and Test Documents

3.1.3.1 Drawings and documents are to be submitted for approval or information in accordance with Table 3.1.3.1.

Summary of Drawings and Documents Table 3.1.3.1

S/N	Documents to be Submitted	Remarks
1	CBS Asset Inventory	Ⓐ[1)2)]
2	Network Topology	Ⓐ[1)2)]
3	Security Capability Description	Ⓐ[1)]
4	Security Capability Test Program	Ⓐ[1)]
5	Security Configuration Guide	Ⓘ[1)]
6	Security Development Lifecycle	Ⓐ[1)]
7	Maintenance and Verification Plan	Ⓘ[1)]
8	Information supporting Response to Cyber Incidents and Recovery Plan	Ⓘ[1)]
9	Change Management Plan	Ⓘ[1)]
10	Configuration Check Report	Ⓘ[2)]

Legends:

X: applicable
Ⓐ：submission for CCS approval；
①：submission for CCS information；
[1)]：submission prior to cyber security capability certification；
[2)]：submission after cyber security capability certification.

3.1.3.2 The specific requirements for submissions are as follows:

(1) CBS asset inventory, including:

① hardware asset inventory, including at least:
a) list of hardware components (such as host equipment, embedded equipment, network equipment);
b) brand/manufacturer
c) model/type
d) function/suage brief
e) physical interface (such as network, serial port)
f) name/type of system software (such as operation system, firmware)
g) version and patch level of system software
h) supported communication protocols.

② software assess inventory, including at least:
a) list of software components (such as application software, practical software)
b) hardware components installed
c) brand/manufacturer
d) model/type
e) function/usage brief
f) software version

(2) The System Network Topology is to describe network or data flow (source, destination, protocol, protocol details and physical implementation) with physical and logical topologies and is to include device name, IP, network zone boundary, etc.:

① The physical network topology describes the physical architecture of the system and can clearly show the connection and access relation between the network transmission medium and each access system and device, including:
a) All terminal and network devices, including redundant units;
b) Communication cables (network, serial port connection), including I/O communication unit;
c) Communication cables connected to other networks or systems.

② The logical network topology describes the network or data flow between system software components, including:
a) Communication terminals (such as workstations, controllers and servers);
b) Layout of network devices (switches, routers and firewalls) in the system;
c) Layout and access mode of terminals such as on-board workstations, servers and controllers;
d) Physical and virtual computers;
e) Physical and virtual communication lines;
f) Communication protocols.

(3) Description of security capability, specifying how CBS and the hardware and software components comply with the required security capability, including at least the following:

① Describe network interfaces with other CBS, including destination CBS, data flow, and communication protocols;

② Describes the network interface to an untrusted network. Describe how the interface meets additional requirements for connecting to an untrusted network and include relevant operating procedures or operator instructions

③ Describe the protection components of the security zone boundary in detail

④ How all CBS hardware and software meet the security capability requirements

⑤ Where the requirements cannot be fully met, effective compensation measures shall be provided

(4) The security capability test outline shall have a separate section for each applicable requirement and shall state the following:

① necessary test settings (i.e. to ensure repeatable tests with the same expected results)

② test device;

③ initial conditions;

④ test method, detailed test steps;

⑤ results evaluation criteria;

⑥ reference standard (if available).

(5) The Security Configuration Files are to ensure that the implementation of security features comply with the requirements of Chapter 4 and all the rules of the system integrators (i.e. user account, authorization, password policy, system security status, firewall rule, etc.), and contain the following:

① recommended configuration and default value of security features;

② Network data traffic limit value;

③ Open ports of device;

④ Configuration list of user access rights;

⑤ Setting of restricted access addresses by the system, such as system whitelist;

⑥ Remote user access right (where applicable);

⑦ Storage and backup methods of configuration files;

⑧ Protections of system configuration files from unauthorized access.

(6) The Secure Development Lifecycle Document is to include at least the contents required in 2.4.1.2 of this Guidelines, specifying the process and control measures of the supplier, and the software update and patches;

(7) The maintenance and verification plan shall include safety-related system maintenance and testing procedures, as well as a description of how the user can verify the correctness of the operation of the safety functions of the system in accordance with the requirements of Chapter 2 2.3.1.3 (3), including at least:

① maintenance contents;

② maintenance method;

③ maintenance intervals.

(8) information supporting cyber incident response and recovery plan are to, at least, include the following:

① Isolation location of the compromised system;

② A description of alarms and indications of cyber incidents or anomalies;

③ A description of main consequences possibly caused by cyber incidents;

④ Response options, prioritizing those which do not rely on either direct shutdown or transfer to local control, if any;

⑤ Local control information for locally operating a system that failed due to a cyber incident;

⑥ Instructions for obtaining evidence through audit records (refer to SR2.8 for the requirements of audit records);

⑦ Backup (refer to SR7.3 for relevant requirements);

⑧ Recovery (refer to SR7.4 for recovery and reconstruction requirements);

⑨ Controlled shutdown, rollback, reset, and restart schemes.

(9) Change of management plan:

① Clarify the responsibilities, scope and process of change management according to the change procedures.

(10) Configuration verification report, a report signed by the supplier, certifying that the supplier has completed the design, construction, test, and configuration and hardening of the security features in accordance with the guides of security configuration and hardening.

Section 2 Test and Verification

3.2.1 General Requirements

3.2.1.1 The relevant tests and verification shall be completed at CCS or CCS-approved test bodies according to the security level applied for the product and the product cyber security test program approved by CCS,

3.2.1.2 The test project shall cover the requirements applicable to the corresponding security level in Chapter 2 of this Guidelines, and the ship network firewall shall be implemented in accordance with the *Guidelines for Ship Network Firewall Inspection* of CCS.

3.2.1.3 The test of system/device is to include at least security vulnerability scanning or penetration testing, load or stress testing and network connectivity testing.

3.2.1.4 The test of network device is to include at least security vulnerability scanning or penetration testing, network storm testing, performance testing to verify the network security status and performance of the network system. The test of the network device can be integrated with that of the system device when the network device is the component of the system.

3.2.1.5 The network security vulnerability scanning of system/device is used to confirm the absence of high-risk items, or if present, prove that effective risk mitigation measures have been taken.

3.2.1.6 Relevant test items can be carried out by using test tools, or by checking configuration files to confirm that relevant device has corresponding protection capabilities, or by checking test results and reports.

3.2.1.7 If the specific application scenarios of the product in the ship system cannot be determined, CCS can verify the cyber security requirements in limited application scenarios. In order to complete the test and verification, CCS may also require the provision of necessary drawings, detailed data, test reports and verification related to the standards declared by the supplier, and the verification results in limited application scenarios can be issued after required inspection and test.

3.2.2 Test and Verification

3.2.2.1 The following test items are to be carried out in the presence of CCS surveyor:

(1) Check the conformity with product asset inventory, security configurations, network topology, interface, etc. before the testing;

(2) Check the security configuration of the system/device, especially the security configuration of network devices such as ship network firewall, router and switch;

(3) Carry out applicable testing on the device in accordance with 2.3.1-2.3.2 and 3.2.1.3-3.2.1.7;

(4) Depending on the basic security level of the system/device and the presence of remote connectivity or remote maintenance, determine the technical clauses to be met according to Section 3, Chapter 2, and then the test methods and verifiable criteria.

3.2.2.2 Security Vulnerability Scanning

(1) Comprehensive detection and vulnerability scanning are carried out for the product by technical means to locate the vulnerability and analyze the cause, and the results are taken as one of the conclusions of test and verification.

(2) After the vulnerability scanning, the applicant is to submit the test report to CCS for verification.

3.2.2.3 Penetration Testing

(1) Comprehensive penetration testing is carried out for the product by technical means, and the results are taken as one of the conclusions of test and verification.

(2) The security policy of the network under test is comprehensively tested in the penetration test environment established by the testing party, in order to actively analyze the vulnerability and technical defects of the network from the possible locations of security attacks.

(3) Penetration testing assists in understanding the current security situation by identifying security problems and facilitates threat and risk reduction through relevant operational planning.

(4) The object of penetration testing is the network system product to be connected to the ship network, and the testing is carried out in the following groups:

① Penetration of system and application functions;

② Database system penetration; and

③ Network device penetration.

(5) After the penetration testing, the applicant is to submit the test report to CCS for verification.

3.2.2.4 Network storm testing

(1) Network storm testing is carried out for the network device by technical means, and the results are taken as one of the conclusions of test and verification.

(2) A network storm refers to a situation in which a large number of broadcasts are replicated and data frames propagated in the network segment due to network topology design and connectivity problems or other reasons, resulting in degraded network performance and even network paralysis. Network storms are usually caused by improper configuration of network device, network card failure, incorrect network loop setting, network virus, malicious attack and other reasons.

(3) After the network storm testing, the applicant is to submit the test report to CCS for verification.

3.2.2.5 Network Connectivity Testing

(1) Network connectivity testing is carried out for the network system product by technical means to verify the operability and functionality of network device connection, and the results are taken as one of the conclusions of test and verification.

(2) After the testing, the applicant is to submit the test report to CCS for verification.

3.2.3 Changes

3.2.3.1 The Supplier/System Integrator is to define the classification of changes.

(1) Classify the change contents according to the expected impact possibly on the security capability;

(2) Define the relationship between the change classification and the software version/revision.

3.2.3.2 Any change affecting the product's security capability is to be submitted to CCS for approval, corresponding test is to be carried out if necessary.

3.2.3.3 A change description is at least to include the contents described in Table 3.2.3.3.

Change Description Information Table 3.2.3.3

Activity	Description
Purpose	Describe the reason for change.
Classification	Define the change classification according to the change policy.
Design	Describe and execute the required design activities, including updating relevant documents.
Version	Update the version according to the change policy.
Consequence	Analyze the possible impact of change.
Approval	Ensure acceptance of change by the supplier and client.
Implementation	Describe and execute required implementation activities.
Verification	Carry out relevant activities such as testing, acceptance, stakeholder witness and reporting according to the procedures.

Chapter 4 Ship Cyber Security Requirements

Section 1 General Provisions

4.1.1 General Requirements

4.1.1.1 Ship cyber security risks are to be managed, and an effective ship cyber security risk management system is to be established and implemented to maintain a certain degree of resilience of the ship network to cyber threats.

4.1.1.2 If the technical measures cannot meet the requirements due to limited conditions, appropriate management measures can be taken instead.

4.1.1.3 "Identify", "Protect", "Detect", "Respond" and "Recover" are the five functional elements supporting effective cyber risk management of ships. All cyber security requirements in this chapter are proposed based on these functional elements. They are defined as follows:

(1) Identify: Develop a comprehensive understanding of on-board systems, personnel, assets, data and other information.

(2) Protect: Develop and implement appropriate safeguards to protect the ship against cyber incidents and maximize continuity of shipping operations.

(3) Detect: Develop and implement appropriate measures to detect and identify the occurrence of a cyber incident on-board.

(4) Respond: Develop and implement appropriate measures and actions for a detected cyber incident on-board.

(5) Recover: Develop and implement appropriate measures and actions to restore any capabilities or services necessary for shipping operations that were impaired due to a cyber incident.

Section 2 Requirements for Class Notation M

4.2.1 General Requirements

4.2.1.1 The ship cyber security risk management system is to be incorporated into the security management system, so as to ensure that cyber security risks are at an acceptable level, and meet the expectations of interested parties (operators, users, regulators, etc.) for cyber security.

4.2.1.2 The security and environmental protection policy of the security management system is to include the content of ship cyber risk management.

4.2.1.3 The information on responsibilities and authorities of the security management system is to include those related to cyber risk management. Ship cyber security management organizations and posts are to be set up with specific management responsibilities assigned, and interested parties (including organizations and persons) are to be notified of the management responsibilities in writing.

4.2.1.4 The Company to which the ship belongs is to hold a valid DOC certificate complying with the ISM/NSM Code, and the ship is to be provided with a valid SMC certificate complying with the ISM/NSM Code.

4.2.1.5 The security management system may be established by referring to Appendix 2 to the *Guidelines, the Guidelines on Maritime Cyber Risk Assessment and Cyber Security Management System* of CCS, and *the Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3)* of IMO.

4.2.1.6 The latest and effective management system documents and relevant personnel data,

management records (including reports, logs, record forms, etc., if any) are to be available at any time on board.

4.2.1.7 In case of any major change, relevant documents are to be submitted to CCS to confirm whether the class notations continue to be valid.

4.2.1.8 In case of any major cyber incident, CCS is to be notified in time, and information, handling measures and solutions of the incident are to be submitted.

4.2.2 Management System

4.2.2.1 An effective security risk management system is a risk-based management system for sustainable improvement.

4.2.2.2 The management system is to include the contents of operation and maintenance management, including but not limited to:

(1) Personnel management, including employment and demission, training and management, third-party personnel, etc.;

(2) Risk management, including vulnerability identification and patching, risk assessment, etc.;

(3) Security inspection, including routine inspection and comprehensive inspection;

(4) Change management, including change declaration, approval and implementation;

(5) Incident and emergency management, including development and drill of emergency plan, incident reporting, response and improvement, etc.;

(6) Backup and recovery management, including development of backup policy, backup implementation and recovery;

(7) Service provider management, including product provider, communication service provider and outsourcing O&M service provider;

(8) Password management, including adopted password standards, relevant technologies and products;

(9) Environmental management, including boarding access, machine room maintenance, etc.;

(10) Asset management, including creation and maintenance of asset inventory, asset addition, update and scrapping, etc.;

(11) Media management, including registration management, physical transmission, use and scrapping;

(12) Device management, including device maintenance, demobilization/return, scrapping, interface control, etc.;

(13) Network and application system security management, including account management, installation and upgrade, configuration management, access control, malicious code protection, operation and maintenance, etc.;

(14) Cloud computing management (if any), including platform selection, data leakage prevention, etc.;

(15) Mobile Internet management (if any), including wireless access control, etc.;

(16) IoT management (if any), including the whole process management of addition and change of sensor nodes and gateway nodes, as well as confidentiality management and availability management;

(17) Big data management (if any), including digital asset security management policy, classified and graded protection policy, automatic desensitization, etc.

4.2.2.3 In the event of O&M management activities, management records are to be made for important matters, including but not limited to:

(1) Cyber security awareness and skills training/education for relevant personnel;

(2) Security management of assets, including asset registration and change;
(3) Daily O&M, emergency preparation, emergency response, periodic inspection/testing, etc.;
(4) Security management of service providers;
(5) Risk assessment of ship network system;
(6) Audits and reviews (internal and/or external) of ship cyber security management.

4.2.2.4 In case of new construction and/or major reconstruction of ship network system, such as reconstruction of network infrastructure, and development and launching of new application systems, the management system is also to incorporate the construction management, including but not limited to:
(1) Requirement determination, including the preparation, demonstration and adoption of requirements;
(2) Planning and design, including scheme preparation, selection of security measures and scheme demonstration;
(3) Project implementation, including determination of responsible person, formulation and implementation of implementation plan, and third-party supervision;
(4) Product procurement and use, including compliance and model selection;
(5) Software development, including coding, security testing, release/update, etc.;
(6) Test acceptance, including preparation and implementation of test plan;
(7) System delivery, including delivery list, application training, etc.
(8) Cloud service provider management (if any), including compliance, service protocol, data leak protection, etc.;
(9) Mobile Internet management (if any), including software distribution channels and developers;
(10) Big data management (if any), including compliance, data security, etc.

4.2.2.5 In the event of construction management activities, management records are to be made for important matters, including but not limited to:
(1) Cyber security awareness and skills training/education for relevant personnel;
(2) Procurement of network products (software, hardware, etc.);
(3) Software development;
(4) Important engineering nodes, such as integration test, security test, on-board installation, trial trip test, acceptance and delivery;
(5) Selection of operator after cyber delivery.

4.2.3 Risk Management

4.2.3.1 The measures in Appendix 1 to the *Guidelines on Maritime Cyber Risk Assessment and Cyber Security Management System* of CCS are to be implemented.

4.2.3.2 Training requirements in cyber security are to be identified and incorporated into the training program of the management system.

4.2.3.3 The asset inventory and network topology for ship cyber risk management are to be identified and established in an appropriate classification manner, and maintained in real time.

4.2.3.4 For risk assessment of identified assets, refer to Appendix 2 to the *Guidelines on Maritime Cyber Risk Assessment and Cyber Security Management System* of CCS and Appendix 1 to the Guidelines.

4.2.3.5 Appropriate security measures are to be developed and implemented for all identified ship, personnel and environmental risks.

4.2.3.6 For cyber incidents, appropriate measures are to be developed and implemented for

detection, response, recovery and recurrence prevention.

Section 3 Requirements for Class Notations P and S

4.3.1 General Requirements

4.3.1.1 The ship network design is to be based on the principle of risk assessment to meet the business expectations of the ship network.

4.3.1.2 For the correspondence between all cyber security requirements in this section and the five functional elements defined in 4.1.1.3, please see Table 4.3.1.2 below.

Correspondence between Functional Elements of Cyber Risk Management and Ship Cyber Security Requirements Table 4.3.1.2

Functional Element	Cyber Security Requirement
Identify	Asset inventory
Protect	Asset protection, asset disposal, physical access control, network defense, security zone, boundary protection, network redundancy, communication security, intrusion prevention, authentication, access control, malicious code protection, remote access, remote maintenance, wireless communication, mobile media security, change management, vulnerability management
Detect	Network operation monitoring and security audit
Respond	Incident response
Recover	Recovery and backup

4.3.2 Asset inventory

No.	Requirements	SL0	SL1	SL2	SL3	SL4
4.3.2.1	An inventory of the asset of each CBS, the network connecting shipboard and shore CBS within the scope of application of this Guidelines shall be provided, which shall: ① include all CBSs in 1.1.1.3 (if applicable); ② be updated during the whole life of the ship, the update record shall include new vulnerabilities that may be introduced by software and hardware modifications and changes in functional dependencies or connections. ③ If the list includes confidential information (such as IP addresses, protocols, port numbers), special measures should be taken to limit access to such information to authorized personnel only.	√	√	√	√	√
4.3.2.2	The asset list shall include all hardware and software to the extent applicable, including at least the information listed in 3.1.3.2 (1) and the system category and security zone to which CBS belongs; The CBS software shall be maintained and updated in accordance with the software maintenance and update management policy established by the ship owner in the Ship Network Security Management Plan.	√	√	√	√	√

4.3.3 Asset Protection

No.	Requirements	SL0	SL1	SL2	SL3	SL4
4.3.3.1	Standardized requirements for asset management and asset category and identification shall be developed, and requirements for the use, physical transmission, storage, protection and disposal of assets shall be clarified.			√	√	√
4.3.3.2	The backup of critical system data (whether temporary or permanent) is to be protected by the same means as the original data.				√	√

4.3.3.3	Critical or sensitive information stored on portable devices is to be encrypted using encryption algorithms that have been best practiced by the industry.				√	√

4.3.4 Asset Disposal

No.	Requirements	SL0	SL1	SL2	SL3	SL4
4.3.4.1	Procedures for the safe disposal of assets are to be developed and are to include at least the following: ① Make clear that authorization has been obtained before data deletion; ② Develop necessary security measures for critical data to prevent information leakage during asset disposal; ③ Clarify the measures for asset disposal to include at least the time of asset removal, verification and recording method of asset return, and identity and role of the person authorized for asset removal; ④ Implement necessary security measures for assets or data to be destroyed to ensure that the assets or data on the storage device, which are protected before the destruction in the storage device, cannot be reconstructed or restored after the destruction.					√

4.3.5 Physical Access Control

No.	Requirements	SL0	SL1	SL2	SL3	SL4
4.3.5.1	Access to CBSs and networks within the scope of application of the Guidelines and all information stored on such systems are only to be allowed to authorized personnel, software processes and devices, based on their responsibilities or their intended functionality.	√	√	√	√	√
4.3.5.2	CBSs of category II and III are normally to be located in controlled space to prevent unauthorized access, or are to be installed in lockable cabinets or consoles. Such locations are to be however easily accessible to the crew and various interested parties who need to access to CBSs for installation, integration, maintenance, repair, replacement, disposal, etc., so as not to hamper effective and efficient operation of the ship.	√	√	√	√	√
4.3.5.3	Visitors such as authorities, technicians, agents, port and terminal officials, and owner representatives are to be restricted regarding access to computers on-board whilst on board, e.g. by allowing access under supervision.	√	√	√	√	√
4.3.5.4	Access points to on-board category II and III CBS networks are to be physically and/or logically blocked except when connection occurs under supervision or according to documented procedures, e.g. for maintenance.	√	√	√	√	√
4.3.5.5	Independent computers isolated from all on-board networks, or other networks, such as dedicated guest access networks, or networks dedicated to passenger recreational activities, are to be used in case of occasional connection requested by a visitor (e.g. for printing documents).	√	√	√	√	√

No.	Requirements	SL0	SL1	SL2	SL3	SL4
4.3.5.6	The access right is to be taken back after the visitor leaves or the authorized crew's access right expires.		√	√	√	√
4.3.5.7	The entrance and exit of the machine room (or similar places) are to be equipped with an electronic access control system to control, identify and record the personnel entering.			√	√	√
4.3.5.8	Physical access to CAT-II and CAT-III CBSs is to be logged, including at least: ① Identity of the visitor; ② Time of access; and ③ Purpose of access.				√	√
4.3.5.9	Physical security devices for physical access control (e.g. surveillance cameras, intrusion detectors, electronic locks) are to: ① Have strong authentication method, such as password, smart card and token. If a password is used, it is to be changed from default and kept non-trivial and updated regularly. ② Be regularly tested to ensure that it is kept working in normal operating state; ③ Have its recorded data maintained and accessed with authorization.					√

4.3.6 Network Defense

No.	Requirements	SL0	SL1	SL2	SL3	SL4
4.3.6.1	The network should be prevented from excessive data traffic and other events that may damage the service quality of network resources	√	√	√	√	√
4.3.6.2	The CBS applicable to this Guideline should be configured in accordance with the “minimum features” principle, that is, provide only necessary functions, restrict the use of non-essential functions, and disable or restrict non-essential functions, ports, protocols, services, and default sharing	√	√	√	√	√
4.3.6.3	The network design should meet the expected data traffic volume and minimize the risk of denial of service (DoS) and network storms/high traffic. The data traffic estimation should at least consider the network capacity, data speed and data format of the intended application	√	√	√	√	√

4.3.7 Security Zone

No.	Requirements	SL0	SL1	SL2	SL3	SL4
4.3.7.1	All CBSs within the scope of application of the Guidelines are to be divided into security zones and meet the same security requirements. The network(s) of a security zone are to be logically or physically segmented from other zones or networks.	√	√	√	√	√
4.3.7.2	A security zone can contain multiple CBS and networks, all of which must meet the applicable requirements in this chapter and Chapter 2 of this Guidelines	√	√	√	√	√
4.3.7.3	The ship networks are to be grouped into different security zones according to factors such as system category (Category I, II or III), asset importance and system capabilities, and the following requirements are to be met: ① The CBS that provides security functions shall be classified into a separate security zone and physically segmented with other security zones ② Navigational and communication systems shall not be in the same safety area as mechanical and cargo systems, and if navigational and/or radio communication systems are approved in accordance with other equivalent criteria in Article 1.1.1.5, such systems shall be placed in a separate safety area ③ Wireless devices are to be grouped in a separate security zone; ④ CBS and networks outside the scope of application of this Guideline shall be physically segmented from the safe areas required by this Guidelines . Alternatively, if these systems meet the equivalent requirements of a security zone, they may be considered part of that security zone ⑤ It should be possible to manually isolate a secure area without affecting the main function of CBS in the secure area ⑥ In the definition of security control policies, the functions allowed to access or operate on the network are to be associated to the roles.	√	√	√	√	√
4.3.7.4	Different zones are to be provided between OT systems and IT systems, and one-way technical isolation means is to be adopted between zones.				√	√
4.3.7.5	A DMZ is to be established to reduce direct communication between trusted and untrusted networks.					√

4.3.8 Boundary Protection

No.	Requirements	SL0	SL1	SL2	SL3	SL4
4.3.8.1	Security zones are to be protected by firewalls or other equivalent means as required by 4.3.7 and are to be capable of monitoring and controlling zone boundary communications.	√	√	√	√	√
4.3.8.2	Access control rules are to be set at network boundary or between zones according to the access control policy. Controlled interfaces deny all communications by default unless otherwise permitted.	√	√	√	√	√
4.3.8.3	Access control rules should be set between network boundaries or zones according to the access control policy, in case of default, the controlled interface shall deny all communications except being permitted		√	√	√	√
4.3.8.4	Redundant or invalid access control rules are to be deleted to optimize the access control list.		√	√	√	√
4.3.8.5	The source address, destination address, source port, destination port and protocol are to be checked to allow/deny packet in and out.		√	√	√	√
4.3.8.6	It is to be possible to allow/deny data flow in and out according to the session state information.		√	√	√	√
4.3.8.7	Access control devices are to be deployed between the OT system and the IT system, and access control policy is to be configured to prohibit any universal network services such as E-Mail, Web, Telnet, Rlogin and FTP traversing the zone boundary.		√	√	√	√
4.3.8.8	An alarm is to be given in time when the boundary protection mechanism between security zones fails.		√	√	√	√
4.3.8.9	It is to be possible to check for and restrict the connection of unauthorized devices to the ship's internal network without permission.				√	√
4.3.8.10	It is to be possible to check for and restrict the unauthorized connection of on-board CBSs to the ship's external network.				√	√
4.3.8.11	Where the boundary protection mechanism fails, all traffic is to be prohibited from passing through, and this fail-close mode is not to impair the security functionality of the system.				√	√
4.3.8.12	Access control based on application protocols and application content is to be implemented for data flows in and out of the network.					√

4.3.9 Network Redundancy

No.	Requirements	SL0	SL1	SL2	SL3	SL4
4.3.9.1	Hardware redundancy of critical network, computing and storage devices and connecting cables is to be provided to ensure the availability of the system.				√	√
4.3.9.2	The redundant system is to have sufficient self-diagnostic capability in the event of a failure to effectively transfer to the standby unit.				√	√
4.3.9.3	Two different firewalls are to be provided for communication with systems affecting human safety or ship safety via firewall. Both of the firewalls are to operate in real time and be highly available. They are to be so arranged that when one fails or a cyber incident occurs, the other can still maintain the security of the ship network.					√

4.3.10 Communication Security

No.	Requirements	SL0	SL1	SL2	SL3	SL4
4.3.10.1	Where cryptographic techniques are employed, recognized industry practices or best practices should be adopted, and the encryption scheme should describe the algorithm, protocol, and key used (including key length, expiration date) and key usage	√	√	√	√	√
4.3.10.2	The ship network should be able to prioritize network resources for high-priority CBS		√	√	√	√
4.3.10.3	Cryptographic technology should be used to ensure the integrity of data during communication				√	√
4.3.10.4	The responsible of crew member shall be automatically notified when the integrity of the data is compromised				√	√
4.3.10.5	Cryptographic technology should be used to ensure the confidentiality of data in the communication process					√

4.3.11 Intrusion Prevention

No.	Requirements	SL0	SL1	SL2	SL3	SL4
4.3.11.1	Cyber attacks are to be monitored at critical network nodes by using IDS, IPS and other systems.		√	√	√	√
4.3.11.2	Where an attack is detected, the attack source IP, attack type, attack target, and attack time are to be recorded, and an alarm is to be given in case of a serious intrusion event.		√	√	√	√
4.3.11.3	The access mode or access network address range of the network management terminal is to be limited.		√	√	√	√
4.3.11.4	The validity of data input is to be verified to ensure that the contents input via the human-machine interface or communication interface comply with the system setting requirements.			√	√	√

4.3.12 Authentication

No.	Requirements	SL0	SL1	SL2	SL3	SL4
4.3.12.1	CBS shall be able to authenticate the user's identity and	√	√	√	√	√

	meet the requirements of 2.3.1.1 (1) SR1.1 and SR1.1RE2					
4.3.12.2	Users should be identified and logon users should be identified. Identity identifiers are unique, and identity authentication information has complexity requirements and should be changed regularly			√	√	√
4.3.12.3	Two or more combinations of authentication technologies, such as password, cryptography, and biotechnology, should be used to authenticate users, and at least one of the authentication technologies should be implemented by cryptography					√

4.3.13 Access control

No.	Requirements	SL0	SL1	SL2	SL3	SL4
4.3.13.1	The CBS and its associated information should be protected through access control lists for file systems, networks, applications, or databases. Login accounts shall be assigned according to the roles and responsibilities of ships and shore-based personnel, limited for periods of activation, and cancelled when no longer needed	√	√	√	√	√
4.3.13.2	Access control policies should not adversely affect the functionality of the system, and CBS requiring strong access controls can be defended with strong encryption keys or multi-factor authentication	√	√	√	√	√
4.3.13.3	Administrator privileges that allow full access to system configurations and all data should only be granted to trained crew members who are required by their duties	√	√	√	√	√
4.3.13.4	All users have only the minimum permissions necessary to implement their functions, that is, operation permissions should not be higher than the level of permissions required to complete the scheduled task	√	√	√	√	√
4.3.13.5	The default permission configuration for all new account should be as low as possible. Allow permissions to be elevated when necessary, such as using interim permissions or one-time credentials. User and process account should be audited periodically to prevent permissions from accumulating over time	√	√	√	√	√

4.3.14 Malicious Code Protection

No.	Requirements	SL0	SL1	SL2	SL3	SL4
4.3.14.1	The CBSs within the scope of application of the Guidelines are to be protected against malicious code such as viruses, worms, trojan horses and spyware.	√	√	√	√	√
4.3.14.2	On CBSs having an operating system for which industrial-standard anti-malware is available and maintained up-to-date, anti-malware is to be installed and regularly maintained, unless the installation of such software impairs the ability of CBS to provide the functionality and level of service required (e.g. for CAT-II and CAT-III CBSs performing real-time tasks).	√	√	√	√	√
4.3.14.3	For CBS that cannot install anti-malicious code software, use operating procedures, physical protection, or the methods recommended by the manufacturer to protect them	√	√	√	√	√
4.3.14.4	Malicious code is to be detected and cleared at critical network nodes, and the upgrade and update of malicious code protection mechanism is to be maintained.		√	√	√	√
4.3.14.5	. Spam is to be detected and prevented at critical network nodes, and the upgrade and update of antispam mechanism is to be maintained.		√	√	√	√
4.3.14.6	The system is to have the capability to manage the malicious code protection mechanism, which is usually implemented by the centralized management of endpoint infrastructure or SIEM solution.				√	√

4.3.15 Remote Access

No.	Requirements	SL0	SL1	SL2	SL3	SL4
4.3.15.1	User manuals should be provided to control remote access to shipboard IT and OT systems, and the roles and permissions of those accessing them should be clear	√	√	√	√	√
4.3.15.2	The IP address of any shipboard CBS should not be exposed to untrusted networks	√	√	√	√	√
4.3.15.3	Untrusted networks should be communicated over a secure connection (such as a VPN) with endpoint authentication, integrity protection, network or transport layer authentication, and encryption capabilities, and the confidentiality of authorization information should be ensured	√	√	√	√	√
4.3.15.4	The on-board CBS is to be capable of: ① terminating connection on board. No remote access is to be made until it has been expressly accepted by the crew; ② controlling the interruption of remote sessions so as not to affect the security functions of the OT system or the integrity and availability of OT system data; ③ providing logging function to record all remote access incidents and keep them for a period of time for	√	√	√	√	√

No.	Requirements	SL0	SL1	SL2	SL3	SL4
	offline review of remote connections, e.g. after detection of a cyber incident					
4.3.15.5	Any access through untrusted networks should be monitored (e.g. logging, displaying, alerting) and controlled (e.g. denial, restriction)	√	√	√	√	√
4.3.15.6	When establishing remote connections from specific locations of the owner, operator and supplier for ship control, the following requirements should be met: ①The position of the operating control right should be clearly displayed at the ship end and the remote control end ②The ship and the remote control end should have a response mechanism to ensure communication connection, and when the remote connection is disconnected, the ship end should be prompted ③Priority should be given to transmission of control signals		√	√	√	√
4.3.15.7	The source address of communication with shipboard CBS should be restricted to avoid the attack behavior of unfamiliar addresses			√	√	√

4.3.16 Remote Maintenance

No.	Requirements	SL0	SL1	SL2	SL3	SL4
4.3.16.1	When remote access is used for remote maintenance, in addition to the requirements of 4.3.15, the following requirements are also to be met: ① Documentation is to be provided on how to interface and integrate with the shore; ② Patches for maintenance and updates are to be tested and evaluated before installation to ensure they are effective and will not cause unacceptable impact or a cyber incident; ③ The supplier is to provide a confirmation report on the above contents before the remote update; ④ A support plan is to be developed by the supplier and made available to the shipowner, for details, refer to 2.4.1.2 (4), (5) and (6); ⑤ During remote maintenance, authorized personnel should be able to interrupt and terminate sessions at any time, and can roll back to the previous security configuration of the system; ⑥ Multi-factor identity authentication is required for any user to access the CBS within the scope of the Guidelines from an untrusted network; ⑦ When the number of access attempts reaches a preset value, it is to be prevented from further authentication; ⑧ If the remote maintenance is interrupted for some reason, the access will be terminated by automatic logout	√	√	√	√	√

4.3.17 Wireless Communication

No.	Requirements	SL0	SL1	SL2	SL3	SL4
4.3.17.1	Wireless communication networks should be designed, implemented and maintained to protect transmitted information from manipulation or disclosure, network events from spreading to other control systems, and access to wireless communication networks should be restricted: ① Only authorized users can access the wireless network; ② Only authorized processes and devices can communicate over wireless networks	√	√	√	√	√
4.3.17.2	Encryption mechanisms, including encryption algorithms, key strength, etc., in accordance with industry's best practices are to be adopted to ensure the integrity and confidentiality of information transmitted via the wireless network	√	√	√	√	√
4.3.17.3	Devices on the wireless network can only communicate via the wireless network (i.e. they are not to be "dual homed")	√	√	√	√	√
4.3.17.4	Class III systems should not employ wireless data links unless specifically considered after engineering analysis by CCS against an acceptable international or national standard	√	√	√	√	√
4.3.17.5	The OT system controlled by wireless communication technology is to be able to identify the unauthorized wireless device in its physical environment and alert and control attempts to access or interfere with the control system (such as denial, restriction).				√	√

4.3.18 Mobile Media Security

No.	Requirements	SL0	SL1	SL2	SL3	SL4
4.3.18.1	A policy for the use of mobile media should be established and restricted to authorized personnel only. Data uploaded to or downloaded from CBS via mobile media should be scanned to check the mobile media for the presence of malware and/or verify the legitimacy of the software through digital signatures and/or watermarks	√	√	√	√	√
4.3.18.2	Only authorized mobile media can connect to CBS and meet the requirements of 2.3.1.2 (3) SR2.3. If the CBS cannot meet the requirements, physically block the interface	√	√	√	√	√
4.3.18.3	Automatic execution of software code by portable devices should be prohibited	√	√	√	√	√
4.3.18.4	Mobile and portable devices that use wireless connections shall meet the requirements related to 4.3.17	√	√	√	√	√
4.3.18.5	Ports that are logically or physically blocked should be clearly identified		√	√	√	√

4.3.19 Network Operation Monitoring

No.	Requirements	SL0	SL1	SL2	SL3	SL4
4.3.19.1	The ship network to which the Guidelines apply is to be	√	√	√	√	√

	continuously monitored and alarms raised when anomalies, failures or degradation of capacity are detected in the network					
4.3.19.2	The network monitoring is at least to include the following aspects: ① Network traffic, such as abnormal network traffic; ② Network connection, including communication link fault; ③ Device management activities, such as access exceptions, operating system attack incidents, and configuration changes; ④ Connection of unauthorized mobile devices; ⑤ If the network bandwidth utilization exceeds the exception threshold specified by the product supplier, an alarm is to be raised ⑥ Security events must have logs that meet the requirements of 2.3.1.2 (8) SR2.8	√	√	√	√	√
4.3.19.3	The IDS is to meet the following requirements if it is installed: ① The IDS is to be qualified by the supplier of the corresponding CBS; ② The IDS is to provide passive rather than active protection, as active protection may affect CBS performance; ③ Relevant personnel are to be trained and qualified for the IDS.	√	√	√	√	√
4.3.19.4	CBS and networks within the scope of application of this Guideline should be able to diagnose the security features required by this Guideline, The device's self-diagnosis function or network monitoring tools, such as ping, traceroute, ipconfig, netstat, nslookup, Wireshark, and nmap may be used to diagnose the integrity and security status of the CBS, and provide the means to maintain security features for safe operation of the ship	√	√	√	√	√

4.3.20 Security audit

No.	Requirements	SL0	SL1	SL2	SL3	SL4
4.3.20.1	Log management is to be performed to allocate storage space as required, and at least one minimum ship survey period is to be preserved		√	√	√	√
4.3.20.2	The audit record is to include the date and time of the incident, user, incident type, whether the incident is successful or not, and other information related to the audit		√	√	√	√
4.3.20.3	The system is to provide read-only access to audit logs for authorized users		√	√	√	√
4.3.20.4	Security audits are to be carried out at the network boundaries and important network nodes, covering every user on important user behaviors and important security incidents, such as access control, error requests, operating		√	√	√	√

No.	Requirements	SL0	SL1	SL2	SL3	SL4
	system incidents, backup and recovery incidents, configuration changes, potential detection activities, etc.					
4.3.20.5	The audit record is to be protected and backed up regularly to avoid unexpected deletion, modification or overwriting			√	√	√
4.3.20.6	As part of the audit, the storage capacity is to be monitored and an alarm is to be sent to relevant personnel before the capacity threshold is exceeded, so as to prevent the loss of the audit record				√	√
4.3.20.7	Behavior audit and data analysis are to be conducted separately for user behaviors such as remote access and Internet access				√	√
4.3.20.8	Centralized management is to be conducted for audit incidents. For example, SIEM technology is used to aggregate log data, security alarms and incidents to provide real-time analysis for security monitoring				√	√
4.3.20.9	Time source is to be protected against unauthorized changes in case of any change, the incident is to be recorded					√

4.3.21 Incident response

No.	Requirements	SL0	SL1	SL2	SL3	SL4
4.3.21.1	The Ship Cyber Incident Response Plan is to be developed by the shipowner, including a set of pre-set instructions or procedure files for detecting, responding to, and limiting the consequences of a network incidents	√	√	√	√	√
4.3.21.2	The parties involved in the design and construction phase of the vessel should provide the owner with information to complete the development of the incident response plan at the time of the first annual survey. The incident response plan shall be kept up to date (if maintained) during the ship's operation	√	√	√	√	√
4.3.21.3	The incident response plan should provide procedures to limit the impact to the initial network segment by notifying the competent authorities, reporting the necessary evidence of the incident and taking timely corrective action in response to the detected network incident. The plan should contain at least the following information: ① Isolation breakpoint of the damaged system; ② Alarm and indication of network incidents or network anomalies; ③ Possible consequences of network incidents; ④ Response options, with priority given to options that do not disconnect the system or transfer to independent or local control (if any); ⑤ Independent and local control information for compromised systems for independent operation of systems that fail due to a network incident (if applicable)	√	√	√	√	√
4.3.21.4	The incident response plan is to be maintained in hard copy	√	√	√	√	√

No.	Requirements	SL0	SL1	SL2	SL3	SL4
	to prevent complete loss of electronic storage devices					
4.3.21.5	The CBS for local backup control required by SOLAS Chapter II-1 Article 31 shall be independent of the main control system and include the necessary human machine interface to enable effective local operation	√	√	√	√	√
4.3.21.6	The CBS used for local control and monitoring should be independent and not rely on communication with other CBS to achieve its intended operation	√	√	√	√	√
4.3.21.7	If the local control and surveillance system communicates with the remote control system or other CBS over the network, it shall be designated as a separate security zone and meet the relevant requirements of Section 4.3.7 and 4.3.8 regarding area division and border protection. In special cases, special consideration may be given with CCS consent.	√	√	√	√	√
4.3.21.8	If network isolation is required for incident response, the following requirements are to be met: ① Communication with a certain network segment can be manually or automatically terminated, such as physically isolate a network segment according to the procedure, for example, by operating a physical ON/OFF switch or taking similar actions on network devices, or by disconnecting a router/firewall cable. There are to be instructions and clear markings on the device to allow personnel to isolate the network in an effective manner; ② The impact of data of a single system on system function and operation correctness (including security) are to be identified. It should be clarified how data or functional inputs will be compensated for when system isolation is marked	√	√	√	√	√
4.3.21.9	If a cyber incident affects a system or network in such a way that it cannot provide the expected service as required, the affected system or network is to be able to roll back to the lowest risk state. Rollback measures may include: ① Completely stop the system or rollback to other pre-defined secure status; ② Disengage the system; ③ Transfer of control privilege to another system or operator; ④ Other compensation measures;	√	√	√	√	√
4.3.21.10	The ship shall be restored to a state of minimum risk within a time frame sufficient for the vessel to remain in a safe state	√	√	√	√	√
4.3.21.11	Vendors and integrators should consider the ability of the system to fall back to the lowest risk state beginning in the design phase	√	√	√	√	√

4.3.22 Recovery and backup

No.	Requirements	SL0	SL1	SL2	SL3	SL4
4.3.22.1	The CBS to which this guidance applies should have recovery and backup capabilities to enable the ship to quickly and safely return to sailing and operational status following a cyber incident	√	√	√	√	√
4.3.22.2	The owner shall develop a ship network event recovery plan to support the return of CBS to operational status after an interruption or failure due to a network event	√	√	√	√	√
4.3.22.3	The various parties involved in the design and construction phase of the vessel should provide information to the owner so that the development of the recovery plan can be completed at the time of the first annual survey. The recovery plan should be kept up to date during the ship's operation (e.g. during maintenance)	√	√	√	√	√
4.3.22.4	The recovery plan should be easy for crew and outsiders to understand and include the necessary instructions and procedures to ensure the recovery of the failed system. If shore support is required, shore contact details should be provided. In addition, the necessary software recovery media or tools should also be provided on board	√	√	√	√	√
4.3.22.5	In the development of the recovery plan, individual systems and subsystems are to be considered comprehensively, and the following recovery objectives are to be developed: ① System recovery: The methods and procedures for recovering communication capability are to be specified according to the recovery time objective (RTO). RTO is the time required to recover the required communication links and processing capacity. ② Data recovery: The methods and procedures for recovering the data required for the safe state of the OT system and the safe operation of the ship are to be specified according to the Recovery Point Objective (RPO). RPO is the maximum time for tolerable data missing	√	√	√	√	√
4.3.22.6	Once the recovery objective has been determined, a list of potential network events should be created and a recovery plan based on the list should include the following information: ① A complete and up-to-date logic network diagram; ② Current configuration information of all components; ③ Procedures for restoring a failed system without interrupting redundant, independent, or local control; ④ Procedures for backing up and storing information securely; ⑤ List of responsible personnel responsible for restoring the faulty system;	√	√	√	√	√

No.	Requirements	SL0	SL1	SL2	SL3	SL4
	⑥ Communicate program and external technical support contact lists, including system support vendors, network administrators, etc					
4.3.22.7	The recovery plan should prioritize the operation and navigation of the ship to ensure the safety of those on board	√	√	√	√	√
4.3.22.8	Personnel responsible for cyber security and assisting in cyber incidents are to have access to the hard-copy recovery plan on board and ashore	√	√	√	√	√
4.3.22.9	Recovery Plan personnel should perform recovery operations to avoid destroying important information and evidence about the cause of the incident (such as erasing drives). Where necessary, professional cyber incident response support should be available to assist in preserving evidence while restoring operational capability	√	√	√	√	√
4.3.22.10	The shipowner shall make a backup plan, which shall include backup scope, backup method and frequency, storage medium and retention period. The information and facilities provided by the backup plan should be sufficient for the system to recover from network events and for the backup to be regularly maintained and tested	√	√	√	√	√
4.3.22.11	Ensure that data can be recovered from secure copies or media	√	√	√	√	√
4.3.22.12	Using offline backups to reduce the impact of malware on online backups is to be considered	√	√	√	√	√
4.3.22.13	The CBS and network are also to have the following functions: ① Controlled shutdown, which allows other connected systems to commit/roll back suspended transactions, terminate processes, close connections, etc., so that the whole system is in a safe, consistent and known state; ② Reset, which guides the system to complete the shutdown, clear memory and reset the device to its initialization state; ③ Rollback, which returns the system to a previous configuration and/or state to recover the integrity and consistency of the system; ④ Restart, which launches and reloads a new mirror image of all software and data from a read-only source (e.g., after a rollback operation). The restart time is to be compatible with the expected service of the system and is not to put other systems or their affiliated systems in an inconsistent or unsafe state Personnel on board shall be provided with documentation on how to perform the above actions to quickly and safely recover from possible damage caused by a cyber incidents	√	√	√	√	√

4.3.23 Change Management

No.	Requirements	SL0	SL1	SL2	SL3	SL4
4.3.23.1	Change management is to be carried out and changes are to be made according to 2.6.10 of Section 6, Chapter 2 of Part 7 of the Classification Rules of Steel Sea-going Ships	√	√	√	√	√

4.3.24 Vulnerability Management

No.	Requirements	SL0	SL1	SL2	SL3	SL4
4.3.24.1	Necessary measures are to be taken to identify security vulnerabilities and hazards, and the security vulnerabilities and hazards found are to be fixed in a timely manner or fixed after assessment of the possible impact		√	√	√	√
4.3.24.2	Vulnerability management is to keep updating by maintaining the functions, configuration, operation, software, firmware, operation code, etc. of the device, and is at least to include the following measures: ① Record the current installation version of the device; ② Regularly determine the upgrades and renewals available for each device; ③ Evaluate patches to ensure that they do not negatively affect the reliability and operability of the device or system (by testing in a simulated environment); ④ Install patches in an appropriate scenario (e.g., one will not cause unplanned downtime, interruption, etc.); ⑤ Update the asset inventory information (such as version information and functions) in time after the patches are installed.		√	√	√	√
4.3.24.3	Vulnerability scanning is to be done regularly and patches or other mitigating measures are to be implemented to reduce the security vulnerabilities in the system.		√	√	√	√

Chapter 5 Ship Cyber Security Survey

Section 1 General Provisions

5.1.1 General Requirements

5.1.1.1 This chapter applies to ships intended to obtain class notations of Cyber Security (M, P/S).

5.1.1.2 The ship cyber security survey may be carried out concurrently with the surveys of the same type, i.e. the initial classification, annual and special survey specified in the CCS rules.

5.1.2 Plans and Documents

5.1.2.1 For a ship applying for ship cyber security class notation (M) , Documents of Systems Related to Ship Cyber Risk Management are be submitted in accordance with requirements of Section 2 Chapter 4 of the Guidelines.

5.1.2.2 For a ship applying for ship cyber security class notations (P[SL0]) and Cyber Security(S[SLx]), the following plans and documents are to be submitted:

(1) product plan that has been approved as required by 3.1.3 of the guidelines;

(2) Ship asset inventory. The Ship Asset Inventory is to contain all systems and devices within the applicable scope of the Guidelines. The Ship Asset Inventory is a collection of system asset inventories. Each system is to have a separate asset inventory, as shown in Figure 5.1.2.2. Besides, the network devices delivered by the system supplier and in compliance with the requirements in Chapter 4 of the Guidelines shall be included in the ship asset inventory.

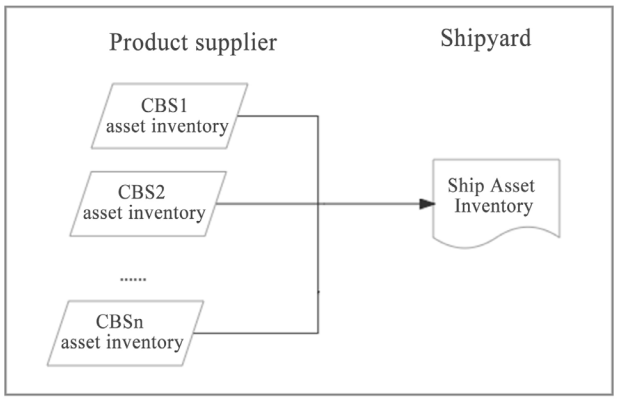

Fig. 5.1.2.2 Ship Asset Inventory

(3) Network Topology Diagram, which is a block diagram that identifies the physical or logical connections between the various on-board CBSs and between the CBSs and external devices or networks. The Network Topology Diagram is to be able to clearly mark the security zone and the physical location of each CBS.

(4) The Manual of Network Security Design shall at least include the following:

① Clearly identify the security zone and each CBS contained in the network topology diagram;

② Describe the security zone and the CBS contained therein of the network topology diagram;

③ Describe the communication and characteristics between CBSs in different security zones, including zone boundary device and traffic allowed to pass through the zone boundary (such as firewall rules);

④ Describe the communication and characteristics between the security zone and untrusted networks, including serial communication and IP-based communication purposes and characteristics (such as protocol and data flow), zone boundary devices, and traffic allowed through zone boundaries (such as firewall rules);

⑤ Wireless network design, explaining the wireless network design scheme, including how to achieve a separate security zone, zone boundary equipment and the traffic allowed to pass through the zone boundary (such as firewall rules);

⑥ Physical access control measures, for the CBS that needs immediate access, if its human-machine interface is already located in the physical access control area, there is no need to carry out identification and authentication. Such equipment shall be described in this document;

⑦ Malicious code protection mechanism, outline the malicious code protection mechanism used by each CBS, for the installation of anti-malicious code software for CBS, should explain how to keep the software updated

⑧ Describe remote access control and communication. Each CBS shall be identified to determine whether it can be accessed remotely or communicate with untrusted networks through secure zone boundaries and, if so, shall indicate compliance with the relevant requirements of Chapter 4, Paragraphs 4.3.15 and 4.3.16 of the guidelines;

⑨ Mobile media usage and management policies;

⑩ The event response and recovery plan shall contain the content required in paragraphs 4.3.21 and 4.3.22, in which the product network incident response and recovery plan required in Section 3.1.3 of Chapter 3 of the Guidelines shall be an important input;

⑪ backup plan;

⑫ compensation measure description (if available);

(5) The ship network security test outline shall include methods for updating and recording results during the test, and specify the necessary test environment, test equipment, initial conditions, test methods, detailed test steps, expected results and acceptance criteria. At a minimum, the ship cybersecurity test outline should verify the following

① The CBSS to which the Guide applies are included in the asset list, and the software version is the latest version. For example, verify the software version by using the vulnerability scanning tool or checking the software version at startup;

② The layout of the network security zone and related systems and devices is consistent with the description of the asset list, network security topology, network security design manual and other related documents, and can be verified by on-site inspection, network scanning, and/or other methods;

③ Security zone boundaries allow only traffic described in approved network security design specifications, which can be verified by evaluating firewall rules or port scans;

④ The components of CBS are located in controlled areas to which only authorized personnel have access;

⑤ Protect the effectiveness of devices against denial-of-service (DoS) attacks, where applicable, and ensure protection against excessive data flows originating within each network segment. Denial of service (DoS) tests should cover network storms (that is, attempts to consume available capacity on a network segment) and application-layer attacks (that is, attempts to consume processing power at selected endpoints in the network).;

⑥ "Minimal functionality" testing, which uses analytical assessments and port scans to test whether non-essential CBS features, ports, protocols, and services have been removed or disabled according to the vendor's security hardening guidelines, refer to the product security hardening

guidelines required in Chapter 2 2.4.1.2 (7) of the Guidelines;

⑦ The effectiveness of malware protection or other compensatory measures can be tested using reliable anti-malware test files;

⑧ User accounts are configured according to the principle of separation of responsibilities and least privilege, and temporary accounts have been deleted;

⑨ Wireless networks use secure wireless communication protocols (such as verification by using network protocol analysis tools) according to the approval documents provided by each supplier. Only authorized devices can access the wireless network;

⑩ Network monitoring and protection mechanisms:

a) Testing network connection triggers an alarm and the incident is noted down;
b) The test generates alarms and logs when it detects abnormally high network traffic
c) Demonstrate that CBS will weather the network storm in a secure manner, considering both unicast and broadcast messages (see also test item ⑤)
d) Verify the generation of auditable records (to record security-related incidents)
e) If there is an intrusion detection system, verify that the system is deployed passively and does not activate protection features that could affect the intended operation of CBS ;

⑪ Verify the effectiveness of procedures for CBS and network security functions;

⑫ Local controls required for the safety of the vessel can be operated independently of any remote or automatic control system and should be tested by disconnecting the local control system from the network of other systems/devices;

⑬ The effectiveness of network isolation should be demonstrated by disconnecting all networks that cross the boundaries of the security zone, demonstrating that the CBS in the security zone can maintain adequate operational functionality without network communication with other security zones or networks;

⑭ Return to the state of minimum risk to verify that CBS can restore the system to a reasonable security state in accordance with the measures provided in Article 4.3.21.9, Section 3, Chapter 4 of the Guide when it encounters a network incident. For example, allowing the operator to perform control and monitoring functions by other means allows the system to maintain its essential services. The test can be carried out together with the test items;

⑮ When connecting to an untrusted network, the relevant requirements applicable to Section 3 of Chapter 2 of the Guidelines for connecting to an untrusted network should be met and can be analyzed using a protocol analysis tool;

⑯ When remote users conduct remote access, the following should be verified:

a) Multi-factor identity authentication;
b) Limit the number of login failures. When a remote user establishes a session, there should be a prompt message;
c) Remote connection after confirmation by the person in charge of the ship;
d) The remote connection may be terminated manually by the personnel on board, or automatically after a period of inactivity;
e) The remote session should form an audit log, the log content is referred to Chapter 2, Section 3, Article 2.3.1.2 (8) of the Guide;
f) Relevant suppliers shall provide operating manuals and procedures.

⑰ Mobile media use control to ensure:

a) Only authorized users may use mobile or portable devices;
b) Ports can only be used by specific devices;
c) Files cannot be transferred directly from mobile media to CBS;
d) Files in mobile media cannot be automatically executed;
e) Mobile media access to the network should be limited to a specific MAC or IP address;
f) Ports that are not in use are closed or physically blocked.

⑱ Compensation measure test (if any).

(6) Recovery and backup planning procedures and the CBS recovery and backup operation manual provided by the supplier;

(7) The ship network security management plan shall contain at least the following:;

① Change management procedures, change management procedures shall be developed according to the requirements of change management in Chapter 2, Chapter 7, Section 6 2.6.10 of the Rules for the Classification of Steel Sea-going Ships, mainly including hardware and software modifications, security patches, etc;

② Management of security zone boundary devices (such as firewalls), including the minimum function principle, clearly allowed traffic, and denial of service (DoS) prevention;

③ Malicious code protection management, including the maintenance and update of protection software, physical protection and operating procedures, the application of mobile media and access control;

④ Physical and logical access control, including physical access control of systems and devices, physical access control of visitors, physical access control of network access points, access control credential management, and minimum permission policies;

⑤ Management of confidential information, including confidential information, information available to authorized personnel, and information transmitted in wireless networks;

⑥ Management requirements for remote access and communication over untrusted networks, including, at a minimum, user manuals, roles and permissions, patches and updates, confirmation before remote updates, interruptions, stops, and rollbacks;

⑦ Mobile media management requirements, including mobile media management policies and procedures, physical blocking of ports, authorized personnel use, only support for authorized device connections, considering the risk of malware infection;

⑧ The management activities of CBS and network anomalies, including the discovery and identification of abnormal activities, the examination of security auditable records, and the description or procedure for detecting events, can be managed together with the incident response;

⑨ Test and regular maintenance management of security functions in CBS and network;

⑩ Incident response plan shall at least:

a) Describe who, when and how to respond to cyber incidents;
b) Describe procedures or instructions for local/manual control;
c) Describe procedures or instructions for isolating security zones;
d) Describe the expected behavior of CBS in the event of a network incidents.

⑪ Incident recovery and backup plan shall including at a minimum:

a) Describe who, when, and how to recover from a cyber incident;
b) A specified backup plan, including backup frequency, backup maintenance and testing, taking into account acceptable downtime, alternative controls, vendor support and the importance of CBS;
c) Procedure manual for performing backup, shutdown, reset, restore and restart of CBS.

5.1.2.3 For a ship applying for class notations of cyber security, the plans to be submitted at each stage and the applicable class notations are shown in Table 5.1.2.3.

Summary of Plans and Documents Table 5.1.2.3

S/N	Drawing Name	CCS			Applicable Class Notations
		Ship Plan Approval	Survey during Construction	Survey after Construction	
1	Documents of Systems Related to Cyber Risk Management			Ⓐ	M
2	Files of Approved Product	Ⓡ			P,S
3	Ship Asset Inventory	Ⓐ			M, P, S

S/N	Drawing Name	CCS			Applicable Class Notations
		Ship Plan Approval	Survey during Construction	Survey after Construction	
4	Network Topology Diagram	Ⓐ			M, P, S
5	Ship Cyber Security Design Scheme	Ⓐ			P, S
6	Ship Cyber Security Test Program		Ⓐ		P, S
7	Ship Cyber Security Management Plan			Ⓐ[1)]	P, S
8	List of Systems Exempted from Cyber Security Requirements and Risk Assessment Reports	Ⓐ			P, S

Legends:
Ⓐ Submit to CCS for approval.
Ⓡ Submit to CCS for reference
1) Prior to the first annual survey, approved by the field ship surveyor

Section 2 Initial Classification Survey

5.2.1 General Requirements

5.2.1.1 The special requirements for ship cyber security survey are closely related to the class notations assigned to the ship. Where a ship has more than one class notation, the special requirements of each class notation apply.

5.2.1.2 All tests of the ship's cyber security test program shall be witnessed by CCS and some test items (e.g. 5.1.2.2(5)⑤-⑮, the test items in the CBS Recovery and Backup Operations Manual provided by the supplier) may be waived if their security features have been tested during the CBS certification period, as confirmed by CCS. During CBS certification, if part of the requirements are met through compensatory measures or modified after CBS certification, the relevant tests cannot be waived.

5.2.2 Survey and Test Items

5.2.2.1 The following survey items are to be completed for the ship applying for class notations of Cyber Security (M):
(1) Confirm that the cyber risk management items have been included in the ship safety management system documents;
(2) Confirm that the ship network management is in good working condition;
(3) Check the cyber risk management documents to confirm that they meet the requirements in Section 2 of Chapter 4.

5.2.2.2 Ships applying for the Cyber Security(P[SL0]) and Cyber Security(S[SLx]) class notifications shall complete field survey in accordance with the Ship's Cyber Security Test Program, Recovery and Backup plan procedures, and the CBS Recovery and Backup Operations Manual provided by the supplier.

5.2.3 Assigning Class Notations

5.2.3.1 After the survey/assessment, class notations to the ship of the appropriate class will be assigned by CCS.

Section 3 Survey after Construction

5.3.1 General Requirements

5.3.1.1 At an appropriate time prior to the ship's first annual survey, shipowners shall submit to CCS the ship's cyber security management plan, documenting the cyber security management within the scope of application of this Guidelines.

5.3.1.2 After the Ship's cyber security Management Plan has been approved by CCS, shipowners shall demonstrate compliance with the processes described in the approved Ship's cyber security Management Plan by providing records or other documentation at the first annual survey.

5.3.1.3 If ship cyber security management plan ungergo changes afterwards, verification shall be renewed.

5.3.2 Annual Survey

5.3.1.1 The following survey items are to be completed in the annual survey :

(1) The operation of the network risk management policy or system meets the requirements of the M suffix mark (when applicable);

(2) The approved change management process has been followed;

(3) Having considered the known vulnerabilities and functional dependencies of the software in CBS, in cooperation with the supplier to install security patches and update other software in accordance with the change management procedures and keep change records;

(4) The ship asset inventory has been updated;

(5) The network topology is updated, and the security area boundaries are managed in accordance with the ship's network security management plan;

(6) All anti-malware software is maintained and updated;

(7) Use mobile media according to management requirements;

(8) Access control in accordance with management requirements shall include:

① Personnel are authorized to visit CBS according to their duties;

② Only authorized devices can connect to CBS;

③ Visitors may access CBS in accordance with relevant policies and procedures.

(9) Credentials, keys, confidential information, certificates, related CBS documents and other sensitive information are managed and kept confidential in accordance with relevant policies and procedures;

(10) Remote access has been recorded and logged in accordance with relevant requirements and user manuals;

(11) Regular monitoring of anomalies in CBS by checking security logs and investigating alarms in CBS;

(12) Regular testing or verification of the safety features in CBS;

(13) The ship has the ability to respond to certain incidents and recover afterwards:

① The responsible personnel on board are able to implement the incident response plan;

② The personnel in charge on board is capable of performing local/manual control, safe area disconnection/isolation procedures or instructions;

③ Has responded to any cyber incident according to the incident response plan;

④ Instructions and/or procedures for incident recovery are available to those responsible on board;

⑤ The equipment, tools, documents and/or necessary software and data required for recovery have been provided to the responsible personnel on board;

⑥ CBS is backed up according to policies and procedures;

⑦ Manuals and procedures for shutdown, reset, recovery and restart are available for use by those in charge on board.

5.3.3 Intermediate Survey

5.3.3.1 Requirements for intermediate survey are the same as annual survey.

5.3.4 Special Survey

5.3.4.1 Shipowners shall conduct safety function tests based on annual inspection items in accordance with the ship cyber security test program, and some safety functions may be tested according to change records.

Appendix 1 Ship CBS Risk Assessment

Section 1 General Provisions

1.1 General Requirements

1.1.1 The shipowner/ship management company is to evaluate the impact on the ship if a security event occurs based on the threat to the ship's network assets and the likelihood that the threat will exploit the vulnerability to cause security incidents, combined with the value of the assets involved in the security incidents.

1.1.2 The Guidelines provide a complete risk assessment process for reference only. Other risk assessment methods recognized by CCS may also be adopted.

Section 2 Risk Management

2.1 Risk Management Process

2.1.1 See Fig. Appendix 1-2.1.1 Risk Management Process for the security risk management process of the ship system.

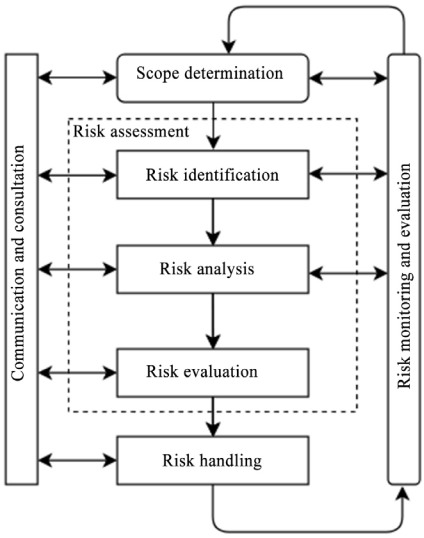

Fig. Appendix 1-2.1.1 Risk Management Process

2.2 Risk Elements Relationship

2.2.1 The basic elements of risk assessment include assets, threats, vulnerabilities and security measures, based on which risk assessment is carried out.

2.2.2 For a risk assessment, the relationship between the basic elements is as follows:
(1) The core of risk elements is assets, and assets are vulnerable;
(2) When security measures are implemented, the difficulty of exploiting the vulnerabilities of assets is increased, thus preventing external threats and protecting assets;
(3) Threats cause risks by exploiting the vulnerabilities of assets;
(4) After the risk is converted into a security incident, it will have an impact on the operational state of the asset.

2.3 Risk Assessment Process

(1) Collect information about the ship's systems, equipment and connections to determine the scope of the risk assessment. It should be supplemented by drawings to better understand the system/equipment interconnection;
(2) Evaluate the different system parameters through the evaluation level or risk assessment methodology in this document. The combination of these parameters will ultimately form a risk level for each system within the scope of the assessment;
(3) Determine whether to address the risk by defining and implementing relevant safety measures, based on the previously assessed risk level, until the residual risk level is considered acceptable.

2.4 Risk Identification

2.4.1 Asset Identification

(1) Asset classification.
According to the requirements of IACS UR E22, computer systems are divided into three categories based on the impact of system function failures, as detailed in Table Appendix 1-2.3.1 (1).

Categories of Computer Systmes Table Appendix 1-2.3.1（1）

Category	Impacts	Typical Systme Function
I	The failure of these systems does not endanger the safety of personnel, the safety of the ship or the environment	Monitoring, information and management functions
II	The failure of these systems can ultimately cause harm to the safety of personnel, the safety of the ship, and the environment	Alarm, monitoring and control functions necessary to keep the ship in normal operation and living conditions
III	The failure of these systems will immediately cause harm or disaster to the safety of personnel, the safety of the ship and the environment	Maintain the ship's propulsion and steering control functions Ship safety functions

Assets can be classified into business assets, system assets, system components and unit assets according to the hierarchy. The assets can also be classified into IT device, IT system, OT system, etc. according to the presentation of the assets. This document provides classification suggestions for the CBS system of UR E26 according to Appendix 1-2.3.1 (1) of Table, as detailed in Appendix 1-2.3.1 (2) of Table. It should be noted that the actual division of the I-III categories is determined by the degree of network connectivity and system function failures of each CBS system.
.

Examples of CBS Classification Table Appendix 1-2.3.1(2)

No.	CBS classification	CBS	Recommended classification
1	Propulsion system	Propulsion control system	III
		Host control system (various forms)	III
		Gearbox/clutch control system	III
		Pitch control system	III
		Push-side control system	II/III（subject to job scenario）
		Propulsion auxiliary system	II
		Energy supply system (oil, gas, battery)	III
2	Steering system	Steering gear control system	III
		Steering gear hydraulic unit control testing system	II
3	Mooring and mooring systems	Anchor mooring control and monitoring system	II

		Mooring winch control and monitoring system	II
		Mooring positioning system (combined DP and anchor chain)	III
4	Power generation and distribution systems	Main generator control system	III
		Battery management system	III
		Power management system	III
5	Fire detection and suppression systems	Fire detection control and alarm system	II
		Fire door control system	II
		Water mist fire extinguishing system	II
		Fire pump control system	II
		Engine room fixed fire extinguishing system	II
6	Bilge and ballast water systems, loading computer systems	Ballast water control and monitoring system	II
		Bilge control and monitoring system	II
		Loading computer system	II
		Valve remote control system	II
		Oil-water separator	II
		Domestic sewage treatment equipment	II
		Incinerator, scrubber control system	II
7	Watertight integrity and water inlet detection system	Watertight door control and monitoring system	II
		Water inlet detection system	II
		Gangway control system	II
8	Illumination	Emergency lighting	III
		Low lighting	III
		Navigation light control	III
9	A system that provides security features	Emergency cutoff system	III
		Gas safety system	III
		Cargo safety system	II
		Pressure vessel safety system	III
		Gas detection system	II
		Ignition source control	III
		ESL（ship-shore connection system）	III
10	Navigation device	ECDIS（Electronic chart system）	II
		ECS(Electronic chart system for domestic navigation ships)	II

		gyrocompass	II
		log	II
		Detector	II
		AIS（Automatic identification system）	II
		RADAR	II
		BNWAS	II
		Heading/track control system	II/III（subject to whether being applied to autonomous navigation）
		VDR（Voyage data recorder）	II
		Driving control information display system	I
11	Internal communication device	Broadcast system	II
		General alarm	II
		Automatic telephone	II
		Two-way voice communication	II
12	Radio equipment	GMDSS	II
		VHF	II
		MF/HF	II
		C station	II
		NAVTEX	II
		Other satellite communication system	I/III（subject to whether it is used for remote control communication）
13	Multifunctional integrated system	Full thruster control system	III
		INS（Integrated navigation system）	II
		IBS（integrated bridge system）	II
		ICS（integrated communication system）	II
		IAS（integrated automation system）	II /III（subject to whether maneuverability is in place）
14	Intelligent system	Implemented in accordance with Rules for Intelligent Ships	

(2) Asset assignment. The assets are assigned values based on the three security attributes of confidentiality, integrity and availability of the assets according to the ship network asset inventory.

① Assets can be classified into different levels according to their different confidentiality requirements. For example, 1 ~ 3 levels (corresponding to low, medium and high levels respectively) correspond to different degrees of confidentiality of assets or the impact on the whole ship system in case of lack of confidentiality;

② Assets can be classified into different levels according to their different integrity

requirements. For example, 1~3 levels (corresponding to low, medium and high levels respectively) correspond to the impact on the whole ship system when the integrity of assets is defective;

③ Assets can be classified into different levels according to their different availability requirements. For example, 1~3 levels (corresponding to low, medium and high respectively) correspond to different degrees of availability of assets respectively;

(3) Levels of asset importance. The most important attribute of an asset's confidentiality, integrity and availability can be selected as the final assignment of the asset depending on the characteristics of the ship system, and the different confidentiality, integrity and availability levels of an asset and their assignments can be weighted to calculate the asset's final assignment result. The final asset assignment can be classified into different levels. For example, 1 to 3 levels (corresponding to: low, medium and high levels respectively). According to the result of asset assignment, the scope of important assets is determined, and further risk assessment centers on the important assets.

2.4.2 Threats Identification

(1) Threats classification. The factors that cause threats can be classified into human factors and environmental factors. They can be classified into malicious and non-malicious ones according to motivation. Environmental factors include force majeure factors in the nature and other physical factors. Threats can take the form of direct or indirect attacks on information systems, causing damage to confidentiality, integrity and availability. They can also be incidental or deliberate incidents. The origins of threats are to be fully considered for the classification of threats, and threats classification is to be done according to the representation thereof. Table Appendix 1-2.3.2 of lists the content of threat identification based on presentation.

Threats Identification Contents Table Appendix1-2.3.2

No.	Threat category	Threat Description
1	Mal-operation	Errors or omissions committed by the operator during work, including operation errors and maintenance omissions, etc.
2	Abuse of authority	Overstep authorization to access to unauthorized resources, or abuse authority to take actions leading to system damage, including unauthorized access to network resources, unauthorized access to system resources, abuse of authority to improperly modify system configuration or data, abuse of authority to disclose secrets
3	Act repudiation	The operator does not acknowledge his own operating behavior, including the original denial, receiving denial, third party denial
4	Malicious code	Infected with program code that performs malicious tasks in the system, including viruses, trojans, worms, backdoors, spyware, eavesdropping software, rogue software, phishing, botnets, logic bombs, malicious scripts, etc.
5	Network attack	Use tools and technology to attack and invade the system through the network, including network detection, information collection, sniffing, vulnerability detection, user identity forgery and deception, user or business data theft and destruction, system operation control and destruction, password attack, cryptanalysis, denial of service, etc.
6	Physical failure	system/network has been physically damaged by illegal users
7	System failure	Services are interrupted due to software and hardware faults or environmental reasons
8	Communication interruption	Transmission interruption caused by an unexpected communication failure
9	Social engineering	Illegal users obtain confidential information about the system/network through social means
10	Inadequate management	System/equipment management is not adequate, usage is not standard, etc.

(2) Threat assignment. Judging the frequency of threats is an important part of threat assignment. The judgment is made and a threat assignment is carried out in accordance with the relevant national norms and recent information security threats combined with industry experience and relevant statistical data. In the assessment, the following three aspects are to be considered in combination:

① Statistics of threats occurred in previous security incident reports and their frequency;

② Statistics of threats discovered in the actual environment through detection tools and their various logs and the frequencies of the threats;

③ Statistics on threats to the whole society or specific industries issued by international organizations in recent years and their frequencies, as well as threat warnings issued.

(3) The frequencies of threats are graded, and different levels represent different frequencies of threats. The higher the level value, the higher the frequency of the threat. For example, 1 to 3 levels (corresponding to: low, medium and high levels respectively).

2.4.3 Vulnerability Identification

(1) Contents identified in vulnerability. Vulnerability identification can be asset-focused. Vulnerabilities that can be exploited by threats are identified for each asset that needs to be protected and the severity of the vulnerabilities is assessed. Vulnerability identification can be based on international or national standards, or on the security requirements of industry norms.

① Vulnerability identification data is to be sourced from shipowners/ship management company, as well as professionals in relevant business areas and hardware. The methods adopted for vulnerability identification mainly include: questionnaire survey, tool detection, manual verification, document review, penetration test, etc.

② Vulnerability identification is mainly carried out from two aspects: technology and management. Technical vulnerabilities involve security issues at various levels such as the physical layer, network layer, system layer and application layer. Management vulnerability can be further divided into two aspects: technical management vulnerability and organizational management vulnerability. The former is related to specific technical activities, while the latter is related to the management environment. See Table Appendix 1-2.3.3.

Vulnerability Identification Content Table Appendix 1-2.3.3

Type	Identification Object	Identification Aspect
Technical vulnerability	Physical environment	Identification is carried out from the aspects of physical position selection, physical access control, installation requirements, power supply and distribution, moisture and static protection, electromagnetic protection, etc.
	Network device and structure	Identification is carried out from the aspects of network structure design, communication security, boundary protection, access control, network isolation/segmentation, network configuration, network redundancy, etc.
	Host system	Identification is carried out from the aspects of authentication, access control, security audit, intrusion prevention, malicious code prevention, patch installation, resource control, system configuration, registry reinforcement, system management, etc.
	Application system (including IT application system and OT system)	Identification is carried out from the aspects of authentication, access control, data security, backup, emergency response, security audit, password protection, etc.
Managing vulnerability	Technical management	Identification is carried out from the aspects of physical environment management, communication and operation management, access control, data integrity, communication, authentication mechanism, password protection, etc.
	Organizational management	Identification is carried out from the aspects of security policy, organizational security, asset classification and control, personnel security and compliance.

(2) Vulnerability assignment: The severity of identified vulnerabilities can be assigned in a hierarchical manner according to the exposure degree of vulnerabilities for assets and the difficulty of technical implementation. Different levels represent different severities of asset vulnerability. The higher the level value, the higher the vulnerability severity. For example, 1 to 3 levels (corresponding to: low, medium and high levels respectively).

2.4.4 Identification of security measures in place.

While identifying vulnerabilities, the effectiveness of the security measures taken is to be identified and validated. The validation of security measures will evaluate the effectiveness, i.e. whether they actually reduce the vulnerability of the system and protect against threats. Effective security measures will be retained, and those identified as inappropriate are to be verified for cancellation, correction or replacement. Security measures can be classified as preventive measures and protective measures.

Preventive measures can reduce the likelihood that threats will exploit vulnerabilities to cause security incidents, such as:

(1) Fully consider possible vulnerabilities, threats and potential impacts of network incidents of CBS through risk assessment;

(2) Fully analyze, determine and record the connections between CBS and other CBS;

(3) Identify the software installed on CBS and provide evidence of the purpose, name, version, etc. of each application software, operating system, and firmware (if applicable);

(4) Organize network security training for crew members.

Protective measures can reduce the impact on a ship or system following a security incident, such as:

(1) CBS is located in a controlled access area;

(2) The physical interface of CBS is not available to untrusted/insecure removable devices;

(3) Develop a CBS maintenance policy in which CBS does not establish permanent or temporary connections to untrusted networks or use untrusted/insecure removable devices;

(4) Develop an incident response plan and recovery plan, including instructions on how to handle CBS in the event of a cyber incident on the ship

2.5 Risk analysis

2.5.1 After asset identification, threat identification, vulnerability identification and validation of existing security measures are completed, the shipowner/ship management company is to adopt appropriate methods and tools to determine the possibility of security incidents caused by threats exploiting vulnerabilities. The impact of losses caused by security incidents on the ship information system, i.e. the security risks of the ship cyber system, is judged based on the asset value related to the security incidents and vulnerability severity.

2.5.2 Ship cyber security risk analysis can be qualitative, quantitative or both:
(1) Identify assets and allocate value to assets;
(2) Identify threats, describe the attributes of threats, and assign values to threat frequencies;
(3) Identify vulnerabilities based on specific assets and assign values to severity of vulnerabilities;
(4) Calculate the possibility of security incidents according to the severity of threats and vulnerabilities;
(5) Calculate the impact of a security incident on the system, i.e., the risk value, based on the possibility and consequent loss of the security incident.
(6) The formula of the risk calculation principle is as follows:

$$\text{Risk value} = R(A, T, V) = R(L(T, V), F(Ia, Va))$$

where:R represents the function of safety risk calculation;A represents the asset;Trepresents threat;V represents vulnerability;Ia represents the value of the asset that the security incident acts on;Va represents the severity of the vulnerability;L represents the possibility of the security incident caused by threats exploiting vulnerabilities;F represents the consequences of the security incident.

2.6 Risk Evaluation

2.6.1 In order to realize the control and management of risks, the results of risk assessment are to be graded. Different levels represent different severities of system asset risks. The higher the level value, the higher the vulnerability severity. For example, 1 to 3 levels (corresponding to: low, medium and high levels respectively).

2.6.2 The risk value of the system assets is to be calculated according to the calculation method adopted, the range of risk value is to be set for each level according to the distribution of risk value, and all risk calculation results are to be graded. Each level represents the severity of the corresponding risk. See Table Appendix 1-2.5.2.

Risk Levels Table Appendix 1-2.5.2

Level	Identification	Description
3	High	High risk. The system and data are unavailable, which seriously affects the safe operation and has a significant impact on the ship operation.
2	Medium	Moderate risk. The ship's network, systems, data and other resources are accessed without authorization, affecting the ship's daily operations, but the impact is not extensive or significant.
1	Low	Low risk. The impact on the availability of the system and data is small and can be compensated by simple measures, or alternative measures are available.

2.7 Risk Handling Measures

2.7.1 Risk handling plan. For unacceptable risks, the risk handling plan is to be formulated for the ship cyber system according to the vulnerability that causes the risks. In the risk handling plan, security measures to make up for vulnerabilities, expected effects, implementation conditions, quarterly arrangements, responsible departments, etc. are to be specified. The selection of security measures will be considered from both management and technology aspects. Where safety measures from any one perspective are insufficient to achieve an acceptable level of residual risk, the shipowner/company/supplier shall adopt a combination of management and technical measures.

2.7.2 Residual risk assessment. After selecting appropriate security measures for an unacceptable risk, in order to ensure the effectiveness of security measures, re-assessment can be carried out to judge whether the residual risk has been reduced to an acceptable level after the implementation of security measures. If the result of the residual risk after taking appropriate security measures is still in the range of unacceptable risks, it is to be considered whether to accept this risk or take further security measures. It shall be included into the emergency plan after approval and drills shall be carried out regularly.

Appendix 2 Ship cyber security management

Section 1 General Provisions

1.1 General Requirements

1.1.1 An effective ship cyber security risk management system is to be established and implemented to improve the resilience to cyber security threats, so as to ensure that cyber security risks are at an acceptable level, and meet the expectations of interested parties (operators, users, regulators, etc.) for cyber security.

1.1.2 An effective safety risk management system is a risk-based management system for sustainable improvement, covering planning and design, implementation and operation, inspection and review, maintenance and improvement, as shown in Fig. Appendix 2-1.1.2.

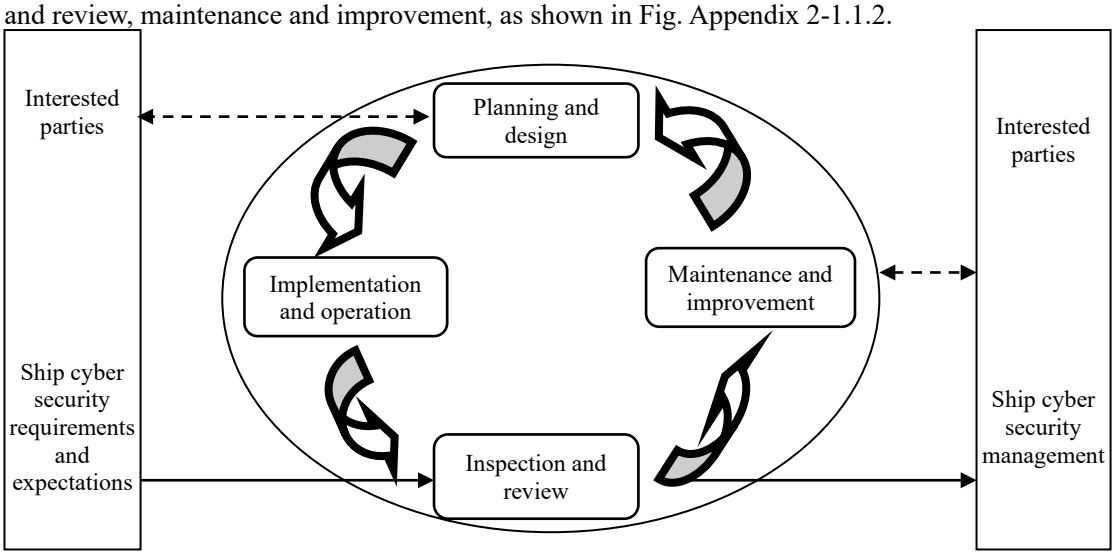

Fig. Appendix 2-1.1.2 Cyber Security Risk Management System

Section 2 Management System

2.1 Systems and Documents

2.1.1 The content of security O&M management is to be included, including but not limited to the applicable management activities listed in Section 4 and Section 5 of this Appendix. If applicable, the content of security construction management is also to be included, including but not limited to the applicable management activities listed in Section 6 of this Appendix.

2.1.2 The management system is to be embodied in a documented form, generally including four levels of the management manual, management regulations/procedures, operating procedures/instructions and record forms/reports.

2.1.3 The management manual is a programmatic document, which explains the objectives, policies, scope, principles, organizational structure, operation framework of management activities and security strategies of security management.

2.1.4 The management regulations/procedures are procedural and prescriptive documents, which describe individual management processes, involved management activities and management standards, and clarify the input, output and interaction of the management processes.

2.1.5 The operating procedures/instructions are guidelines and operational documents used to specifically guide the implementation of management work, including various operating instructions, user manuals and technical procedures.

2.1.6 Record forms/reports are recording documents used to further standardize the input and output of management work.

2.2 Formulation and Issuance

2.2.1 Special departments or personnel are to be designated or authorized to be responsible for the formulation of the management system.

2.2.2 The management system is to be issued and implemented in a formal and effective way after approval, and the document versions are to be controlled.

2.3 Audit and Improvement

2.3.1 Internal audits are to be conducted regularly or when significant changes occur to determine whether the implementation of the security management system meets expectations, as well as the requirements of relevant organizations and relevant laws and regulations.

2.3.2 Management review is to be carried out regularly or in case of significant changes to demonstrate the suitability, conformity, continuity, stability, adequacy and effectiveness of the security management system, and evaluate and determine the opportunities for improvement and the need for changes.

2.3.3 For non-conformities found in inspection, audit, review, security incident investigation and other activities, corrective and preventive control measures are to be taken, and when necessary, the security management system with deficiencies or in need of improvement is to be revised.

Section 3 Management Organization

3.1 Organization and Posts

3.1.1 The network builder and/or user is to set up a three-level management organization and related posts composed of decision-making level, management level and execution level, define post responsibilities, and allocate post personnel or assign post responsibilities to specific personnel. Conflicting areas of duties and responsibilities are to be separated to reduce the opportunity for unauthorized or unintentional modification or misuse.

3.1.2 The decision-making level is generally a committee or leading group that guides and manages cyber security work, and its top leader is assumed or authorized by the unit director/leader in charge, and is responsible for making decisions on ship cyber security policies, strategies, major issues, etc.

3.1.3 The management level is generally the functional department or working group of cyber security management, which is responsible for the specific organization and coordination of the daily management of ship cyber security.

3.1.4 The execution level of the builder is generally composed of security administrators, system administrators and other posts, and they are responsible for implementing specific management work. The security administrator is the person in charge of cyber security. The system administrator is responsible for the deployment, installation, configuration, technical support and daily O&M management of the cyber system and related facilities.

3.1.5 The execution level of the user is generally composed of on-board security administrator, on-board system administrator, on-shore system administrator and other posts. The on-board security administrator is the person in charge of ship cyber security, who is usually the captain or a person assigned by the captain. The on-shore system administrator is responsible for the deployment, installation, configuration and technical support of the ship cyber system and related facilities. The on-board system administrator is responsible for the daily O&M management of the ship cyber system and related facilities.

3.2 Authorization and Approval

3.2.1 Authorized approval matters, approval departments and approvers, etc. are to be clearly defined according to the responsibilities of each functional department and post.

3.2.2 Approval procedures are to be established for system changes, important operations, physical access and system access, etc., and the approval process is to be executed in accordance with the approval procedures.

3.2.3 Approval matters are to be regularly reviewed (interval not longer than 1 year), and the matters to be authorized and approved, approval departments and approvers, etc. are to be updated in a timely manner.

3.3 Communication and Cooperation

3.3.1 Cooperation and communication among various managers, internal agencies and external organizations (regulation, inspection, etc.) are to be enhanced, and coordination meetings are to be organized when available to collaborate in dealing with cyber security issues.

3.3.2 Cooperation and communication with external organizations related to cyber security, various suppliers, industry experts and security organizations are to be strengthened.

3.3.3 A contact list of cyber security-related external units is to be established, including the name, cooperation content, contact person and contact information of the external units.

3.3.4 Circulars and notices about cyber security incidents from competent authorities, CCS and industry associations are to be closely followed to understand the motives and attack methods of cyber security incidents so that threats can be identified and acted upon.

Section 4 Basic Management Requirements

4.1 Personnel Management

4.1.1 Employment and Termination

(1) A dedicated department or person is to be designated or authorized to be responsible for the recruitment of personnel;

(2) The identity, security background, professional qualifications or credentials of the personnel employed are to be examined, and the technical skills they possess are to be assessed;

(3) A confidentiality agreement is to be signed with the employed personnel, and a post responsibility agreement is to be signed with the personnel in key posts (on-shore system administrator, on-board security administrator, etc.);

(4) All access privileges of personnel terminated from post are to be terminated in a timely manner and all kinds of IDs, keys, badges, etc., as well as software and hardware equipment, user accounts and other related assets provided by the unit are to be recovered;

(5) Strict transfer procedures are to be handled, and key post personnel are yet to promise their confidentiality obligations after transfer before leaving.

4.1.2 Training and Assessment

(1) Security awareness education and post skills training are to be provided to all types of personnel (including operators), and relevant security responsibilities and disciplinary measures are to be informed;

(2) A targeted training plan is to be developed to provide training on security fundamentals, post operating procedures, etc;

(3) Ship cyber security management and/or operational skills assessment is to be carried out regularly for personnel in different posts.

4.1.3 Third Party Personnel

(1) Before third party personnel physically visit the controlled area, a written application is to be made, approved and accompanied by a person throughout the process and registered for the record;

(2) Before third party personnel access the controlled network to access the system, a written application is to be submitted and approved, then the account is to be opened and privileges are to assigned by a dedicated person, and registration is to be done for the record;

(3) When remote access by third party personnel, the remote access point cannot be a public place and is to be mutually confirmed before, during and when access is completed;

(4) Before third party personnel use the cyber system (including devices and application systems), they are to receive the necessary security training/education;

(5) After third party personnel leave the site, all their access privileges are to be cleared or disabled in a timely manner;
(6) Third party personnel who are granted access to the system are to sign a confidentiality agreement and receive appropriate security training/education. They are not to perform unauthorized operations and are not to copy or disclose any sensitive and important information.

4.2 Risk Management

4.2.1 Necessary measures are to be taken to identify security vulnerabilities and hazards in construction and O&M. The identified security vulnerabilities and hazards are to be patched in a timely manner or patched after assessing the possible impact.

4.2.2 Cyber security risk assessment is to be conducted on a regular basis or in the following cases, and a risk assessment report is to be formulated:
(1) When a major cyber and information security incident occurs on the ship;
(2) When major changes occur or are proposed;
(3) When it is determined necessary within the organization or required by an external organization.

4.2.3 The cyber security risk assessment is to consider, but not be limited to, the following:
(1) Threats, such as malware and phishing attacks;
(2) Identification and protection of vulnerable systems, such as ECDIS (Electronic Chart Display and Information System), ENPs (Electronic Nautical Publications);
(3) Mitigation measures, such as USB control;
(4) Identification of internal key personnel, such as administrators, persons reporting suspicious incidents;
(5) Hard copies of key contacts such as DPA (designee), CSO (security officer);
(6) Password management;
(7) Commitment of the Supplier/Contractor.

4.2.4 The cyber security risk assessment during O&M is to include technical tests.

4.2.5 Risk handling and re-assessment (residual risk assessment) are to be carried out for the security risks found in the risk assessment.

4.3 Security Inspection

4.3.1 Routine security inspections, including daily system operation, system vulnerabilities and data backups, are to be conducted on a regular basis, and security vulnerabilities and hazards found are to be patched in a timely manner or patched after assessing the possible impact.

4.3.2 Comprehensive security inspection is to be conducted on a regular basis, including the effectiveness of existing security technology measures, the consistency of security configuration and security policy, and the effectiveness of the security management system.

4.3.3 A security inspection form is to be developed to implement security inspections, security inspection data is to be summarized to form the security inspection report, and security inspection results are to be communicated.

4.4 Change Management

4.4.1 Change demands are to be clarified before the change is made, and a change plan is to be formulated. The change plan is to be implemented only after approval.

4.4.2 Change reporting and approval control procedures are to be established to control all changes according to the procedures and record the change implementation process.

4.4.3 For major changes, a risk assessment of change failure is to be conducted and procedures for aborting changes and recovering from failed changes are to be established. Process control methods and personnel responsibilities are to be clarified, and the recovery process is to be rehearsed when necessary.

4.5 Incident and Emergency Management

4.5.1 Security vulnerabilities and suspicious incidents identified are to be reported to the administrator and other relevant personnel in a timely manner.

4.5.2 The security incident report and handling management regulations are to be formulated to clarify the reporting, handling and response processes for different security incidents, including responsibilities for on-site handling, incident reporting and post-recovery, etc.

4.5.3 The causes of the incident are to be analyzed and identified in the process of security incident reporting and response handling, evidence is to be collected, the handling process is to be recorded, and lessons learned are to be summarized.

4.5.4 Different handling procedures and reporting procedures are to be used for major security incidents that cause system outages and information leaks.

4.5.5 For major security incidents, after the on-site emergency response is over, an incident investigation is also to be conducted and an incident investigation report is to be formulated, a risk assessment is to be initiated if necessary, and the management system documents with deficiencies are to be revised.

4.5.6 An emergency plan is to be developed to indicate how a cyber security incident will be detected and measures taken to limit the consequences in a timely manner, as well as to ensure security and recover affected systems through appropriate response actions. As a minimum, this includes symptoms to look for, control measures to be taken immediately, system recovery measures, and personnel communication methods. All emergency measures are to be easily understood by the crew, and if on-shore support is required, instructions are to be given on how to obtain external assistance.

4.5.7 Relevant personnel are to be regularly trained on the emergency plan, and emergency plan drills are to be carried out.

4.5.8 The original emergency plan is to be re-evaluated, revised and improved regularly or after the emergency response.

4.5.9 The emergency plan is to be kept where it is easily accessible to responsible personnel and its validity is to not be nullified by the occurrence of a cyber security incident, either in hard copy (paper copy) or electronic devices independent of the ship's network.

4.6 Backup and Recovery Management

4.6.1 According to the importance of data and the impact of data on system operation, data backup and recovery strategies, backup procedures and recovery procedures are to be formulated.

4.6.2 Important business information, system data and software systems that need regular backup are to be identified, and a backup plan is to be formulated. The backup plan is to specify the backup scope, backup method, backup frequency, storage medium, storage period, etc. of the backup information.

4.6.3 The backup data and recovery procedures are to be tested regularly to ensure that the backup data is working properly. The validity of the backup media is to be checked and tested to ensure that the backup is recovered within the time specified in the recovery procedure.

4.7 Service Provider Management

4.7.1 The selection of service providers is to comply with the regulations of relevant organizations, including product suppliers, communication service providers and outsourcing O&M service providers, etc.

4.7.2 Agreements are to be entered into with the selected service provider to define the cyber security-related obligations to be fulfilled by all parties throughout the service supply chain.

4.7.3 The services provided by service providers is to be regularly monitored, reviewed and audited, and their service changes are to be controlled.

4.7.4 Security mechanisms, service levels and management requirements for all network services are to be identified and included in the network service protocol.

4.7.5 Outsourcing O&M service providers are also to meet the following requirements:

(1) When outsourcing O&M service providers are selected, it is to be ensured that they have the ability to carry out security O&M work as required in terms of technology and management, and the ability requirements are to be specified in the signed agreement;
(2) An agreement is to be signed to clearly specify the scope, work content and security requirements of outsourced O&M, such as the requirements for access, processing and storage of sensitive/important information, and the emergency support requirements for interruption of IT/OT facilities, networks and application systems.

4.8 Password Management

4.8.1 Password-related requirements are to be followed.

4.8.2 Cryptology and products certified and approved by the cryptographic management regulatory authority are to be used.

4.9 Confidentiality Management

4.9.1 The confidentiality-related requirements of relevant organizations for state secrets, trade secrets, privacy, etc. are to be met.

4.9.2 The release of information included in the scope of confidentiality, undesirable information and other information is to be controlled.

4.9.3 Information transmission is to be controlled to protect the security of all types of information transmitted through communication facilities, and there are to be corresponding confidentiality agreements or non-proliferation agreements to prevent the transmitted information from being disclosed.

Section 5 Initial Classification Survey

5.1 Environment Management

5.1.1 Management regulations are to be formulated for physical access, entry and exit of articles, etc. Boarding visits are to be approved, accompanied by designated personnel, and registered.

5.1.2 Security zones are to be defined to protect areas containing sensitive or critical information and information processing facilities. Security zones are to be suitably protected by access controls to ensure that only authorized personnel have access.

5.1.3 Visitors are not to be received in the security zone, and paper documents and mobile media containing sensitive/important information are to not be placed at will.

5.1.4 Special personnel are to be designated to regularly maintain and manage the power supply and distribution, air conditioning, temperature and humidity control, firefighting and other facilities in the machine room and other places.

5.1.5 Devices are to be properly located and protected to reduce threats and hazards from the environment and reduce unauthorized access.

5.1.6 The device are to be protected from power or communication interruptions and other interruptions due to failure of support facilities.

5.1.7 It is to be ensured that the unattended device is properly protected, for example, by locking the screen or placing it under video surveillance to prevent unauthorized use.

5.1.8 The strategy of clearing desktop paper and removable storage media and the strategy of clearing information processing facility screens (such as screen lock, screensaver, etc.) are to be adopted.

5.2 Asset Management

5.2.1 A asset inventory related to the protected objects (host devices, network/security devices, etc.) is to be prepared and kept, indicating the asset user, maintainer, location, importance, backup method and cycle (if any), etc.

5.2.2 The assets are to be identified, registered and managed according to their importance, and appropriate management measures are to be selected to control their basic condition such as addition, change, maintenance/repair, demobilization/return and scrapping.

5.2.3 The use of assets is to be monitored, adjusted, and future capacity requirements reflected to ensure system performance.

5.3 Media Management

5.3.1 The media are to be stored in a safe environment, and all kinds of media are to be controlled and protected, managed by special personnel, and checked regularly. The media used for updating and maintaining the ship system software are to be used by special personnel.

5.3.2 The selection of personnel, packaging and delivery in the physical transmission process of the medium are to be controlled to prevent unauthorized access, abuse or damage during transportation, and the archiving and query of the medium are to be registered and recorded.

5.3.3 Access to private mobile media (except crew entertainment networks) is to be prohibited, and critical devices such as ECDIS are only to be allowed to access special mobile media.

5.3.4 On scrapping, the media are to be handled reliably and safely in accordance with formal procedures.

5.4 Device Management

5.4.1 All kinds of devices (including backup and redundant devices), lines, etc. are to be regularly maintained and managed by designated personnel to ensure their continuous availability and integrity.

5.4.2 A management system is to be established for the maintenance of supporting facilities, software and hardware to effectively manage their maintenance, including clarifying the responsibilities of maintenance personnel, approval of maintenance and service, supervision and control of maintenance process, etc.

5.4.3 Information processing devices are to be approved before they are taken off the ship, and the time of their demobilization and return is to be recorded. For devices containing storage media, the important data is to be encrypted or cleared when they are taken off the ship. Devices off-site (such as leaving the ship on business trips, etc.) are to be well secured to prevent unauthorized use and information leakage (such as device theft, loss, etc.), and special consideration is to be given to the network and information security-related regulations of the competent authorities in the relevant countries / regions when entering and leaving the country.

5.4.4 Devices are not to be taken off the site without prior authorization. The shipowner is to designate the responsible person on site with the authority to permit the removal of the devices (including device components). The time of taking the removed devices off site is to be restricted and the return time is to be recorded.

5.4.5 Devices containing storage media are to be completely cleared or securely overwritten prior to scrapping or reuse to ensure that sensitive/important data and licensed software on the device cannot be recovered for reuse.

5.4.6 The external communication interfaces such as USB interface and network interface of each device are to be managed by physical locking and/or technical encryption and other means for effective access control to prevent unauthorized use.

5.4.7 The use of portable computers, PDAs and other mobile devices (including external devices carried by crew members and third party personnel) on board is to be effectively controlled to prevent unauthorized access and use. Access by private devices is to be prohibited, except for the crew entertainment network.

5.5 Network and Application System Security Management

5.5.1 Network and application system security management systems are to be established to specify account management, installation and upgrade, O&M operations and logs, access control, malicious code prevention, configuration management, etc.

5.5.2 Account Management

(1) Different roles are to be assigned for the management and use of network and application systems, and the responsibilities and privileges of each role are to be clarified;

(2) Account application, account establishment and account deletion are to be controlled, and the accounts and access privileges are to be regularly reviewed. Users are only allowed access to networks and network services that they are explicitly authorized for use, and the assignment and use of privileges are to be restricted and controlled.

5.5.3 Installation and Upgrade

(1) Devices and software are to be installed, configured, updated, upgraded and patched by trained and appropriately authorized personnel. The device and software installed are to be approved and a log is to be generated after successful operation. The installation, configuration and operation manuals are to be formulated, and the security configuration and optimized configuration are to be carried out according to the manuals;

(2) Vulnerabilities and patch releases are to be closely monitored, software installation, upgrades and patch management are to be strictly enforced, and professional technical institutions are to be entrusted with security assessment and testing verification before software upgrades and patch installation for critical OT systems;

(3) Before installation, configuration, renewal, upgrade and patching, a plan is to be formulated to restore when necessary.

5.5.4 O&M Operations and Logs

(1) The O&M logs are to be recorded in detail, including daily patrol inspection, O&M records, parameter setting and modification, etc.;

(2) Changeable O&M are to be strictly controlled, and only after approval can the connection, software/component installation or configuration parameters be changed. Unchangeable audit logs are to be kept during the operation, and the configuration file/information base is to be updated synchronously after the operation;

(3) The use of O&M tools are to be strictly controlled, especially those capable of overriding software systems and application privilege control. The tools are to be accessed for operation only after approval, unchangeable audit logs are to be retained during operation, and sensitive data in the tools are to be deleted after the operation;

(4) The activation of remote O&M is to be strictly controlled, and the remote O&M interface or channel can only be opened after approval. Unchangeable audit logs are to be retained during the operation, and sensitive data in the tool is to be deleted after the operation. The remote access point is not to be at a public place and is to be mutually confirmed before, during and after access. All activities during remote maintenance are to be monitored by trained in-house personnel;

(5) The operational state of the network and application system should be monitored, and the alarm is to be responded to in time;

(6) Logs, monitoring and alarm data are to be analyzed and counted regularly to detect suspicious behaviors in a timely manner.

5.5.5 Access Control

(1) All connections to the outside are to be authorized and approved, violations of wireless Internet access and other cyber security policies are to be checked regularly, and cyber security awareness education and training are to be enhanced when necessary;

(2) When access control is required, access to the network and application systems is to be controlled through secure login procedures.

5.5.6 Malicious Code Protection

(1) All users' awareness of preventing malicious codes is to be improved. Malicious codes are to be checked before access to external computers and storage devices, and before use (reading or execution, etc.) of external files (email attachments, files downloaded from network, etc.);

(2) Detection, prevention and recovery measures are to be implemented to deal with malicious codes/software, and the effectiveness of technical measures (such as anti-virus software and virus database) to prevent malicious code attacks is to be verified regularly.

5.5.7 Configuration Management

(1) Basic configuration information is to be recorded and saved, including network topology, software/components installed on each device, version and patch information of software/components, configuration parameters of each device or software/component, etc.;
(2) The change of basic configuration information is to be included in the scope of change, the change of configuration information is to be controlled, and the basic configuration information base is to be updated in time.

5.6 Cloud Computing Management

5.6.1 A confidentiality agreement is to be signed with the cloud service provider who is required not to disclose the cloud service customer data.

5.6.2 The security incident information or security threat information of the supply chain is to be communicated to the cloud service customers in a timely manner.

5.6.3 Important changes of suppliers are to be communicated to cloud service customers in a timely manner, and the security risks caused by the changes are to be evaluated and measures are to be taken to control the risks.

5.6.4 The selection of O&M locations for the cloud computing platform and the implementation of O&M operations are to take into account the regulations of regulatory authorities and relevant organizations.

5.7 Mobile Internet Management

5.7.1 A configuration library of legal wireless access devices and legal mobile terminals is to be established for the identification of illegal wireless access devices and illegal mobile terminals.

5.8 IoT Management

5.8.1 Personnel are to be designated to regularly patrol the deployment environment of sensing node devices and gateway node devices, and record and maintain environmental abnormalities that may affect the normal operation of sensing node devices and gateway node devices.

5.8.2 The processes of warehousing, storage, deployment, carrying, repair, loss and scrapping of sensing node devices and gateway node devices are to be clearly specified and managed throughout the process.

5.8.3 The confidentiality management of the deployment environment of sensing node devices and gateway node devices is to be enhanced. For example, when the personnel responsible for inspection and maintenance are transferred from their posts, the relevant inspection tools and inspection and maintenance records are to be returned immediately.

5.9 Big Data Management

5.9.1 A security management strategy for digital assets should be established to specify the operation specifications, protection measures, and responsibilities of management personnel throughout the data life cycle, including but not limited to data collection, storage, processing, application, flow, destruction, and other processes.

5.9.2 Data classification and hierarchical protection strategies should be formulated and implemented, and different security protection measures are to be formulated for different categories and levels of data.

5.9.3 On the basis of data classification and grading, the scope of important digital assets is to be divided, and the use scenarios and business processing procedures for automatic desensitization or de-identification of important data is to be defined.

5.9.4 The category and level of data are to be reviewed regularly. If the category or level of data needs to be changed, the change is to be implemented according to the change approval process.

Section 6 Survey after Construction

6.1 Demands Determination

6.1.1 Ship cyber security demands, objectives and ship network scope are to be stated in writing.

6.1.2 Relevant parties and relevant safety technical experts are to be organized to demonstrate the rationality and correctness of security demands and objectives.

6.1.3 The identified security demands and objectives are to be agreed by the shipowner.

6.2 Planning and Design

6.2.1 Overall safety planning and scheme design are to be carried out according to the security objectives, and supporting documents shall be formed.

6.2.2 The basic security measures are to be selected according to the security objectives, and the security measures are to be supplemented and adjusted according to the results of risk analysis.

6.2.3 Relevant parties and relevant security experts are to be organized to demonstrate and verify the rationality and correctness of the overall security plan and its supporting documents, and they can only be formally implemented with the consent of the shipowner.

6.3 Project Implementation

6.3.1 A special department or personnel is to be designated or authorized to be responsible for the management of the project implementation process.

6.3.2 A security project implementation scheme is to be formulated to control the project implementation process, properly ensure the security of the development environment, and monitor outsourced development activities.

6.3.3 The implementation process of the project is to be controlled through third party project supervision.

6.4 Procurement and Use of Products

6.4.1 The procurement and use of cyber security products are to comply with the relevant provisions.

6.4.2 The procurement and use of password products and services are to meet the requirements of password management.

6.4.3 Product selection test is to be carried out in advance to determine the scope of candidate products, and the list of candidate products is to be regularly reviewed and updated.

6.5 Software Development

6.5.1 The development environment is to be separated from the actual operating environment, and the test data and test results are to be controlled.

6.5.2 A software development management system is to be formulated to clearly explain the control method and personnel behavior code in the development process.

6.5.3 Security specifications for code writing are to be formulated, requiring developers to write codes according to the specifications.

6.5.4 Relevant documents and user guidelines for software design are to be available, and the use of documents is to be controlled.

6.5.5 The security is to be tested during the software development process. For outsourced development, possible malicious codes are to be detected before software delivery. For self-development, possible malicious codes are to be detected before software installation.

6.5.6 Software system updates and releases are to be authorized and approved, and versions of program repository modifications are to be controlled.

6.5.7 In case of self-development, the developers are to be full-time personnel and the development activities of them are to be monitored.

6.5.8 In case of outsourced development, the development unit is to provide the software source code and review the possible backdoors and hidden channels in the software.

6.6 Test and Acceptance

6.6.1 Before implementation on board, a test plan is to be formulated to specify the test contents (including at least password application security), the test is to be implemented according to the test plan, and a test report is to be developed.

6.6.2 After implementation on board, an acceptance test plan is to be formulated to specify the contents of the acceptance test. The acceptance test is to be carried out according to the acceptance test plan, and an acceptance report is to be developed.

6.6.3 Test data are to be carefully selected, protected and controlled.

6.7 System Delivery

6.7.1 A delivery list is to be prepared, and the devices, software and documents handed over are to be counted according to the delivery list. This list is to be kept on board.

6.7.2 Technicians responsible for O&M are to be provided with corresponding skill training.

6.7.3 Construction process documents and O&M documents are to be provided.

6.8 Cloud Service Provider Management

6.8.1 Cloud service providers with secure and compliant ship cyber systems are to be selected, and the cloud computing platform provided by them is to provide corresponding security protection capabilities for the business application systems they carry.

6.8.2 The service content and specific technical indicators of the cloud service are to be specified in the service agreement with the cloud service provider.

6.8.3 The privileges and responsibilities of the cloud service provider are to be specified in the service agreement with the cloud service provider, including management scope, division of responsibilities, access authorization, privacy protection, code of conduct, liability for breach of contract, etc.

6.8.4 The service agreement with the cloud service provider is to specify that the cloud service customer data are to be completely provided when the service contract expires, and promise that the relevant data will be cleared on the cloud computing platform.

6.8.5 A confidentiality agreement is to be signed with the cloud service provider who is required not to disclose the cloud service customer data.

6.8.6 The security incident information or security threat information of the supply chain is to be communicated to the cloud service customers in a timely manner.

6.8.7 Important changes of suppliers are to be communicated to cloud service customers in a timely manner, and the security risks caused by the changes are to be evaluated and measures are to be taken to control the risks.

6.9 Mobile Internet Management

6.9.1 In the procurement of mobile application software, the application software installed and running on the mobile terminal is to come from reliable distribution channels or be signed with reliable certificates.

6.9.2 In the procurement of mobile application software, the application software installed and running on the mobile terminal is to be developed by the designated developer.

6.9.3 In the development of mobile application software, the qualification of mobile service application software developers is to be examined.

6.9.4 In the development of mobile application software, the validity of the signature certificate for developing mobile service application software is to be ensured.

6.10 Big Data Management

6.10.1 A secure and compliant big data platform is to be selected, and the big data platform services provided by it is to provide corresponding security protection capabilities for the big data applications it carries.

6.10.2 The privileges and responsibilities of the big data platform provider, various service contents and specific technical indicators, especially the security service contents, are to be agreed in writing.

6.10.3 The responsibility of the recipient regarding data exchange and sharing to protect the data is to be clearly specified, and the recipient is to have sufficient or equivalent security protection capability.