Guidelines for Requirement and Security Assessment of Ship Cyber System

2020

Effective from: March 01, 2020

Contents

Introduction 1
Chapter 1 General 1
Section 1 General provisions 1
1.1.1. Application 1
1.1.2. General requirements 1
Section 2 Class Notation 1
1.2.1. Class notation and assessment report 1
1.2.2. Application 3
Section 3 Definitions and references 3
1.3.1. Definitions 3
1.3.2. References 5
Chapter 2 Management Requirements 1
Section 1 General provisions 1
2.1.1. General requirements 1
2.1.2. Construction management 1
2.1.3. Operation and maintenance management 2
Section 2 Management system 2
2.2.1. System and documentation 2
2.2.2. Formulation and release 3
2.2.3. Review and improvement 3
Section 3 Management organization 3
2.3.1. Organization and post 3
2.3.2. Authorization and approval 4
2.3.3. Communication and cooperation 4
Section 4 Basic management requirements 4
2.4.1. Personnel management 4
2.4.2. Risk management 5
2.4.3. Security inspection 5
2.4.4. Change management 6
2.4.5. Incident and emergency management 6
2.4.6. Backup and recovery management 6
2.4.7. Service provider management 7
2.4.8. Password management 7
2.4.9. Confidentiality management 7
Section 5 Supplementary requirements for construction management 7
2.5.1. Determination of needs 7
2.5.2. Planning and design 7
2.5.3. Project implementation 8
2.5.4. Product purchase and use 8
2.5.5. Software development 8
2.5.6. Testing and acceptance 8

2.5.7. System delivery....9
2.5.8. Management of cloud service providers....9
2.5.9. Mobile internet management....9
2.5.10. Operation system management....9
2.5.11. Big data management....10
Section 6 Supplementary requirements for operation and maintenance management....10
2.6.1. Environmental management....10
2.6.2. Asset management....10
2.6.3. Media management....11
2.6.4. Device management....11
2.6.5. Security management of cyber and application system....11
2.6.6. Cloud computing management....13
2.6.7. Mobile internet management....13
2.6.8. Internet of Things management....13
2.6.9. Big data management....13
Chapter 3 Technical Requirements....15
Section 1 General provisions....15
3.1.1. General requirements....15
3.1.2. Physical security....15
3.1.3. Network architecture....15
3.1.4. Network boundary....16
3.1.5. Computing environment....16
3.1.6. Security audit....16
Section 2 Physical security....16
3.2.1. Location....16
3.2.2. Physical access control....16
3.2.3. Installation....17
Section 3 Network architecture....18
3.3.1. Network redundancy....18
3.3.2. Network segregation and segmentation....18
3.3.3. Communication security....19
3.3.4. Wireless....20
3.3.5. Asset list....21
3.3.6. Network test....22
Section 4 Network boundary....22
3.4.1. Boundary defense....22
3.4.2. Malicious code prevention....23
3.4.3. Intrusion prevention....23
3.4.4. Monitor and alarm....24
3.4.5. Access control....25
3.4.6. Remote operation and maintenance....27
Section 5 Compute environment....28
3.5.1. Authentication....28
3.5.2. Data security....28
3.5.3. Software installation and update....29
3.5.4. Emergency response....29

3.5.5. Backup 30
Section 6 Security audit 30
3.6.1. Configuration 30
3.6.2. Security audit (log) 31
Chapter 4 Product Assessment 32
Section 1 General provisions 32
4.1.1. General requirements 32
4.1.2. Assessment process 32
4.1.3. Basic technical requirements 32
Section 2 Drawings & documents and test items 33
4.2.1. Drawings & documents 33
4.2.2. Test methods 36
Chapter 5 Surveys during construction 38
Section 1 General provisions 38
5.1.1. General requirements 38
5.1.2. Plans and documents 38
Section 2 Initial survey 40
5.2.1. General requirements 40
5.2.2. Survey process 40
5.2.3. Survey and test items 42
Section 3 Surveys after construction 42
5.3.1. Annual surveys 42
5.3.2. Occasional surveys 43
Appendix 1 Risk Analysis 44
Appendix 2 Pre-assessment Form of Ship Cyber Security 51
Appendix 3 Ship cyber system/ Device Assessment Form 54
Appendix 4 Detailed Assessment Form of Ship Cyber Security (Product) 57
Appendix 5 Detailed Assessment Form of Ship Cyber Security (Ship) 60
Appendix 6 Additional Suggestions for Firewall Settings of Ship Industrial Control System 69

Introduction

In recent years, with digital, intelligent and cyber-based advancement of ships, an increasing number of control systems, communication and navigation systems, information management systems and devices are applied in ship cyber to realize external information interaction. Increasing "online" configurations give rise to mounting potential cyber threats of ships. Under such a background, ship cyber security is of great importance.

Responding to urgent need of improving cyber risk and threat awareness, the IMO released the Circular on the *Maritime Cyber Risk Management Guideline* (MSC-FAL.1/Circ3) on 98th session of Maritime Security Committee, which proposes countermeasures to cyber risks. IACS issued 12 recommendations for ship cyber security in 2018. International maritime organization is constantly raising the importance of ship cyber risks management.

In order to meet industry requirements, ISC works out the Guideline to standardize the construction, operation and maintenance, assessment and inspection of ship cyber, have the managing and technical personnel get aware of importance of ship cyber security, build new awareness of comprehensively enhancing ship cyber system construction and threat defense competence, ensure stability of ship cyber environment, and lay basic conditions and guarantee for intelligentization, digitalization and networking of ships.

Targeting at risk points of operation, integration, maintenance, design, security awareness and management level in such links as design, implementation, operation and retirement of ship cyber system, the Guideline guides cyber system construction for shipowners/ship management companies and system developers, and sets forth measurable security assessment methods, inspection and test requirements.

Chapter 1 General

Section 1 General provisions

1.1.1. Application

1.1.1.1. The Guideline is applicable to digital communication-based ship cyber system and its devices.

1.1.1.2. The Guideline provides guidance to the construction, operation and maintenance, assessment and survey of ships (including the ships and offshore facilities) cyber and system to ensure security and necessary threat defense competence of ship cyber and system, and works as a reference and operation guidance for ship cyber security risk management.

1.1.1.3. The Guideline mainly includes the following content:

(1) Guidance to construction, operation and maintenance of ship cyber system with technology and management.

(2) Product security assessment requirements;

(3) Ship survey and assessment requirements.

1.1.2. General requirements

1.1.2.1. Effective technical measures should be taken, and an effective ship cybersecurity risk management system should be established and implemented in order to improve the ability to resist cybersecurity threats, ensure that cybersecurity risks are at an acceptable level, and meet expectations for cybersecurity of the relevant parties (operators, users, supervision etc.). The acceptable extent is the maximum tolerable limit for security risks (the likelihood and consequences of security events).

1.1.2.2. The ship cyber designer shall plan ship cyber security, clarify overall policies and strategies of ship cyber security, and compile ship cyber security plan specification that shall include objectives, ranges and principles of security tasks and explain how management and technical measures together form a complete safety system.

1.1.2.3. The ship cyber designer shall carry out cyber security risk assessment at design stage, analyze and evaluate the compliance of design scheme and cyber security plan (objectives and requirements) with applicable standards, in order to improve design scheme and serve as the basis for risk control in the process of cyber system construction.

1.1.2.4. Builders such as ship manufacturer and/or ship cyber integrator shall prepare and improve cyber security construction management regulations before construction of cyber system, and better devices, facilities and technical measures, with a view to ensuring cyber security risk during construction within an acceptable extent.

1.1.2.5. Operator and maintainer such as ship operator and/or ship manager shall, before ship's sea trial/cyber system operation, carry out cyber security risk assessment at operation and maintenance stage, work out and improve management regulations of ship cyber system operation and maintenance based on assessment results, and better devices, facilities and technical measures, so as to ensure cyber security risk during system operation and maintenance within an acceptable extent.

Section 2 Class Notation

1.2.1. Class notation and assessment report

1.2.1.1. Ship cyber system products, applied for assessment and qualified in drawing review and assessment by ISC, will be granted with assessment reports.

1.2.1.2. Ship, applied for assessment and qualified in drawing review and assessment by ISC, t will be granted with the following additional notation.

Cyber Security (P, S)

Where, P indicates meeting basic requirements and S meeting higher requirements.

(1) Where ship is found in compliance with the provisions of management requirements in Chapter 2 and technical requirements as listed in Table 1.1.3.2 of this guideline after plan approval and surveys, the class notations Cyber Security (P) will be assigned.

Technical Requirements of Class Notation Cyber Security (P) **Table 1.1.3.2**

	Clauses	Description	Class-P
Physical security	3.2.1	Physical location requirements	√
	3.2.2	Physical access control	√
	3.2.3	Device installation	√
Cyber architecture	3.3.1	Network redundancy	-
	3.3.2	Network segregation and segmentation	√
	3.3.3	Communication security	√
	3.3.4	Wireless network	√
	3.3.5	Assets List	√
	3.3.6	Network testing	√
Region boundary	3.4.1	Boundary protection	√
	3.4.2	Malicious code prevention	√
	3.4.3	Intrusion prevention	-
	3.4.4	Monitoring and alarming	-
	3.4.5	Remote operation and maintenance (if applicable)	√
	3.4.6	Access control	√
Computing environment	3.5.1	Identity authentication	√
	3.5.2	Data security	√
	3.5.3	System installation and update	√
	3.5.4	Accident response and recovery	√
	3.5.5	Backup	√
Security	3.6.1	Configuration requirement	√

audit	3.6.2	Security audit (log)	-

(2) Where ship is found in compliance with the provisions of management requirements in Chapter 2 and technical requirements in Chapter 3 of this guideline after plan approval and surveys, the class notations Cyber Security (S) will be assigned.

1.2.1.3. Assignment, maintenance, suspension, cancellation and reinstatement of class notation for ship cyber security shall conform to provisions in Section 9, Chapter 2, Part 1 of ISC *Rules for Classification of Sea-going Steel Ships*.

1.2.2. Application

1.2.2.1. The party who intends to apply for ISC ship cyber security assessment of system and/or ship shall submit written application to ISC, or its designated organ, or its branch in the locality, and if necessary, enter into assessment service contract and/or agreement.

1.2.2.2. Where system and/or ship applying for additional marking of ship cyber security has not yet received the above assessment, ISC will conduct pre-assessment pursuant to Appendix 2 before accepting the application.

Section 3 Definitions and references

1.3.1. Definitions

1.3.1.1. Access control refers to a selective limit specific to system interaction competence and mode, including control in using system resource to process information, in accessing system information and knowledge, or using components and functions of control system.

1.3.1.2. Asset management refers to a control of any data, computer or device.

1.3.1.3. Authorization refers to prevention of system access or use by unauthorized user, namely, data access authority of user.

1.3.1.4. Backbone network refers to connection of various sub-networks or LANs by bridges or routers to form a single bus or ring topology.

1.3.1.5. Configuration management refers to operations and programs working to handle hardware and software changes systematically in order to maintain integrity of system or device.

1.3.1.6. Control system refers to a management system that is composed of control subject, object and medium, and is furnished with its own objectives and functions. It works to maintain or change interests or variables in a machine, mechanism or other device by expected way.

1.3.1.7. Cyber security refers to characteristics of confidentiality, integrity and availability of information stored, transmitted and processed in cyber environment.

1.3.1.8. Data loss prevention (DLP) system refers to a system in which works to control internal files by virtue of identity authentication, encryption control and statistics of use log.

1.3.1.9. Cyber-attack refers to any form of attack operation specific to IT and OT systems, computer network and PC device for the purpose of accessing, threatening and destroying system and data of a company and/or a ship.

1.3.1.10. Cyber incident refers to an incident that exerts actual or potential negative influence on ship system, network and computer, or information processed by, stored in and transmitted via the system, network and computer, and whose consequences are eliminated by response measures.

1.3.1.11. Cyber system refers to a system integrating facilities, personnel, procedures, communications and network services, such as information management system, control system and access control system.

1.3.1.12. Defect refers to an unexpected software function.

1.3.1.13. Deny of Service (DoS) refers to a type of cyber-attack which prevents legal and authorized user from accessing the information generally by the means of server buffer overflow.

Distributed DoS refers to a DoS through controlling multiple computers and/or servers by a cyber attacker.

1.3.1.14. Firewall refers to a logic or physical block working to prevent unauthorized access to cyber system facilities and information.

1.3.1.15. Information security refers to security measures of information to prevent unauthorized access, closing, modification or destroy.

1.3.1.16. Intrusion detection system (IDS) refers to device or software application working to monitor cyber or system activities, detect malicious or rule-breaking operations and report such operations.

1.3.1.17. Intrusion prevention system (IPS), also known as intrusion detection and protection system, refers to a cyber security device working to monitor cyber and system malicious activities.

1.3.1.18. Local area network (LAN) refers to a network connecting computers within limited area covered by network media.

1.3.1.19. Malware generally refers to software infecting computer system and impairing system performance.

1.3.1.20. Network topology refers to a physical layout in which the various devices are connected by transmission media.

1.3.1.21. Network transmission media refer to physical channels bridging senders and receivers in the network, such as coaxial cable, optical fiber and wireless transmission.

1.3.1.22. Information technology (IT) refers to technology and system working to manage and process information.

1.3.1.23. Operation system, namely, industrially automatic control system, refers to a system working to enable more automatic, effective and precise industry manufacture and operation process in controllable and visual manner by virtue of computer technology, microelectronics technology and electrical means.

1.3.1.24. Operational technology (OT) refers to technology and system working to monitor and control ship software, hardware and network.

1.3.1.25. Recover refers to important system service and operation within a short term and recovery activities of all abilities within a long term after an incident.

1.3.1.26. Risk assessment refers to a data collection and value distribution process involving notification of priorities, establishment of action plan and notification of decisions and risks.

1.3.1.27. Risk management refers to a process involving risk identification, analysis, assessment and communication, acceptance, avoiding, transfer or control within an acceptable extent, as well as consideration of cost and efficiency measures.

1.3.1.28. Router refers to device transmitting data from one network to another, such as from satellite communication network to ship computer network.

1.3.1.29. Virtual local area network (VLAN) refers to a network enabling geographically-scattered network nodes to communicate just like in the same physical network.

1.3.1.30. Virtual private network (VPN) refers to a network enabling user to transmit and receive data via shared or public network and accordingly to enjoy functions, security and management strategies of private network just like a case in which the computer is directly connected to the private network.

1.3.1.31. Virus refers to hidden and self-replicable computer software that maliciously infects and operates computer program and system.

1.3.1.32. Wi-Fi refers to a kind of technology allowing electronic devices to access a wireless local area network (WLAN).

1.3.1.33. For definitions of Category-I/II/III systems, refer to the provisions in 2.6.3, Chapter 2, Part

7 in ISC *Rules for Classification of Sea-going Steel Ships*.

1.3.2. References

References to relevant documents in the guideline constitute requirement of the guideline. For references with no date indication, their latest version applies to the guideline.

(1) ISC *Rules for Classification of Sea-going Steel Ships* and its modification notification

(2) UR E22

(3) *Review on Industrial Control Network and System Information Security Standardization - Part 2-1: Industrial Automation and Control Security Management System* (IEC 62443-2-1)

(4) *Review on Industrial Control Network and System Information Security Standardization - Part 3-3: System Security Requirements and Security Levels* (IEC 62443-3-3)

Chapter 2 Management Requirements

Section 1 General provisions

2.1.1. General requirements

2.1.1.1. It is required to establish and implement effective ship cyber security risk management system in order to enhance competence of defense against cyber security threats, ensuring cyber security risks within an acceptable extent, and meeting cyber security expectations of interested parties (operators, users and supervisors).

2.1.1.2. Effective security risk management system refers to risk-based sustainable improvement management institution, composed of planning, design, implementation, operation, inspection, assessment, maintenance and improvement, as shown in Figure 2.1.1.2.

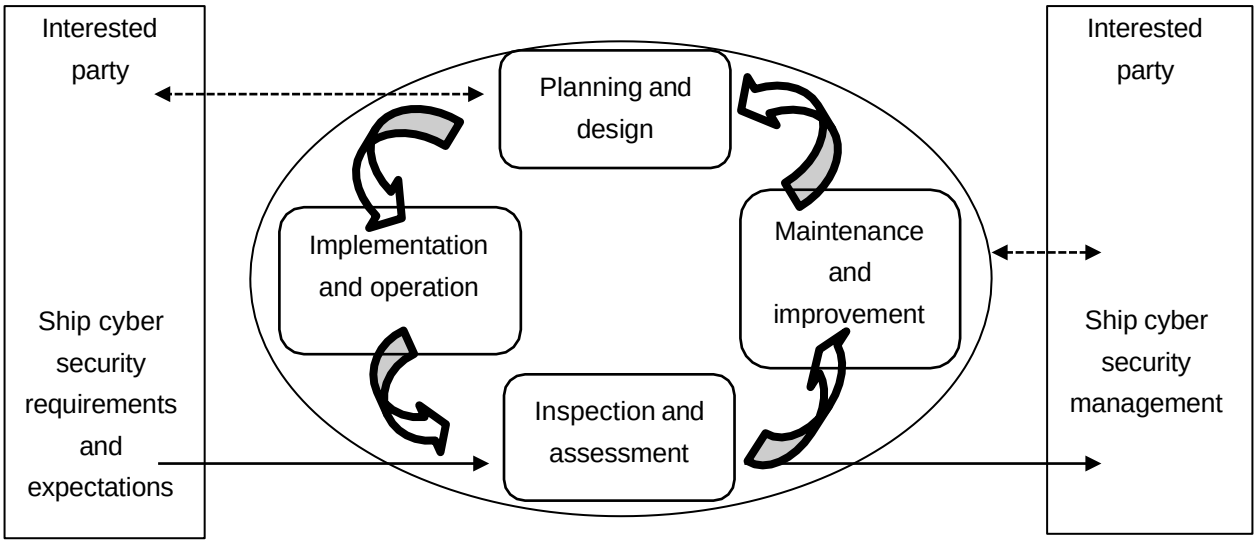

Figure 2.1.1.2

2.1.1.3. Section 2 to 6 of this Chapter are recommended requirements, covering security and safety key-points to be considered in ship cyber security risk management, in order to guide interested parties to establish and implement ship cyber security risk management system. The requirements may be replaced by other effective management measures or technical measures.

2.1.2. Construction management

2.1.2.1. Construction management system shall be established, setting out security management organ and posts, management responsibilities of specific organ and personnel, which shall be notified to interested parties (including organ and personnel) in written form.

2.1.2.2. During ship cyber system construction, management shall be carried out in accordance with the developed construction management system, and the records related to important events shall be taken, including but not limited to:

(1) Cyber security awareness and skill training/education of relevant personnel;

(2) Purchase of cyber products (software and hardware);

(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 service provider after cyber delivery.

2.1.2.3. Prior to commencement of construction of ship cyber system, the surveyor is to review and confirm the latest effective ship cyber security construction management documents, and to assess the integrity of management system.

2.1.2.4. During the construction process, the information concerning ship cyber security management organ and personnel, management recording documents (including reports, logs and record sheets) shall be submitted to the ship surveyor for inspection to verify compliance of security management efforts with management system operation and security strategy requirements.

2.1.2.5. Important engineering nodes, such as ship cyber integration test, cyber security test, on-board installation, sea trial, acceptance and delivery, shall be witnessed by the ship surveyor on site.

2.1.3. Operation and maintenance management

2.1.3.1. Operation and maintenance management system shall be established, setting out security management organ and posts, management responsibilities of specific organ and personnel, which shall be notified to relevant parties (including organ and personnel) in written form.

2.1.3.2. During ship cyber system operation and maintenance, management shall be carried out pursuant to the developed operation and maintenance management system, and management records related to important events shall be taken, including but not limited to:

(1) Cyber security awareness and skill training/education of relevant personnel;

(2) Security management of ship cyber and information assets, including asset registration and change;

(3) Operation and maintenance management, including routine operation and maintenance, emergency preparation, emergency response, and regular inspection/detection.

(4) Security management of operator;

(5) Ship cyber system risk assessment;

(6) Ship cyber security management review and assessment (internal and/or external review(s)).

2.1.3.3. The latest effective ship cyber security operation and management documents shall be on shipboard for reference at any time. In initial survey, the ship cyber security operation and maintenance management documents shall be submitted to the surveyor for inspection to verify integrity of management system.

2.1.3.4. In annual survey, the information concerning ship cyber security operation and maintenance management organ and personnel, management recording documents (including reports, logs and record sheets) shall be submitted to the surveyor for inspection to verify compliance of security management efforts with management system requirements.

2.1.3.5. When ship cyber system have undergone major modification, relevant documents and drawing shall be submitted to ISC, and inspected by surveyor to confirm that the modified and related portions are to comply with the requirements of the management system. In case of major safety incidents, ISC shall be informed in time, and the accident information, accident treatment solutions shall be submitted to ISC.

Section 2 Management system

2.2.1. System and documentation

2.2.1.1. The builder shall develop security construction management system, including but not limited to applicable management activities as specified in Section 4 and Section 5 of this Chapter. The operator shall develop security operation and maintenance management system, including but not limited to applicable management activities as specified in Section 4 and Section 6 of this Chapter.

2.2.1.2. The management system shall be documented, generally cover four levels of documents, namely, management manual, management regulations/procedures, operation specifications/instructions, and recording sheets/reports.

2.2.1.3. Management manual, as a guiding document, specifies security management objectives, policies, ranges, principles, organizational structure, operational framework of management activities and security strategies.

2.2.1.4. Management regulations/procedures, as documents concerning procedures and regulations, specify management processes, management activities and management standards concerned, and clarify the input, output and interaction of management process.

2.2.1.5. Operation specifications/instructions, as documents concerning guidelines and operations, serve to guide specific management implementation, including operation instructions, operation manuals and technical specifications.

2.2.1.6. Recording sheets/reports, as documents concerning records, work to further standardize management input and output.

2.2.2. Formulation and release

2.2.2.1. Departments or personnel shall be designated and authorized to work out management system.

2.2.2.2. The management system shall be released and implemented in official and valid manner upon approval, and be controlled in terms of document version.

2.2.3. Review and improvement

2.2.3.1. Internal review shall be triggered regularly or in case of major change in order to ensure performance of security management system meets expectation and conforms to requirements of competent organization and applicable laws and regulations.

2.2.3.2. Management assessment shall be conducted regularly or in case of major change in order to demonstrate suitability, conformity, sustainability, stability, sufficiency and effectiveness of security management system, assess and determine improvement opportunities and change needs.

2.2.3.3. The non-conformance found in inspection, review, assessment and security incident investigation shall be corrected by taking corrective and preventive measures for control. If necessary, the security management system shall be modified in terms of insufficiency or matters to be improved.

Section 3 Management organization

2.3.1. Organization and post

2.3.1.1. The builder and the operator should set up a three-layer management organization including the decision layer, the management layer and the executive layer, and relevant posts, define post duties, and assign personnel or allocate post duties to specific personnel. Conflicting duties and areas of responsibility should be separated to reduce possibilities of unauthorized or unintentional modification or misuse.

2.3.1.2. The decision layer generally refers to the committee or the leading group guiding and managing the cyber security management work, with the top leader to be taken or authorized by the unit director/leader in charge, responsible for the decision-making of ship cyber security policies, strategies and major issues, etc.

2.3.1.3. The management layer generally refers to the functional department or the working group of cyber security management, which is responsible for specific organization and coordination of routine ship cyber security management.

2.3.1.4. The executive layer of the builder is generally composed of security administrators, system administrators and other relevant posts, which is responsible for performing specific management. The security administrator is the responsible person of cyber security. The system administrator is responsible for deployment, installation, configuration, technical support, routine operation and maintenance management of cyber system and relevant facilities.

2.3.1.5. The executive layer of the operator is generally composed of on-board security administrators, on-board system administrators, on-shore system administrators and other relevant posts. The on-board security administrator is responsible person of ship cyber security, who is

generally taken by the captain or the person assigned by the captain. The on-shore system administrator is responsible for deployment, installation, configuration and technical support of ship cyber system and relevant facilities. The on-board system administrator is responsible for routine operation and maintenance management of ship cyber system and relevant facilities.

2.3.2. Authorization and approval

2.3.2.1. Authorization and approval matters, approval departments and approval persons shall be identified according to duties of functional departments and posts.

2.3.2.2. Approval procedures shall be worked specific to such matters as system change, important operation, physical access and system access. And the approval process shall be carried out in accordance with the approval procedures.

2.3.2.3. It is necessary to review approval matters regularly (with intervals of less than one year), and update matters requiring authorization and approval, approval departments and approval persons timely.

2.3.3. Communication and cooperation

2.3.3.1. Cooperation and communication shall be strengthened among managers, internal and external organizations (in supervision and inspection) by holding coordination meetings if applicable to tackle cyber security issues cooperatively.

2.3.3.2. Cooperation and communication shall be enhanced with external organizations, suppliers, experts and security organizations concerning cyber security.

2.3.3.3. Contact list of external organs concerning cyber security shall be worked out, containing such information as organ name, cooperation content, contact and contact information.

2.3.3.4. Close attention shall be paid to notices and circulars related to cyber security incidents released by the competent authorities, classification societies and industry associations to have a good understanding of motives and attack modes of cyber security incidents, and accordingly identify threats and take measures.

Section 4 Basic management requirements

2.4.1. Personnel management

2.4.1.1. Employment and demission

(1) Designate or authorize specific department or personnel to take charge of employment;

(2) Review identities, security background and qualifications of personnel employed, and examine their technical skills;

(3) Sign confidentiality agreements with employed personnel and agreements of post duties with personnel in key posts (on-shore system administrators and on-board security administrators);

(4) Terminate all access authorities of personnel leaving office timely; reclaim identity permits, keys, badges as well as hardware, software, user accounts and other relevant assets provided by the employer;

(5) Strict transfer procedures shall be handled, and personnel at key positions shall promise confidentiality obligations after transfer before leaving.

2.4.1.2. Training and examination

(1) Organize security awareness education and post skill training for personnel (including operators) and have them informed of relevant security responsibilities and punishments;

(2) Work out targeted training plans and organize training specific to basic security knowledge and post operation specifications;

(3) Organize examinations for personnel in different posts regularly in terms of ship cyber security management and/or operation skills.

2.4.1.3. Third-party personnel

(1) Before physical access to controlled area, the third-party personnel shall submit a written application, be accompanied by specially-assigned person after approval, and register for filing.

(2) Before access to controlled network access system, the third-party personnel shall submit written application, be granted account and permissions opened and distributed by specially-assigned person after approval, and register for filing.

(3) In remote access, the access point shall be not in public place, and the mutual confirmation shall be made before, in and after access.

(4) Before use of cyber system (including device and application system), the third-party personnel shall receive necessary security training/education.

(5) After departure of third-party personnel, all access authorities shall be cancelled or disabled timely.

(6) The third-party personnel who are granted system access permissions shall sign confidentiality agreements and receive sufficient security training/education, and shall neither conduct unauthorized operations, nor duplicate and disclose any sensitive and important information.

2.4.2. Risk management

2.4.2.1. It is required to take necessary measures to identify security vulnerabilities and potential hazards in construction, operation and maintenance; fix vulnerabilities and hazards found timely or fix them after assessment of possible influence.

2.4.2.2. It is required to carry out cyber security risk assessment regularly or in case of the following circumstances, and prepare risk assessment reports:

(1) When serious cyber and information incident occurs;

(2) When major change occurs or is proposed;

(3) When the internal organ believes it is necessary or when it is required by the external organ.

2.4.2.3. Cyber security risk assessment shall consider but not limited to the following:

(1) Threats, such as malware and network phishing attack, etc;

(2) Identification and protection of fragile system, such as ECDIS and ENPs, etc;

(3) Mitigation measures, such as USB control, etc;

(4) Identification of internal key personnel, such as administrators and personnel reporting suspected incidents, etc;

(5) Hard copies of key contacts, such as DPA (assigned personnel) and CSO (security administrators), etc;

(6) Password management;

(7) Commitments of suppliers/contractors.

2.4.2.4. Cyber security risk assessment during operation and maintenance shall cover technical detection.

2.4.2.5. Security risks found in risk assessment shall be tackled and re-assessed (residual risk assessment).

2.4.3. Security inspection

2.4.3.1. It is required to organize routine security inspection regularly specific to routine system operation, system vulnerabilities and data backup; fix security vulnerabilities and potential hazards found timely or fix them after assessment of possible influence.

2.4.3.2. It is required to organize overall security inspection specific to effectiveness of existing security technical measures, consistency between security configuration and security strategy, and effectiveness of security management system.

2.4.3.3. It is required to prepare security checklist and implement security inspection, collect security inspection data, compile security inspection report and notify security inspection results.

2.4.4. Change management

2.4.4.1. It is required to define change requirements before change, work out change scheme and implement the scheme upon approval.

2.4.4.2. It is required to establish change application and approval control procedures, control all changes pursuant to procedures, and record change implementation process.

2.4.4.3. For major changes, it is required to conduct risk assessment for possible change failure, work out procedures to suspend change and recover from failed change, define process control methods and personnel duties, and if necessary, organize drills specific to recovery process.

2.4.5. Incident and emergency management

2.4.5.1. Security weakness and suspected incident shall be reported to the administrator and other relevant personnel timely.

2.4.5.2. Security incident reporting and handling management regulations shall be worked out to set forth reporting, handling and responding processes of different security incidents, including field handling, incident reporting and duties of recovery.

2.4.5.3. Efforts shall be made in security incident reporting, responding and handing process to analyze and figure out incident cause, collect evidence, record handling process and summarize experience and lesson.

2.4.5.4. Major security incidents resulting in system suspension and information leak shall be handled and reported following different procedures properly.

2.4.5.5. For major security incidents, it is required to launch incident investigation after field emergency response, work out incident investigation report, trigger risk assessment if necessary, and modify deficient documents of management system.

2.4.5.6. Emergency plans shall be worked out to set out how to timely find security incidents and take measures to lower incident consequences. Proper response actions shall be taken to ensure security and recovery of affected system. Symptoms to be found, control measures to be taken immediately, actions to restore system and communication mode among personnel shall be covered at least. All emergency measures shall be easy to understand by the seamen. Where on-shore support is needed, the way to obtain external assistance shall be explained.

2.4.5.7. Emergency plan training and drills shall be organized regularly for relevant personnel.

2.4.5.8. Emergency plans shall be re-assessed, modified and improved regularly or after emergency response.

2.4.5.9. Emergency plans shall be stored in such places for easy access by responsible persons. Their validity shall not lose due to occurrence of cyber security incident, which is independent of ship cyber hard copy (paper version) or electronic device.

2.4.6. Backup and recovery management

2.4.6.1. Data backup and recovery strategies, backup and recovery procedures shall be worked out according to data importance and influence of data on system operation.

2.4.6.2. Important business information, system data and software system requiring regular backup shall be identified. And backup plans shall be charted, specifying backup scope, mode and frequency, storage medium and period.

2.4.6.3. Regular tests shall be conducted specific backup data and recovery procedures to ensure backup data works normally. Backup medium validity shall be inspected and tested to ensure backup recovery is completed within the time as specified by the recovery procedures.

2.4.7. Service provider management

2.4.7.1. It shall be ensured that selection of service providers conforms to regulations of relevant organs, including product supplier, communication service provider and outsourced operation and maintenance service provider.

2.4.7.2. Agreements shall be signed with selected service providers, defining cyber security obligations that shall be performed by parties concerned throughout the whole service supply chain.

2.4.7.3. It is required to monitor, assess and review services offered by service providers regularly, and control service changes.

2.4.7.4. Security mechanism, service level and management requirements of all cyber services shall be identified and be included in cyber service agreements.

2.4.7.5. Outsourcing operation and maintenance service providers shall also meet the following requirements:

(1) Operation and maintenance services shall be outsourced to service providers with the ability to carry out security operation and maintenance meeting requirements in terms of technology and management. And ability requirements shall be defined in the signed agreements.

(2) Agreements shall be concluded, specifying outsourced operation and maintenance scope, work description and security requirements, such as requirements for access, processing and storage of sensitive/important information, and emergency guarantee requirements for service suspension of IT/OT facilities, network and application systems.

2.4.8. Password management

2.4.8.1. The password standards shall be met.

2.4.8.2. Password technology and products that are certified and recognized by the password management regulatory authority shall be adopted.

2.4.9. Confidentiality management

2.4.9.1. Confidentiality requirements of state secrets, business secrets and privacy specified by competent organs shall be met.

2.4.9.2. Disclosure of information in confidentiality scope and malicious information shall be controlled.

2.4.9.3. Information transmission shall be controlled to protect security of all types of information transmitted via communication facilities. Furthermore, confidentiality agreements or no-disclosure agreements shall be signed to prevent information transmitted from being disclosed.

Section 5 Supplementary requirements for construction management

2.5.1. Determination of needs

2.5.1.1. Ship cyber security needs and objectives, and ship cyber scope shall be set forth in writing form. Security needs include requirements and expectations of interested parties.

2.5.1.2. Interested parties and security technology experts shall be organized to demonstrate rationality and accuracy of security needs and objectives.

2.5.1.3. Security needs and objectives determined shall be approved by the shipowner.

2.5.2. Planning and design

2.5.2.1. Overall security plan and scheme design shall be worked out according to security objectives. And corresponding documents shall be formulated.

2.5.2.2. Basic security measures shall be selected according to security objectives, and be

supplemented and adjusted referring to risk analysis results.

2.5.2.3. Interested parties and security experts shall be organized to demonstrate and review rationality and accuracy of overall security plan and corresponding documents. And the plan shall be implemented only upon approval by the shipowner.

2.5.3. Project implementation

2.5.3.1. Departments or personnel shall be designated or authorized to take charge of managing the project implementation.

2.5.3.2. The project implementation management scheme shall be worked out to control project implementation, ensure security of development environment and monitor outsourcing development activities.

2.5.3.3. Third-party project supervisors shall be assigned to monitor and control project implementation.

2.5.4. Product purchase and use

2.5.4.1. Purchase and use of cyber security products shall meet applicable regulations.

2.5.4.2. Purchase and use of password products and services shall meet password management requirements.

2.5.4.3. Model selection test of products shall be conducted in advance to determine product candidates. And the list of product candidates shall be reviewed and updated regularly.

2.5.5. Software development

2.5.5.1. Development environment and actual runtime environment shall be separated. Test data and test results shall be controlled.

2.5.5.2. Software development management regulations shall be worked out, setting forth control methods of software development and code of conduct for personnel.

2.5.5.3. Coding security specifications shall be worked out. And developers shall write code according to specifications.

2.5.5.4. Documents of software design and use guidelines shall be worked out. Use of documents shall be controlled.

2.5.5.5. The security test shall be carried out in the software development process. For outsourced development, the potential malicious code shall be detected before software delivery. For independent development, the potential malicious code shall be detected before software installation.

2.5.5.6. Update and release of the software system shall be authorized and approved. Modification versions of program resource library shall be controlled.

2.5.5.7. For independent development, all developers shall be of full-time nature and all development activities shall be monitored.

2.5.5.8. For outsourced development, the software source code shall be provided by the development party and the potential back-doors and hidden channels in the software shall be detected.

2.5.6. Testing and acceptance

2.5.6.1. Before on-board implementation, it is required to work out the testing scheme, clarifying testing content (at least including password use security), conduct test according to the testing scheme, and prepare the test report.

2.5.6.2. After on-board implementation, it is required to work out acceptance testing scheme, clarifying testing content, conduct acceptance test according to the scheme, and prepare the acceptance test report.

2.5.6.3. Testing data shall be selected carefully, and shall be protected and controlled properly.

2.5.7. System delivery

2.5.7.1. It is required to work out delivery checklist and check devices, software and files to be delivered according to the checklist. Such checklist shall be attached in the ship.

2.5.7.2. The technical personnel in charge of operation and maintenance shall receive corresponding skill training.

2.5.7.3. Construction Process documents and operation and maintenance documents shall be prepared.

2.5.8. Management of cloud service providers

2.5.8.1. It is required to select such cloud service providers of the ship cyber system as meet security regulations. The cloud computing platform provided shall be able to protect security of the business application system.

2.5.8.2. All cloud services and specific technical parameters shall be specified in service agreements signed with cloud service providers.

2.5.8.3. All authorities and responsibilities of cloud service providers shall be specified in service agreements signed with cloud service providers, including but not limited to management scope, division of responsibilities, access authority, privacy protection, code of conduct and violation liabilities.

2.5.8.4. Service agreements signed with cloud service providers shall specify that upon service expiration, the cloud service data of clients will be provided fully, and that the relevant data will be cleared from the cloud computing platform as committed.

2.5.8.5. Confidentiality agreements shall be signed with cloud service providers, not allowing the providers to disclose the cloud service data of clients.

2.5.8.6. The information concerning security incidents of supply chain or the information concerning security threats shall be transmitted to the cloud service clients.

2.5.8.7. Important changes of suppliers shall be notified to the cloud service clients. Furthermore, security risks arising from changes shall be assessed. Accordingly, measures shall be taken to control risks.

2.5.9. Mobile internet management

2.5.9.1. In purchase of mobile application software, the application software installed and used in the mobile terminal shall source from reliable distribution channels or use reliable signature certificate.

2.5.9.2. In purchase of mobile application software, the application software installed and used in the mobile terminal shall be developed by the designated developer.

2.5.9.3. In development of mobile application software, the software developer shall be assessed in terms of qualification.

2.5.9.4. In development of mobile application software, the signature certificate of software shall be legal.

2.5.10. Operation system management

2.5.10.1. The important devices shall be purchased and used only upon security detection by the professional organization as recognized by the classification society.

2.5.10.2. In outsourcing of software development, the outsourcing development contracts shall

specify binding clauses specific to development parties and suppliers, involving confidentiality of devices and system in life cycle, no disclosure of key technology and professional application of devices.

2.5.11. Big data management

2.5.11.1. It is suggested to select such big data platforms as meet security regulations. The big data platforms provided shall be able to protect security of big data application.

2.5.11.2. It is suggested to specify authorities and responsibilities of big data platform providers, details of services (security services especially) and specific technical parameters.

2.5.11.3. It is suggested to define data protection responsibilities of the receivers of exchanged and shared data, and ensure that the receivers have sufficient or required security protection abilities.

Section 6 Supplementary requirements for operation and maintenance management

2.6.1. Environmental management

2.6.1.1. Management regulations shall be worked out specifically to physical access and carrying-in and carrying-out of personal device. Visits to the ship shall be approved, and visitors shall be accompanied by specially-assigned persons and record their visits.

2.6.1.2. Security zones shall be defined which is used to protect areas containing sensitive information or critical information and information processing facilities. Security zones shall be protected with proper access control to ensure only authorized personnel have access to the zones.

2.6.1.3. Visitors shall not have access to security zones. Paper documents and mobile storage media containing sensitive/important information shall not be placed at will.

2.6.1.4. Special personnel shall be designated to periodically maintain and manage power supply and distribution, air conditioning, temperature and humidity control, fire control and other facilities in the computer room and other places.

2.6.1.5. Devices shall be arranged and protected properly to minimize threats and hazards from the environment and to minimize possibilities of unauthorized access.

2.6.1.6. Devices shall be prevented from power or communication suspension and from suspension due to failure of supporting facilities.

2.6.1.7. Unattended devices shall be protected properly by such measures as locking screen or video surveillance to prevent unauthorized use.

2.6.1.8. It is required to adopt strategies of removing desktop paper and mobile storage media, and strategies of hiding screens of information processing facilities (such as lock screens and screensavers).

2.6.2. Asset management

2.6.2.1. Inventory of assets related to protected objects (hosts and network/security devices) shall be prepared and maintained, indicating user, maintainer, location, importance level, backup method and period (if any) of each asset.

2.6.2.2. Assets shall be identified and registered, and management measures shall be selected according to importance level of the assets to control adding, change, maintenance/repair, leave/return, scrap and other basic conditions of assets.

2.6.2.3. Use of assets shall be monitored and adjusted, and the future capacity requirements of assets shall be reflected to ensure system performance.

2.6.3. Media management

2.6.3.1. The media shall be stored in a safe environment, and be controlled and protected. Special management and periodical inventory check shall be conducted. The media for update and maintenance of ship system software shall be used by specially-assigned persons.

2.6.3.2. Personnel selection, packaging and delivery shall be controlled in order to prevent unauthorized access, abuse or damage in transport of media. Furthermore, archiving and inquiry of media shall be recorded.

2.6.3.3. Access to private mobile media (except for seaman-dedicated entertainment network) are not allowed, and only access to dedicated mobile media shall be allowed for key devices such as ECDIS.

2.6.3.4. As for scrapping, the media shall be disposed reliably and safely according to formal procedures.

2.6.4. Device management

2.6.4.1. All devices (including backup and redundancy devices) and circuits shall be maintained periodically by specially-assigned persons in order to ensure their continuous availability and integrity.

2.6.4.2. The management system related to supporting facilities, hardware and software maintenance shall be established to effectively manage their maintenance, include responsibilities of maintenance personnel, approval of maintenance and service, supervision and control of maintenance process.

2.6.4.3. The information processing devices shall be approved before being taken off the ship. Time of taking the device off the ship and returning the device shall be recorded. When the device containing storage media is taken out, the important data thereof shall be encrypted or cleared. The devices shall be protected against unauthorized use and information disclosure (such as device theft and loss) during off-site (such as being taken off the ship). Special consideration shall be given to cyber and information security regulations specified by competent authorities of the relevant nation/region when the device is taken in or out of a nation/region.

2.6.4.4. No device shall be taken off the site without prior authorization. The shipowner shall designate a responsible person who has the right to permit dismantlement of a device (including parts of a device) on site. Time limit of taking a device dismantled off the site shall beset and return time shall be recorded.

2.6.4.5. As for a device containing storage media, data in the media shall be completely cleared or covered safely before the device is scrapped or reused, in order to ensure sensitive/important data and authorized software in the device cannot be recovered for reuse.

2.6.4.6. External communication interfaces such as USB interfaces and network cable interfaces of the devices shall be effectively controlled for access through physical locking and/or technical encryption to prevent unauthorized use.

2.6.4.7. Portable computers, pocket computers and other mobile devices (including external devices carried by seamen and third-party personnel) shall be effectively controlled for use on board to prevent unauthorized access and use. Access to private devices is not allowed except for access to seaman-dedicated entertainment network.

2.6.5. Security management of cyber and application system

2.6.5.1. The security management system of cyber and application system shall be established, specifying provisions related to account management, installation and update, operation and maintenance and log, access control, malicious code prevention and configuration management.

2.6.5.2. Account management

(1) Assign different roles to manage and use cyber and application system; clarify responsibilities and authorities of each role.

(2) Control such acts of applying for, establishing and deleting accounts; review accounts and access authorities periodically; only allow users to access network and its services explicitly authorized to use; limit and control allocation and use of privileges.

2.6.5.3. Installation and upgrade

(1) Designate personnel that have received training and possess proper authorities to install, configure, update, upgrade and patch devices and software; apply for approval of installed devices and software; generate logs after successful operation; work out manuals about installation, configuration and operation; make safety and optimization configurations pursuant to the manuals.

(2) Pay close attention to release of vulnerabilities and patches; manage software installation, upgrade and patches strictly; employ professional technical organizations for security assessment, testing and verification before software upgrade and patch installation of key OT systems.

(3) Work out plans before installation, configuration, update, upgrade and patching, so as to restore if necessary.

2.6.5.4. Operation and maintenance and its log

(1) Record the operation and maintenance log in detail, including routine inspection, operation and maintenance records, parameter setting and modification.

(2) Control changeability of operation and maintenance strictly; change connection, software/component installation, or configuration parameters adjustment shall be approved; keep unchangeable audit logs during operations; update synchronously configuration file/information database after operations.

(3) Control the use of operation and maintenance tools strictly, especially those that can cover software system and application permission control; enable access for operation only after approval; keep unchangeable audit logs during operations; delete sensitive data in tools after operations.

(4) Control activation of remote operation and maintenance strictly; activate ports or channels of remote operation and maintenance only after approval; keep unchangeable audit logs during operations; delete sensitive data in tools after operations; remote access points shall be not allowed to come from public places; make mutual confirmation before access, during access and upon access completion; designate trained internal personnel to monitor all activities during remote maintenance.

(5) It is advisable to monitor running state of cyber and application system and respond to the alarm timely.

(6) It is advisable to make periodical analysis and statistics on log, monitoring and alarm data to identify suspicious behaviors timely.

2.6.5.5. Access control

(1) Ensure that all external connections are authorized and approved; periodically check acts which violate wireless access and other cyber security strategies; strengthen cyber security awareness education and training if necessary.

(2) Control access to cyber and application system through secure login procedures if the access control is required.

2.6.5.6. Malicious code prevention

(1) Enhance awareness of all users against malicious code; check malicious code of externally-sourced computers and storage devices before access; check the malicious code of externally-sourced files (email attachments and files downloaded from the web etc.) before use (read or execute).

(2) Implement detection, prevention and recovery measures against malicious code/software;

periodically verify effectiveness of technical measures (such as anti-virus software and virus database) against malicious code attacks.

2.6.5.7. Configuration management

(1) Record and save basic configuration information, including network topology, software/components installed in each device, version and patch information of software/components, and configuration parameters of each device or software/components.

(2) Incorporate change in basic configuration information into change management scope; control configuration information change; update basic configuration information base timely.

2.6.6. Cloud computing management

2.6.6.1. Confidentiality agreements shall be signed with cloud service providers, not allowing the providers to disclose the cloud service data of clients.

2.6.6.2. The information concerning security incidents of supply chain or the information concerning security threats shall be notified to the cloud service clients timely.

2.6.6.3. Important changes of suppliers shall be notified to the cloud service clients timely. Furthermore, security risks arising from changes shall be assessed. Accordingly, measures shall be taken to control risks.

2.6.6.4. Location Selection of operation and maintenance for cloud computing platforms and implementation of operation and maintenance shall comply with regulations of regulatory authorities and related organizations.

2.6.7. Mobile internet management

2.6.7.1. Legal wireless access device and legal mobile terminal configuration library shall be established to identify illegal wireless access device and illegal mobile terminal.

2.6.8. Internet of Things management

2.6.8.1. Personnel shall be assigned to inspect deployment environment of sensing node devices and gateway node devices periodically, record and maintain environmental abnormalities that may affect normal operation of sensing node devices and gateway node devices.

2.6.8.2. Regulations shall be specified clearly to the procedure of warehousing, storage, deployment, carrying, maintenance, loss and scrapping of sensing node devices and gateway node devices. And the management shall be carried out throughout the process.

2.6.8.3. It is necessary to strengthen confidential management for deployment environment of sensing node devices and gateway node devices. For example, the personnel responsible for inspection and maintenance shall immediately return relevant inspection tools, and inspection and maintenance records when they are transferred from posts.

2.6.9. Big data management

2.6.9.1. It is advisable to establish digital asset security management strategies, specifying operation specifications, protection measures and responsibilities of managers in the whole life cycle of data, including but not limited to data acquisition, storage, processing, application, flow and destruction and other processes.

2.6.9.2. It is advisable to develop and implement data classification and classified protection strategies, and work out different security protection measures for different classification and grading of data.

2.6.9.3. It is advisable to divide the scope of important digital assets based on data classification

and grading, and define use scenarios and business handling process of automatic desensitization or de-identification of important data.

2.6.9.4. It is advisable to review classification and grading of data periodically. If it is needed to change classification and grading of data, the changes shall be implemented according to change approval procedures.

Chapter 3 Technical Requirements

Section 1 General provisions

3.1.1. General requirements

3.1.1.1. Proper technical measures shall be taken in such aspects as physical security, network architecture, network boundary, computing environment and security audit to improve threat defense capability of the cyber system.

3.1.1.2. Where technical measures are disabled due to limited conditions, proper management measures may be taken instead.

3.1.2. Physical security

3.1.2.1. Installation of computer-based system shall comply with the requirements of on-board conditions and standby power supply.

3.1.2.2. Computer based system shall meet the requirements of physical access control.

3.1.2.3. Computer based system shall meet the requirements of applicable installation and implementation.

3.1.3. Network architecture

3.1.3.1. Design of the network architecture shall be based on risk assessment.

3.1.3.2. Network design shall ensure that the ship continues operations of critical tasks while maintaining confidentiality, integrity and availability of data required for security.

3.1.3.3. Network equipment, cables and wireless equipment, and related tests shall comply with relevant requirements in Chapter 4 hereof.

3.1.3.4. Redundancy design is required for backbone network, including network communication equipment, network control equipment, and storage equipment.

3.1.3.5. Network segregation shall be carried out by either physical or logical measures (such as virtual private network), and the perimeter of each network zone shall be defined. When connection among different network zones is allowed, the perimeter shall be controlled through proper boundary protection equipment (such as proxies, gateways, routers, firewalls, unidirectional gateways, guards and encrypted tunnels).

3.1.3.6. Network segmentation shall be carried out according to systems of Category-I, II and III, asset importance, system function and other factors. For details of network segmentation, please refer to IEC 62443-2-1.

3.1.3.7. Network protection devices shall be installed on the boundary and proper network security defense devices shall be installed on the boundary between internal and external network of the ship.

3.1.3.8. Network incident monitoring and alarm systems shall be deployed to ensure expected performance and reliability of the cyber, which shall provide sufficient information to describe the cyber incidents for use by expected users. When onboard systems can be accessed from a remote location (not onboard the ship), the cyber Incidents originating from the place outside shall be identified.

3.1.3.9. Network protection safeguards shall be provided for inter network, such as malicious code prevention, intrusion prevention and other measures.

3.1.3.10. Such factors as integration of different networks, interfaces, safety measures, device redundancy and failure alarms shall be considered in the design of network integration.

3.1.3.11. Emergency response plan shall be developed to deal with detected cyber security incidents.

3.1.3.12. Backup and recovery plan shall be developed, including scope, mode, frequency, storage medium and period of backup.

3.1.3.13. Network designed based on Category-II and III systems and integrated systems shall be resilient. That is, fault of any part due to network device failure or cyber accident shall not affect other systems connected to the unaffected cyber.

3.1.3.14. Category-II and III systems and their data shall be separated from non-critical data and processes to minimize damage resulting from attacks.

3.1.4. Network boundary

3.1.4.1. Network boundary shall be identified and controlled based on network segregation and segmentation.

3.1.4.2. Malicious code prevention mechanism shall be established by certain technical means.

3.1.4.3. External or internal cyber-attacks shall be detected, prevented or restricted.

3.1.4.4. External and internal communications shall be monitored and controlled.

3.1.4.5. Remote operation and maintenance of cyber system shall be monitored and restricted.

3.1.4.6. Access control shall be implemented for cyber system.

3.1.5. Computing environment

3.1.5.1. Users (personnel, software and devices) and accounts in the cyber system shall be authenticated.

3.1.5.2. Data in the cyber system shall be safely managed based on risk analysis.

3.1.5.3. The emergency response and accident recovery mechanism shall be established and ensured in terms of its effectiveness.

3.1.5.4. Based on risk analysis, backup plan shall be made specific important business information, system data and software system and be ensured in terms of its effectiveness.

3.1.6. Security audit

3.1.6.1. Network equipment shall meet certain security configuration requirements.

3.1.6.2. Audit shall be made specific to important user behaviors and important security incidents on network boundaries and important network nodes regularly.

Section 2 Physical security

3.2.1. Location

3.2.1.1. On-board computer-based devices shall be stored in such manner as conforms to the ship-dedicated requirements.

3.2.1.2. Cyber system that is still necessary in case of normal power loss shall be able to automatically connect to the reserve power source when the normal power loss occurs. The reserve power source may be UPS, and shall be able to maintain power supply for at least 30 minutes.

3.2.2. Physical access control

3.2.2.1. The server-type equipment shall be installed in the room that can be locked normally to prevent unauthorized access. In case of difficulty, the equipment shall be installed in the cabinet or console that can be locked.

3.2.2.2. Network equipment (routers, switches, firewalls, gateways and protocol converters) of the backbone network shall be installed in the protected facilities.

3.2.2.3. When a mobile device or a portable storage device is used, special attention shall be paid to the following matters to ensure that the device is protected properly:

(1) It is not allowed to connect mobile devices (such as laptops, IPADs and smartphones), including portable storage devices (such as USB drives, HDDs, CDs and DVDs) to any equipment unless specifically authorized.

(2) The portable storage devices that are used for software maintenance shall be authorized by the responsible person before use.

(3) Access to the inter network shall be physically blocked unless access to external devices is for maintenance or similar operation.

(4) Improper and unauthorized connection of portable devices to OT system shall be prevented by strategies and physical or logical means.

3.2.2.4. The security zone shall be protected by the following entrance control means, such as guard by specially-assigned person, installation of barriers or electronic access control system to only allow the authorized person to enter:

(1) Visit log sheets shall be prepared to record the dates and time when visitors enter and leave the area. Particularly, visitors such as service engineers of system integration providers or suppliers shall be identified by ID cards. Only authorized visits are allowed.

(2) All visit records shall be maintained and monitored by the ship owner.

3.2.2.5. Physical security devices

(1) Physical security devices (such as monitoring cameras, intrusion detectors and electronic locks) shall have effective login authentication methods such as passwords, smart cards and tokens. A password, if adopted, shall be a non-default value, keep complex sufficiently and be updated regularly.

(2) Physical security devices shall be tested regularly to ensure that they work in normal operation.

(3) Recorded data of physical security devices can be maintained and accessed only with authorization.

3.2.2.6. It is required to establish access control lists (ACL) for system assets (including devices, equipment, systems, workstations, servers, programmable logic controllers, cyber protocol converters and cyber connections) and make update timely.

3.2.2.7. Access to OT system via the USB port is not allowed unless the device and/or data transmitted via that port has been detected.

3.2.3. Installation

3.2.3.1. In addition to the applicable requirements in Section 2 and Section 3, Chapter 1, Part 4 in ISC *Rules for Classification of Sea-going Steel Ships,* the installation of network devices shall also comply with the requirements of this Section.

3.2.3.2. The redundant devices ensuring stable operation of the network and related systems shall be installed in two different locations as far as possible.

3.2.3.3. Installation of cables shall comply with the relevant requirements in Section 12, Chapter 2, Part 4 in ISC *Rules for Classification of Sea-going Steel Ships*. When the ship backbone network is wired in the form of redundancy, the redundant cables shall keep away from each other as far as possible by, such as, laying cables separately from the port and starboard sides of ship.

3.2.3.4. Critical computers and network devices connected to Category-II and III systems shall be installed in security zones to avoid access by outsiders.

Section 3 Network architecture

3.3.1. Network redundancy

3.3.1.1. Business requirements of cyber systems available shall be identified, and the redundant components or architectures may be considered if availability is not guaranteed by the existing system framework. In general, the redundant components for communication cables, critical network devices, critical computer devices and security devices shall be provided to ensure system availability.

3.3.1.2. The redundant system shall be equipped with failure self-diagnosis function to ensure that the activity execution can be effectively transferred to the standby unit in case of system failure.

3.3.2. Network segregation and segmentation

3.3.2.1. General requirements

(1) Segregation of networks shall be conducted according to plans and documents and risk analysis results. Segregation can be implemented by physical and/or logical means (such as VPN). The boundary of each zone shall be clearly defined.

(2) Critical systems shall be separated into various zones with common security level to facilitate cyber security management.

(3) OT systems that need real-time control and data transmission (such as propulsion system and cargo control system) shall be networked with independent network devices to enable physical security segregation from other data network and external public information network.

3.3.2.2. Where the physical segregation is adopted, the following requirements shall be met at least:

(1) Permanent gateways to the other areas shall not be installed on the network perimeter.

(2) No permanent wireless access should be connected to the network perimeter for OT systems of Category II and III except where specific approval is obtained from Classification Society.

(3) Ports used for removable devices shall be logically unusable. Where the cyber system contains sensitive data, physical locks shall be enabled to prevent unauthorized access to these ports.

3.3.2.3. Where the logical segregation is adopted, the following requirements shall be met at least:

(1) There shall be no data communication between different network zones except through appropriate boundary protection devices.

(2) Ports used for removable devices shall be subject to measures the same as in Section 3.3.2.2 (3).

3.3.2.4. The network shall be segmented according to system category (Category-I, II and III), asset importance, system function and other factors. For details of network segmentation, please refer to IEC 62443-2-1.

(1) For the cyber system containing Category-III systems, physical segmentation shall be provided and independent switches shall be used.

(2) For the cyber containing Category-II systems, logical segmentation on VLANs (Virtual Local Area Networks) may be adopted.

(3) Each segmentation shall have its own address range.

3.3.2.5. Uncontrolled networks, such as crew or passengers-dedicated entertainment network, shall forbid to connect to controlled networks (communication between uncontrolled networks and controlled networks not allowed). The uncontrolled networks are considered insecure.

3.3.2.6. Where interconnection between networks which include systems of different security requirements, all interconnected systems should be treated as the highest requirements.

3.3.2.7. Demilitarized zone (DMZ)

(1) When there exists data exchange or business access between the ship and the outside network, a DMZ ("demilitarized zone"-) may be set up.

(2) Access to the DMZ by the internal and external cyber systems shall be authorized.

(3) DMZ shall be independent of the vessels internal network.

3.3.3. Communication security

3.3.3.1. Communication transmission and interfaces shall be designed by considering possibility and consequences of extending failure of one system or device to another system. And proper technical measures shall be worked out.

3.3.3.2. Communication traffic estimation shall be carried out in network design or change of network architecture based on communication needs in order to meet the peak bandwidth for each part of the business. Communication traffic estimation specification meeting requirements of Clause 3.3.3.3 shall be provided for review.

3.3.3.3. The following factors shall be considered to determine proper data throughput when doing sizing calculations of the cyber system:

(1) Data speed requirement for application;

(2) Data format.

3.3.3.4. Standard interfaces shall be adopted for data exchange between different networks. Design of each network shall meet recognized standards, such as IEC 61158 or IEC 61784.

3.3.3.5. Data classification, grading, format and content shall comply with acceptable international standards such as IEC61162 or other equivalent standards.

3.3.3.6. Critical systems shall be with certain fault-tolerance ability. For Category-II and III systems, the interface devices between sub-systems and their networks shall have some verification capability to ensure normal data transmission. Local control and indicators shall be part of the fault-tolerance architecture.

3.3.3.7. Communication paths and protocols shall be documented in specification.

3.3.3.8. Where the ship cyber supports remote access, the ship-to-shore interface devices shall have the ability to terminate connection and revert to the uncorrupted state. Where the device itself does not have such ability, additional devices shall be installed to meet such function requirement.

3.3.3.9. Interfaces enabling network services for ships shall be managed:

(1) Establish a traffic strategy for each interface;

(2) Ensure confidentiality and integrity of information transmitted through each interface;

(3) Monitor communication interfaces to prevent traffic that is inconsistent with the security configuration strategy;

(4) Record tasks / business requirements and durations that traffic policies should support, and periodically remove policies that are no longer supported;

(5) Limit the number of external networks connections to the system;

(6) Terminate the network connection associated with communications after dialogues or after a period of inactivity.

3.3.3.10. Provide secure out-of-band communication channels as needed to support incident response.

3.3.3.11. No system, module, component, device, or application shall communicate over a network or out-of-band without express permission.

3.3.3.12. IT-OT gateways or interface systems shall be subject to strict and standard-based ports, protocols and services.

3.3.3.13. IT-OT gateways or interface systems shall be maintained under strict file transfer control and filtering.

3.3.3.14. Content filtering modules may be installed to filter communication paths for messages (such as e-mail and social messages) before they are transmitted to a private network, in order to detect and eliminate potentially malicious files, attachments and links.

3.3.3.15. Communication security

(1) Communication encryption: when communicating the external network, communication encryption shall be adopted.

(2) Firewall filtering

① The requirement of communication through firewalls shall be defined. The authorization sources (MAC and IP addresses), protocols, and port numbers shall be controlled and filtered through firewalls.

② To ensure control over security, the communication will be blocked in default state.

③ Security strategies (rules) shall be implemented, allowing expected operation of significant data traffic through the network.

④ The application firewall shall be able to intercept detected intrusions and abnormal communications.

⑤ The next generation firewall shall include application firewall and identity recognition function module.

(3) The intrusion protection system (IPS) works to detect cyber-attacks by virtue of different techniques, such as threat feature code, known vulnerability attacks, abnormal activity, and traffic behavior analysis, and to abandon detected suspicious data packets.

3.3.4. Wireless

3.3.4.1. Design and test of wireless devices shall conform to the requirements of IACS UR E22.

3.3.4.2. Wireless network architecture

(1) Requirement for transmission over wireless network shall be defined and validated.

(2) Systems connected to wireless network shall share the same security requirements.

(3) Wireless communication between OT systems shall be authorized. IT and OT systems shall not be allowed to access the same wireless network.

(4) Critical systems or controlled systems shall not be connected to both wireless and wired networks at the same time.

(5) A mechanism of wireless access shall be protected by entity and encryption authentication.

3.3.4.3. Wireless access control

(1) Ability to uniquely identify and authenticate all users (persons, software processes or devices) participating in wireless communication shall be enabled.

(2) Authorization, monitoring and use of wireless access points connected to control systems shall be controlled in accordance with generally-accepted best practices in industrial circles.

3.3.4.4. It is required to select radio antenna and calibrate transmitted power level to reduce possibility of receiving available signals outside the controlled boundary.

3.3.5. Asset list

3.3.5.1. The shipowner/shipyard shall provide ISC with a list of assets based on the computer cyber system prior to vessel's delivery. The list shall at least contain the following content:

(1) Hardware devices

① Programmable logic controllers (PLCs) and associated devices;

② Distributed control system (DCS) and associated devices;

③ Supervisory control and data acquisition (SCADA) systems and associated devices;

④ Communication devices (such as routers and switches);

⑤ Network devices (such as firewalls and gateways);

⑥ Human-computer interface (HMI);

⑦ Devices connected to OT and IT systems (such as, computers, servers, storage devices and printers);

⑧ Devices connected to important systems of the ship (such as navigation system, propulsion system and cargo control system).

Each of the above devices shall be marked with the following information:

a) Name;

b) Brand/manufacturer (supplier);

c) Model;

d) Embedded firmware version

e) Physical characteristics (if applicable);

f) Actual physical position (engine room and living place, etc);

g) Connected switches (for Ethernet switches, VLAN number shall be designated for each port);

h) Functional description.

(2) Software list

① The software list (including system software and application software) shall at least contain the following content:

a) Software name and publisher;

b) Installation date, version number and functional description;

c) Maintenance mode (local/remote);

d) Accounts type (generic/dedicated);

e) Access control list;

f) IP/Ports destination address (if unknown, information should be identified as "missing");

g) License number

② List of network services

a) IP-based services

- Protocol name and version;

- Listening port and motivation;

b) Non-IP-based services

- Listening interface and motivation

③ Integration files.

3.3.5.2. The list of assets shall be tracked throughout the service life of the ship and be updated in case of changes in hardware or software devices.

3.3.6. Network test

3.3.6.1. After installation of network cables and devices, tests shall be performed to verify expected performance he systems. Testing of the network system shall at least cover the following items:

(1) All wiring (cabling) and network devices constituting the system;

(2) All external and internal communications;

(3) Monitoring and alarm systems; (if applicable)

(4) Effectiveness of backup program;

(5) Cyber incident response mechanism (response and recovery capability of critical computer systems after failure);

(6) Local control capability of cyber incident;

(7) Network load;

(8) Network storm test;

(9) Redundancy testing (if applicable).

3.3.6.2. New devices and network system shall be tested in terms of performance, potential system impact and security access methods before they are installed onboard.

Section 4 Network boundary

3.4.1. Boundary defense

3.4.1.1. Boundary control

(1) The boundary security shall be defined according to classification of computer systems to protect areas containing computer-based systems.

(2) When connection among different network zones is allowed, the boundaries shall be controlled through proper boundary protection devices (such as agents, gateways, routers, firewalls, unidirectional gateways, protection and encrypted tunnels).

3.4.1.2. Communication interfaces between on board network and external network shall be controlled, and perimeter firewall shall be installed.

3.4.1.3. Internal firewalls shall be set up between each network segment.

3.4.1.4. Where the communication with a system that affects personal or ship safety is made through firewalls, then two different firewalls shall be provided, and both shall run in real-time manner

and be set to heartbeat mode.

3.4.1.5. When failure occurs to the boundary protection device, alarm shall be triggered.

3.4.1.6. Protection devices shall be installed between IT and OT to track and record the traffic, and limit traffic types, protocols and sources.

3.4.1.7. Any system, workstation, or device shall activate any built-in protection system by default.

3.4.1.8. Password access shall be enabled for every server, system, module, component, device or application. In special cases, password access may be disabled, which shall be approved by ISC.

3.4.1.9. No OT system or process control system can be directly connected to the internet.

3.4.2. Malicious code prevention

3.4.2.1. Anti-virus software shall be installed on each on-board computer-based system or any programmable device with a standard operating system. For PLCS or other –equipment without standard operating system, security measures shall be taken as recommended by the manufacturer.

3.4.2.2. Anti-virus software program shall –carry out update and security audit regularly.

3.4.2.3. A method of identifying the status of an anti-virus database shall be provided for each on-board computer.

3.4.2.4. Malicious code protection system shall at least contain the following configuration:

(1) Scan the system periodically at defined frequency;

(2) Scan in real-time manner while downloading, opening or executing files from external sources;

(3) Block and isolate malicious code, when the malicious code is detected, and trigger an alarm.

3.4.2.5. Attention shall be paid to mis-report arising from detection and disposal of malicious code and its potential impact on system availability.

3.4.2.6. The spam mail prevention mechanism shall be launched and updated timely according to strategies and procedures.

3.4.2.7. Before the authorized mobile computer system or mobile medium is connected to an OT system, it shall be scanned for the existence of malicious code.

3.4.2.8. It is required to scan malicious code and unauthorized software by the detection system regularly.

3.4.3. Intrusion prevention

3.4.3.1. It is necessary to detect, prevent or limit external or internal cyber-attacks at critical network nodes, and to trigger alarms when cyber-attacks and abnormal traffic are detected.

3.4.3.2. It is required to check ports and services of network systems and devices, stop useless daemons and processes, close unnecessary system services, default sharing and high-risk ports, such as Port 135, 137, 138, 139 and 445.

3.4.3.3. It is required to perform regular vulnerability scan and security audit to identify potential vulnerabilities and fix them timely after sufficient testing and evaluation.

3.4.3.4. Network system shall provide data validity verification function to ensure that the content input through human machine interfaces or the communication interfaces meets the system setting requirements.

3.4.3.5. Network terminal shall be restricted by setting the terminal access mode or network address range, and the access of unauthorized wireless access devices and mobile terminals shall be detected.

3.4.3.6. It is required to enable detection of cyber scanning, DDoS attacks, key cracking, man-in-the-middle attacks and spoofing attacks against wireless access devices.

3.4.3.7. Intrusion detection systems (IDS) and intrusion protection systems (IPS) may be deployed for the onboard network, which work to block abnormal traffic. IPS shall be able to send alarm to manned stations where an incident is detected that may impair security.

3.4.3.8. Mechanisms shall be in place to prevent or limit impact of Deny of Service (DoS).

3.4.3.9. The users shall turn off idle machines to prevent potential machine intrusions.

3.4.3.10. Servers, workstations, desktops, laptops or other mobile devices shall not allow unauthorized software to run automatically.

3.4.4. Monitor and alarm

3.4.4.1. Wireless network shall be monitored to prevent access of unauthorized point to the computer-based system or infrastructure.

3.4.4.2. It is necessary to monitor workstations, servers and mobile devices continuously and automatically, record monitoring incidents and alarm abnormal behaviors.

3.4.4.3. It is required to perform protective audit and filtering of VPN traffic and monitor the visited nodes.

3.4.4.4. Related equipment can be isolated from the network when monitoring anomalies or accidents affecting ship safety.

3.4.4.5. Cyber devices of Category-II and III systems shall be able to perform self-diagnosis to monitor the following states:

(1) Up-link of each port on the network device;

(2) Down-link of each port on the network device;

(3) Power-on or hardware reset;

(4) Network storm monitoring;

(5) Fan failure (only when the cyber device has a fan and is equipped with fan stop monitoring function);

(6) Abnormal temperature (only when the cyber device is equipped with abnormal temperature monitoring function).

3.4.4.6. The network monitoring device shall have the function of detecting abnormal state change, and inform the user of the following abnormal states:

(1) When the network device or network terminal disconnects the link or the power supply;

(2) When network devices or terminals that are not part of the network are connected;

(3) When network congestion reaches the threshold.

3.4.4.7. An alarm shall be triggered in case of any abnormality or failure, and all functions shall be maintained to ensure normal operation of the basic system in the integrated cyber.

3.4.4.8. It is required to record and check all remote login attempts, e time, date, duration, and source of each remote access incident, as well as failed remote access attempts.

3.4.4.9. It is required to monitor attack parameters of the network log analysis device, including but not limited to:

(1) Abnormal communication IP traffic on OT system boundary;

(2) IP traffic of malicious connection within the network;

(3) Detected malware and acts attacking network host;(4) User login time/place to detect evidence of being stolen or improper access;

(5) User account or user management behavior deviating from normal behavior.

3.4.4.10. For the automatic alarm response system, the triggered alarms shall be captured, recorded, managed by virtue of the automatic security response protocol, and be reported to authorized personnel for further review.

3.4.4.11. When an intrusion attempt against the OT system is detected, it is required to perform the following actions:

(1) Record and report all OT system security incidents by incident, severity, and type;

(2) Record and report accident recovery measures and post-accident remedial effect (if any);

(3) Record and check all access attempts;

(4) Aggregate and correlate incident data detected by multiple sources and sensors within practical scope to fully describe the incident.

(5) Provide all incident data to the incident response team for incident control and summary of lessons and experience;

(6) Assess the impact on security, environment, production, lost time and cost (actual or expected).

3.4.5. Access control

3.4.5.1. Users (personnel, software and devices) and accounts in the cyber system shall be identified, and identification management measures shall be formulated, for example, it is forbidden to use public symbols for identification.

3.4.5.2. Such measures as filtering mechanism, access control list, complex password and/or multi-factor authentication and out-of-band communication shall be taken to protect sensitive resources and assets from unauthorized access.

3.4.5.3. User management

(1) Users who log in the network system shall be assigned with accounts and privileges.

(2) Default accounts shall be re-named or deleted, and their default passwords shall be changed.

(3) No redundant user accounts shall be issued.

(4) Accounts shall be managed and reviewed periodically. And expired accounts shall be deleted or disabled timely.

(5) It is required to monitor all accounts that access the network system; remove unnecessary users and administrator accounts where service periods of accounts are defined; disable expired accounts and those unrelated to any business; lock accounts that are logged out in time-out manner, and that are failed to log out after several attempts.

(6) It is required to grant each user a unique account to enable the user to take responsibility for his/her actions; avoid shared accounts except that such share account is for business or operation need, which shall be approved and recorded.

3.4.5.4. Password management

(1) Make strict password management, timely change the preset password made during system installation, and eliminate weak and empty passwords;

(2) Before providing new, alternative or temporary access authentication information, a program should be established to validate the identity of the users;

(3) Temporary access authentication information should be provided to users in a secure manner, avoiding the employment of external parties or unprotected (clear text) e-mails. Temporary access to

authentication information should be exclusive to individuals and should not be guessable;

(4) After the system or software is installed, the default access certification information for suppliers should be modified;

(5) Appropriate authentication technology should be employed to verify the declared user's identity. If strong authentication is required, a combination of authentication methods such as password, smart card, token device or biometric identification should be used;

(6) The login program should be designed to minimize the opportunity of unauthorized access. Therefore, the login program should disclose the information about the system or applications to a minimum extent to avoid providing any unnecessary assistance to unauthorized users.

3.4.5.5. Password-based authentication shall meet the following:

(1) Enforce the complexity of password by case sensitive number of characters, mix of upper and lower case letters, digits and special characters;

(2) When creating a new password, at least enforce to change the number of characters;

(3) The storage and transmission of password should be encrypted;

(4) The password should be changed regularly;

(5) The password is prohibited from reusing for several generations;

(6) A temporary password is permitted for system login but should be changed to a permanent password immediately.

3.4.5.6. Authority management

(1) Confer corresponding authority to identified persons, organizations, roles and devices in the network;

(2) Cyber access restrictions should be exercised for specific task needs and privileged accounts of special systems;

(3) Establish and implement system user authorization management;

(4) The minimum authority required for administrative users should be conferred to achieve separation of authorities for administrative users.

3.4.5.7. Third-party access

(1) Authorized third parties (equipment supplier, system developer, system maintainer, etc., the same below) shall be audited for access to the network system. Audit the access authority of third parties on a regular basis to confirm that they are within the controllable range;

(2) Third-party access requires multi-factor authentication or strong password. A third party's behavior log in the network system should be recordable and savable;

(3) Minimum access authority shall be conferred and an authorized storage medium shall be used for access of a third party to the network system (if necessary). If not necessary, third parties are not authorized to collect and store data.

3.4.5.8. Access rules

(1) An access control policy shall be configured, which specifies the rules for the user's access to the network, including the methods of access to network and network services (for example, use of a VPN or wireless network);

(2) Access control rules shall be laid between network boundaries or zones according to the access control policy. By default, controlled interfaces deny all communications except for those permitted;

① Access control mechanisms should be deployed and access control rules should be laid at the virtualized network boundaries;

② Access control mechanisms should be deployed and access control rules should be laid at different grades of network boundary;

(3) Redundant and invalid access rules should be deleted, the access control list should be optimized, and the number of access control rules should be ensured to a minimum extent;

(4) The source address, destination address, source port, destination port and protocol should be checked to allow or deny data packages to import and export;

(5) It should be ensured that the access control policy migrates with the virtual machine;

(6) Cloud service clients should be permitted to lay access control policy between different virtual machines;

(7) Wireless access device should enable access authentication function and forbid WEP authentication. If a password is used, it would not be less than 8 characters;

(8) An access control device should be deployed between the OT system and other systems, which is configured with access control policy and forbids any universal network services such as E-Mail, Web, Telnet, Rlogin and FTP that cross the region boundaries;

(9) An alarm signal should be given when the boundary protection mechanism of the OT system fails;

(10) Continuous invalid login attempts are limited. When the maximum unsuccessful attempts are exceeded, engage one of the following automatic executes:

① Lock account/node for a while;

② Lock account/node until the administrator releases it;

③ Delay the next login prompt according to the delay algorithm.

3.4.5.9. Before installing into a network environment, delete all the default settings that were originally configured on client systems, devices, applications and assets, including:

(1) Modifying the supplier's default password;

(2) Conferring no account administration authority to common users by default;

(3) Endpoints can only perform horizontal network access or be visible thereto within their function needs, rather than default to other systems or assets on the network;

(4) Configuring single sign-on (SSO) for applications as needed;

(5) Pre-configured software using OEM or manufacturer call-out methods will be disabled in the standard user profiles to prevent unauthorized communication.

3.4.6. Remote operation and maintenance

3.4.6.1. The license for remote operation and maintenance should be limited.

3.4.6.2. Cyber system should be able to restrain remote maintenance when running normally.

3.4.6.3. For remote maintenance, the following requirements should be met:

(1) The network connections of remote operation and maintenance shall be controlled, and the remote external access points of such connections shall be protected to prevent unauthorized access;

(2) Authentication should be performed at the start of a session. Password shall not be transmitted in unencrypted form. If the system cannot provide encryption, an encrypted virtual private network (VPN) should be employed for communication;

(3) The lockup period activation function in the event of failed access attempts should be provided;

(4) The remote operation and maintenance should be able to be cancelled locally at any time;

(5) If the remote maintenance connection is interrupted for some reason, access to the system should be able to be terminated automatically;

(6) Remote operation and maintenance logs shall be performed. The logs shall include start time, end time, operator, etc.

3.4.6.4. The OT system should also have the necessary capabilities to mitigate the risks of remote operation and maintenance, as follows:

(1) Capability to terminate connection and immediately restore to an undamaged state;

(2) Capability not to affect the integrity and availability of the system in the event of an abnormal interruption.

Section 5 Compute environment

3.5.1. Authentication

3.5.1.1. Authenticate the users (persons, software, devices) and accounts in the network system, and implement multi-factor authentication for network access and dynamic address allocation and other authentication methods for access devices.

3.5.1.2. It is recommended to authenticate users by means of two or more combinations of authentication technologies such as password, cryptology and biotechnology, and at least one of these authentication technologies should be implemented using cryptology.

3.5.2. Data security

3.5.2.1. Risk analysis of data shall be conducted to assess the value of data security and its potential impact on system performance.

3.5.2.2. Data encryption

(1) Effective measures shall be taken to the data stored, transmitted and processed in the system to ensure its availability, confidentiality and integrity;

(2) It is prohibited transmitting command and control signals of the OT system in non-dedicated channels or network zones;

(3) In case of third-party usage data, corresponding data using requirements and control rules shall be formulated;

(4) In case that services or data provided by a third party are used, service safety and data security shall be guaranteed;

(5) When employing an insecure network for communication, the communication path and the data of critical systems or functions shall be encrypted;

(6) Manage the company and personnel privacy data, and observe the national or local laws and regulations;

(7) Strictly control the access to and distribution of privacy data;

(8) The privacy data of crew and shipowner/ship management company shall be stored separately from other data;

(9) Data legitimacy (data quality)

3.5.2.3. Reduce attacks on critical processes and data by separating them from non-critical data and processes. The system should also have decoupling capability to prevent chain reactions caused by a single cyber incident.

3.5.2.4. Data storage

(1) The power supply of the data storage device shall be stable;

(2) The data storage device shall be capable of preventing electromagnetic interference;

(3) The data storage device shall be suitable for the intended use and be applicable for the maritime environment as specified in UR E10;

(4) Data loss prevention (DLP) software shall be employed to prevent "leakage" of important data;

(5) If the data used for Category-II or Category-III systems is stored on a hard drive, it shall be stored on multiple hard drives to protect the data in the event of a drive failure, for example, RAID storage or equivalent devices. Backup compatible drives shall be available on board.

3.5.2.5. As part of cyber risk management, the shipowner shall also provide a training relating to data security for those who are authorized to interact with the ship's cyber system.

3.5.2.6. Prevent unauthorized and unexpected information transmission by means of sharing system resources.

3.5.2.7. Provide logging capabilities for data access to sensitive data storage, asset type or data location.

3.5.2.8. Provide secure data destruction methods for data processing.

3.5.3. Software installation and update

3.5.3.1. Software installation and change

(1) The historical versions of the software shall be retained, in conjunction with all required information and parameters, procedures, configuration details and supporting software, as emergency restoration measures;

(2) Establish and implement user's management rules for software installation;

(3) Follow the principle of minimal installation and install only the required components and applications;

(4) Determine the rollback policies before updating. In case of damage, the system should be able to simply restore to the earlier version;

(5) Upon a successful update, relevant information log shall be formed, including time, version and operator.

3.5.3.2. Software update verification

(1) Ensure the integrity and authenticity of update, such as encryption or cyclical redundancy check (CRC);

(2) Scan for malicious codes before updating;

(3) Verify that the system is running properly after the update.

3.5.4. Emergency response

3.5.4.1. In general, the following procedures shall be considered:

(1) Detect cyber incidents and identify faulty systems;

(2) Determine effective solutions and take appropriate actions;

(3) Restore the failure systems;

(4) Investigate and record the cyber incidents;

(5) Assess the validity of emergency procedures and update events as well as emergency management procedures and emergency plans.

3.5.4.2. The software/hardware tools necessary for implementation of emergency responses

shall be prepared.

3.5.5. Backup

3.5.5.1. The backed-up data is at least single redundant, and limited access authority shall be maintained.

3.5.5.2. If the backup data is stored on a hard drive, backup compatible drives (e.g. RAID storage or equivalent devices) shall be furnished to protect the data in the event of a drive failure.

Section 6 Security audit

3.6.1. Configuration

3.6.1.1. Select security configuration according to the application of device. When the network configuration changes, the basic configuration information list in the assets list shall be updated in a timely manner.

3.6.1.2. For the purpose of firewall, at least the following configurations shall be enabled:

(1) Security strategies (rules) shall be provided on each firewall, and settings shall be made to merely allow transmission of basic or important data among switches;

(2) Firewall rules shall be designed to meet the data traffic necessary for the intended operation of the network;

(3) Set a SUPER password and store it encrypted;

(4) Configure password protection for CONSOLE port;

(5) Assign accounts by user to avoid account sharing;

(6) Enable the traffic monitoring log function;

(7) Enable the routing protocol authentication encryption function;

(8) Formulate routing policies and forbid the distribution or receipt of insecure routing information;

(9) Configure the common vulnerability attack and virus texts in ACL filtering;

(10) Shut down the AUX port;

(11) Attack prevention configuration;

(12) Disable unnecessary network services;

(13) The last entry in the access rules list is all traffic denied.

3.6.1.3. For the purpose of router and protocol, at least the following configurations shall be enabled:

(1) A router should be installed between different cyber segments;

(2) Each segment shall have its own IP address range;

(3) Data transmitted through Category-II & Category-III systems shall be encrypted.

3.6.1.4. For the purpose of switch, at least the following configurations shall be enabled:

(1) If it is applied to network segregation and segmentation, a three-layer switch shall be adopted;

(2) Password encryption shall be enabled for the switch;

(3) Configure password protection for CONSOLE port;

(4) Avoid account sharing;

(5) Enable the account locking policy;

(6) Shield unnecessary protocols on user port;

(7) Enable the known typical attack protection;

(8) Enable the traffic control;

(9) Disable unnecessary services;

(10) Check if there's basic safety protection;

(11) Enable the spanning tree protocol.

3.6.2. Security audit (log)

3.6.2.1. Perform log management and allocate storage space as needed to maintain sufficient log time to support the attack defense cycle. Some organizations can be retained for at least 12 months.

3.6.2.2. The important user behaviors and security incidents shall be audited at network boundaries and important network nodes. The audit record shall include the following:

(1) Users (remote access users, Internet access users, etc.);

(2) The date and time of the events;

(3) Event type (abnormalities, failures);

(4) Event successful or not (connection (success/fail), authentication (success/fail)), including those generated by the following devices:

① Any wireless access point (WAP);

② Any wireless local area network (WLAN);

③ Any local area network (LAN);

④ Any firewall;

⑤ Any applications firewall;

⑥ Any stateful packet inspection (SPI);

⑦ Any intrusion prevention system (IPS);

⑧ Any device used to identify and authenticate network access;

⑨ Any device used to implement or ensure cyber security.

3.6.2.3. The audit records shall be analyzed through the audit administrator and be processed according to the analysis results, including the storage, management and query of audit records in accordance with the security audit policies.

3.6.2.4. It shall be possible to conduct behavior auditing and data analysis separately for user behaviors on remote access and those on Internet access.

3.6.2.5. The audit administrator shall be authenticated, and is allowed only to perform security audit operations with specific commands or operation interfaces, and these operations shall be audited. The activities of the audit administrator and operator should be logged, and these logs should be protected and regularly reviewed.

3.6.2.6. The audit records should be protected and regularly backed up to prevent tampering and unauthorized access.

3.6.2.7. The audit process shall be protected from unauthorized interruptions.

3.6.2.8. Immediately after the audit is completed, the access authority and the technical means employed by the auditor, including the remaining devices and testing tools, shall be deleted.

Chapter 4 Product Assessment

Section 1 General provisions

4.1.1. General requirements

4.1.1.1. The IS Class (ISC) specifications and/or guidelines propose that cyber security assessment of a product, if required, shall be carried out in accordance with the requirements of this Chapter.

4.1.1.2. Cyber system refers to the entry defined in Chapter 1, Section 3 herein.

4.1.1.3. Network device refers to the physical entity connected to a network. Basic network devices include: computer, server, hub, switch, bridge, router, gateway, network interface card (NIC), wireless access point (WAP), printer, modem, etc.

4.1.1.4. Technical assessment refers to the work related to the cyber security assessment of ship's cyber system products in accordance with the relevant requirements herein.

4.1.2. Assessment process

4.1.2.1. Product assessment covers drawing review, technical assessment and field test.

4.1.2.2. Drawing review: The drawings and documents required in Clause 4.2.1 shall be reviewed in accordance with the relevant requirements in Clause 4.1.3 of this Chapter.

4.1.2.3. Technical assessment: A technical assessment shall be carried out in accordance with the requirements in Clause 4.1.3 of this Chapter and Appendix 4.

4.1.2.4. Field test: ISC shall perform necessary tests on the cyber system based on the drawing review and technical assessment and in accordance with the test methods described in Clause 4.2.2 of this Chapter.

4.1.2.5. After the drawing review, technical assessment and field test are all qualified, ISC shall sign Appendix 6 - Ship's Cyber Security Assessment Report (Product).

4.1.3. Basic technical requirements

4.1.3.1. The technical assessment of ship cyber system (product) shall meet all the requirements in Table 4.1.3.1.

Table 4.1.3.1 Technical Requirements of Ship Cyber System (Product)

Category	Clauses	Remarks
Network architecture	Cyber redundancy	The relevant terms of Chapter 3 shall be met.
	Communication security	The relevant terms of Chapter 3 shall be met.
	Wireless network	The relevant terms of Chapter 3 shall be met.
Network boundary	Boundary protection	The relevant terms of Chapter 3 shall be met.
	Access control	The relevant terms of Chapter 3 shall be met.
	Remote operation and maintenance	The relevant terms of Chapter 3 shall be met.
Computing environment	Identity authentication	The relevant terms of Chapter 3 shall be met.
	Data security	The relevant terms of Chapter 3 shall be met.
	Backup	The relevant terms of Chapter 3 shall be met.

4.1.3.2. In addition to meeting the requirements of Table 4.1.3.1, the technical assessment of ship cyber system (product) shall meet other relevant requirements in Chapter 3 hereof according to the actual condition.

Section 2 Drawings & documents and test items

4.2.1. Drawings & documents

4.2.1.1. The cyber system applying for technical assessment shall provide relevant data in accordance with the requirements of Table 2.1.6.3 in Chapter 2, Part 7 of the *Rules for Classification of Sea-going Steel Ships*.

4.2.1.2. In addition to those required in Clause 4.2.1.1, the following drawings and documents are to be submitted to ISC for approval:

(1) System Specification (Product Technical Specifications), specifying the overall performance requirements and overall design requirements of the product, including at least the applicable parts of the following:

① Requirements for environmental conditions of the product: The requirements for working conditions (including electromagnetic compatibility) stipulated in the *Rules for Classification of Sea-going Steel Ships* shall be met;

② Detailed description of product functions: including system configuration, scope of application of the product, detailed description of implementable control and monitoring functions of the product and implementation methods, detailed description of the security status of each function implemented, features of the system under various operating conditions (including emergency and fault conditions) and the instructions under normal and abnormal conditions;

③ Detailed description of redundant settings and conversion mechanism;

④ Detailed description of fault monitoring and identification functions (Auto and Manual);

⑤ Detailed description of data security and user security level (function access restriction);

⑥ List of control and monitoring items: List of all I/O signals of the system (service description, instrumentation, system, signal type, range and limited setting range);

(2) Hardware Specification, including at least the applicable parts of the following:

① List of technical specifications of hardware and external devices;

② System chart: The connections among all major components (software and hardware units, modules) of the system and the interfaces with other systems are described;

③ Detailed description of main hardware configuration of the product;

④ Details of I/O device;

⑤ Details of power supply unit;

⑥ Specification of network transmission medium and maximum data transmission traffic;

⑦ Main communication protocol standard adopted by the network transmission medium;

⑧ Basic parameters of access network device, such as transmission port, subnet mask, gateway address, accepted communication protocol, etc.;

⑨ Specification of storage medium.

(3) Software Specification, including at least the applicable parts of the following:

① List of software installed on the system and version numbers;

② Description of basic software installed in each hardware unit;

③ Description of communication software installed in the network node;

④ Description of application software: maintain the information of the system modules that must operate for the functions and the information of its dependence on other systems, maintain the relations between the software modules that must operate for each function, and the data flow and control flow between software modules;

⑤ Software configuration, including priority scheme;

⑥ Switching mechanism between redundant systems;

(4) User Interface Manual, including at least the applicable parts of the following:

① Description of the function allocation of each work station and operation station and the control conversion between the stations;

② Description of functions assigned to each input device;

③ I/O devices layout, dimensions and necessary physical pictures;

④ User input interfaces description and menu description;

(5) Topology of the Cyber System, including at least the following information about the cyber system:

① Network topology, which can clearly show the connections and access relations of network transmission medium with the access systems and devices;

② Layout of router, and the network zones connected thereto;

③ Layout and access modes of system firewall, and the zoned security protection area;

④ Layout and access modes of on-board work stations and servers;

⑤ Systems and devices accessed to the network, such as the communication navigation system, cabin status monitoring system and display control unit connected via a router or directly accessed to the network;

⑥ Layout and access modes of intrusion detection and intrusion prevention system (where applicable);

⑦ The power supply modes of inside and outside of the system and the units.

(6) Configuration System Files, including at least the following:

① List of devices and systems accessed to the network, including the basic information of version numbers, installation and maintenance dates and the identification names in the

cyber system;

② Network data traffic limit;

③ Open ports in the devices after the system is put into operation;

④ Users permitted to access the network and the conferred authorities;

⑤ The system's settings of restricted access addresses, such as the system white list;

⑥ Remote user access authority (where applicable);

⑦ Locations where configuration files are stored and backed up;

⑧ Necessary measures taken to protect system configuration files from malicious reading or tampering.

(7) System Operation and Test Procedures, including at least the following:

① Test items;

② Test methods;

③ Result evaluation criteria;

④ Reference standards.

4.2.1.3. In addition to those required in Clause 4.2.1.1, the following drawings and documents are to be submitted to ISC for future reference:

(1) Cyber System Hardware Installation Instructions, including at least the following:

① Installation locations and methods of router, firewall, work stations, servers, etc.;

② Necessary measures taken to protect hardware devices from physical damages (where applicable);

③ Requirements of devices installed in special areas for environmental conditions (temperature, pressure);

(2) Operation Manual (incl. Troubleshooting Instructions)

① It shall at least include system start-up, functions recovery, maintenance and routine test, data security and data backup, user authority limits, software re-installation and system recovery, fault location and shooting, system update and other matters that users need to pay attention to;

② Software maintenance and instructions (incl. necessary procedures for software and hardware alteration management);

(3) Software verification evidences

① Verification evidence of software modules in line with software programming standards (detection and correction of software errors);

② Test evidence of programmable device functions for software modules, subsystems and

system levels.

4.2.2. Test methods

4.2.2.1. Assessment of the cyber system, which shall generally be carried out taking into account the following technical means:

(1) Security vulnerability scanning;

(2) Penetration test;

(3) Stress test;

(4) Load test;

(5) Network storm test;

(6) Network connection test.

4.2.2.2. At least, security vulnerability scanning, load test and network connection test shall be performed for cyber system testing.

4.2.2.1. Devices used for Category-II and III systems shall be tested in accordance with IACS UR E22 and E10.

4.2.2.2. The relevant test items can be carried out by means of hardware and software testing; it is also possible to confirm that relevant devices have the corresponding protective capabilities by verifying configuration files; or they can be carried out by verifying the test results and reports.

4.2.2.3. Security vulnerability scanning

(1) The testing party, using technical means, conducts comprehensive detection and vulnerability scanning on the cyber system product, locates vulnerabilities and analyzes the causes, and takes the result as one of the conclusions of technical assessment;

(2) After the vulnerability scanning is completed, the applicant shall provide a test report to ISC for verification.

4.2.2.4. Penetration test

(1) The testing party, using technical means, conducts a comprehensive penetration test on the cyber system product, and takes the result as one of the conclusions of the technical assessment;

(2) Through the penetration test environment established by the testing party, perform a comprehensive review of the cyber security strategies under test, and actively analyze the network's vulnerability and technical defects from the possible locations of security attacks;

(3) The penetration test helps the applicant understand the current security status by identifying security issues and facilitates the reduction of threats and risks through relevant operation planning;

(4) The penetration test object is the cyber system product to be connected to the ship's cyber. The test is performed by groups as follows:

① System and application function penetration;

② Database system penetration;

③ Network devices penetration.

(5) After the penetration test is completed, the applicant shall provide a test report to ISC for verification.

4.2.2.5. Stress test

(1) The testing party, using technical means, performs a stress test on the cyber system product, and takes the result as one of the conclusions of technical assessment;

(2) Stress test is also called strength test, which is to run the testing software in a long-period or extra-large-load manner to test the performance, reliability and stability of the system under test by simulating the practical software and hardware environment and the system load in the user's using process. A system bottleneck or non-receivable performance point shall be determined for the stress test to obtain the maximum service level available in the system;

(3) After the stress test is completed, the applicant shall provide a test report to ISC for verification.

4.2.2.6. Load test

(1) The testing party, using technical means, performs a load test on the cyber system product, and takes the result as one of the conclusions of technical assessment;

(2) Load test is also called "volume test" or "endurance test/persistence test", whose objective is to determine and ensure that the system can still run normally beyond the maximum expected workload. Load test is to discover design errors or verify the load capacity of the system by testing the performance of the system under resource overload. In this test, the test object will be subjected to different workloads to evaluate and assess the performance behavior of the test object under different workloads and the capability of continuous normal operation;

(3) After the load test is completed, the applicant shall provide a test report to ISC for verification.

4.2.2.7. Network storm test

(1) The testing party, using technical means, performs a network storm test on the cyber system product, and takes the result as one of the conclusions of technical assessment;

(2) Network storm refers to a large number of replicates of broadcasting in the network segment and propagation of data frames due to network topology design and connection or other reasons, resulting in a network performance degradation and even network paralysis. The occurrence of network storm is usually caused by improper configuration of network device, network card failure, network loop setting error, network virus and malicious attack;

(3) After the network storm test is completed, the applicant shall provide a test report to ISC for verification.

4.2.2.8. Network connection test

(1) The purpose of network connection test is to verify the operability and functionality of network device connection;

(2) Cyber monitoring device and monitoring function shall operate properly in the cyber system, specifically as follows:

① Function of showing physical architecture diagram;

② Alarm function;

③ Journal function;

④ Traffic indication;

⑤ Configuration setting function;

⑥ Fault recovery supporting function;

(3) After the test is completed, the applicant shall provide a test report to ISC for verification.

Chapter 5 Surveys during construction

Section 1 General provisions

5.1.1. General requirements

5.1.1.1. This chapter applies to ships proposed to obtain a Cyber Security (P, S) class notation.

5.1.1.2. The survey requirements specified in this Chapter are supplement to those applicable to all ship surveys. The survey may be carried out simultaneously with the same types of surveys, namely, annual, intermediate and special surveys, as specified in Section 2, Chapter 5 of Part 1 of the *Rules for Classification of Sea-Going Steel Ships*, at a survey interval of the same thereof.

5.1.2. Plans and documents

5.1.2.1. Ships applying for Cyber Security (P) class notation shall submit the following drawings and documents for approval:

(1) Ship's cyber security planning instructions (at submission of the design for approval);

(2) Cyber security construction management document (before construction of the cyber system);

(3) Cyber security operation and maintenance management document (before ship's sea trial/before operation of the cyber system);

(4) Assets list, including those required in 3.3.5.1 of Chapter 3;

(5) Cyber system architecture instructions;

(6) Design schemes of the functional systems in the network;

(7) Cyber security risk assessment report at design stage (at submission of the design for approval);

(8) Cyber security risk assessment report at operation and maintenance stage (before ship's sea trial/before operation of the cyber system);

(9) communication traffic estimation specification.

5.1.2.2. Ships applying for Cyber Security (P) class notation shall, based on the drawings and documents of ships for application of Class-P Cyber Security class notation, additionally submit the following drawings and documents for approval:

(1) Detailed instructions for cyber security technical measures;

(2) Cyber monitoring plan.

5.1.2.3. Cyber security planning instructions should include but not limited to the following:

(1) Class notation proposed to apply;

(2) Cyber security demands, goals, scope, principles, functional description, etc.;

(3) Cyber security technology planning (technical design thought and brief description to achieve security objectives);

(4) Cyber security management planning (brief description of management organs and posts allocated and management system established to achieve security objectives).

5.1.2.4. Cyber security management documents should include but not limited to the following:

(1) Management manual (containing security objectives, guidelines, scope, organization, management activity operation framework, security strategies, etc.);

(2) Documents and records control;

(3) Personnel management;

(4) Risk management (containing risk identification, risk analysis, risk disposal, etc.);

(5) Security inspection, auditing and management review;

(6) Non-conformity correction and prevention management;

(7) Change management;

(8) Security incidents, emergency, backup and recovery management;

(9) Service provider management;

(10) Password management;

(11) Construction management (where applicable), including project implementation, procurement, development, test and acceptance, system delivery, etc.;

(12) Operation and maintenance management (where applicable), including environmental management, asset management, medium management, device maintenance management, cyber and system security management, malicious codes prevention management, configuration management, etc.

(13) Risk assessment report (if any).

5.1.2.5. Cyber system architecture instructions should include at least the following:

(1) Network topology clearly showing the connections and access relations between the network transmission medium and the access systems and devices, including the connection to external network and the physical locations of key devices;

(2) Type of transmission medium (such as twisted pair, coaxial cable, optical fiber, etc.);

(3) Layout of router, and the network zones connected thereto;

(4) Layout of switches and the network zones connected thereto;

(5) External connections;

(6) Layout and access mode of firewall;

(7) Layout and access modes of on-board work stations and servers;

(8) Systems and devices accessed to network;

(9) Layout and access modes of intrusion detection and intrusion prevention system (where applicable);

(10) Network isolation (e.g. VLAN partitioning);

(11) IP addresses assignment list should include at least the following:

① List of relevant switches;

② Functional description of IP scope;

③ Interlink to other scopes;

(12) Non-IP networks list (where applicable) should include:

① List of MAC addresses or list of specific addresses of industrial protocols on the network; list of relevant switches;

② Functional description of networks;

③ Devices connected to other networks (connectors);

(13) Non-ethernet access point should include:

① List of access ports;

② Special protocol (if any);

③ List of connected devices;

(14) List of logic servers and desktops should include:

① IP address (network, mask, gateway);

② Operating system version;

③ Underlying physical server;

④ Applications and their versions;

⑤ Services and versions.

5.1.2.6. Detailed instructions for cyber security technical measures should include but not limited to:

(1) Region boundaries (intrusion prevention, password policy, monitoring and alarm, etc.);

(2) Data security strategies (data encryption, data storage);

(3) Logs auditing policies.

5.1.2.7. Design schemes of the functional systems in the network should include at least: system goals, system architecture, system composition, system's main functions, key technical indicators, technical parameters, system interfaces, backup plans and others.

5.1.2.8. Risk assessment report consists of design stage and operation and maintenance stage. At design stage, it is to mainly analyze and assess the compliance of the design schemes and cyber security planning (objectives, demands, etc.) with relevant standards in order to perfect the design schemes and take it as the basis for risk control in the cyber system construction process. At operation and maintenance stage, it is to mainly understand and analyze the security risks in the operation of cyber system in order to perfect the management mechanism and technical measures for the operation and maintenance of the cyber system, which can be referred to Appendix 1.

5.1.2.9. Cyber monitoring plan refers to a plan developed for monitoring network service, equipment failure, network traffic, network abnormality alarm and others.

Section 2 Initial survey

5.2.1. General requirements

5.2.1.1. In the initial survey, for ships proposing to apply for a Cyber Security class notation, the ship surveyor shall survey in accordance with the approved drawings and documents (including plan approval comments), confirm the implementation of measures taken by the shipyard, and report to the plan approval department in a timely manner the shipyard's different comments on implementation of plan approval and its comments.

5.2.2. Survey process

5.2.2.1. The main survey process of the ship's cyber system is:

(1) Pre-assessment: Make a risk analysis for the ship's network with reference to *Appendix 2 - Ship's Cyber Security Pre-assessment Form*, to grasp the overall situation of the ship's cyber system;

(2) Detailed assessment: Make a classified security assessment of the ship's cyber system

according to the requirements of the cyber system;

(3) After the completion of pre-assessment and detailed assessment, ISC will issue assessment reports to the applicant and grant a ship's class notation.

5.2.2.2. Pre-assessment

(1) As the initial work of cyber security assessment activities, pre-assessment shall be completed by the shipowner/ship management company;

(2) The pre-assessment aims to quickly understand the security status of the ship's cyber and provide a basis for the formulation of subsequent assessment items.

(3) At pre-assessment stage, the ship's cyber is basically grasped from the following aspects:

① Understand if ISPS Code is effectively applied on the shipowner/management company and ships;

② Grasp the main supervisory programs and technical means applied to ships to prevent network threats;

③ Master the key devices and systems vulnerable to cyber-attack;

④ Master the operation process of the devices and systems vulnerable to cyber-attack;

⑤ Grasp the major measures to be taken on board to deal with incidents and mitigate the hazards caused thereby when a cyber security incident takes place;

⑥ Understand the primary users of the ship's cyber system and the risk points they may face during operation;

⑦ Understand the technical support of equipment manufacturers on the maintenance and upgrade of the ship's cyber and its devices;

(4) The pre-assessment shall be carried out in accordance with Appendix 2 - *Ship's Cyber Security Pre-assessment Form*.

5.2.2.3. Drawings review

(1) To review the relevant drawings required in Clause 5.1.2 of this Chapter;

(2) To review according to the relevant requirements of Chapter 2 & 3 herein.

5.2.2.4. Detailed assessment

(1) Detailed assessment is carried out by means of comprehensively analyzing the assessment indicators in the ship's cyber, identifying the security risks existed in the ship's cyber, and analyzing the ship's capability to deal with cyber risks;

(2) ISC carries out a detailed assessment of the ship's cyber system that has been subjected to pre-assessment and reached the baseline score;

(3) ISC carries out assessment from both management and technical aspects;

(4) The steps of detailed assessment are as follows:

① The shipowner/ship management company file an application;

② ISC assesses the ship systems/devices included in the detailed assessment form based on the operation of the cyber system on the ship in accordance with Appendix 3 - Ship's Cyber System/Equipment Assessment Form;

③ ISC verifies according to the requirements of Appendix 5 - Detailed Ship's Cyber Security

Assessment Form, and determines whether or not to conduct a field ship assessment depending on the ship's condition;

④ If the requirements are met, ISC will issue an assessment report (see Appendix 7 - Ship's Cyber Security Assessment Report (Ships) for details).

5.2.2.5. Class notation

(1) After the assessment is completed, ISC will grant the appropriate class of class notation to the ship;

5.2.3. Survey and test items

5.2.3.1. When the cyber system is under construction/reconstruction, check the ship's cyber security construction management documents, confirm the integrity of the construction management system, and verify if they are the latest valid documents.

5.2.3.2. During the construction/reconstruction of the ship's cyber system, check the ship's cyber security management organ and staff information as well as management records (including reports, logs, record forms, etc.), and confirm that security management activities meet the requirements of the management system operation and security strategies.

5.2.3.3. Witness important engineering nodes, such as ship cyber integration test, cyber security test, on-board installation, sea trial test, acceptance and delivery.

5.2.3.4. Before the formal operation of the ship's cyber system, check the ship's cyber security operation and maintenance management documents, confirm the integrity of the operation and maintenance management system, and verify if they are the latest valid documents.

5.2.3.5. Check that the arrangement, installation and craftsmanship of network devices, such as servers, work stations, firewalls and cables, comply with approved drawings, diagrams, instructions, calculation sheets and other technical documents.

5.2.3.6. Verify the consistency of assets list with the physical ship.

5.2.3.7. Verify the configuration of network devices such as firewalls and switches according to the configuration requirements stipulated in 3.6.1 of Chapter 3.

5.2.3.8. Test the cyber system according to the requirements stipulated in 3.3.6 of Chapter 3.

5.2.3.9. Verify the ship's cyber security management documents to confirm if they have been formally released.

5.2.3.10. Verify the assessment of the ship's cyber system (products) when a cyber security assessment of the ship's cyber system product is required.

5.2.3.11. Submit the cyber system's mooring test schedule and sea trial schedule for review of the field ship surveyor.

5.2.3.12. Determine whether to conduct on-site technical verification as appropriate.

5.2.3.13. Verify the compliance with relevant requirements in Appendix 5.

Section 3 Surveys after construction

5.3.1. Annual surveys

5.3.1.1. Annual surveys

5.3.1.2. Prior to the annual surveys of the ship's classification, an annual report on the operation of the ship's cyber system shall be submitted to the ISC's executive survey unit. The report shall include at least the following since the last annual survey:

(1) The overall operation of the cyber system;

(2) The maintenance record of the cyber system;

(3) Fault/failure of access systems/devices in the cyber system and the cause analysis;

(4) Record of the seamen's cyber security training.

5.3.1.3. During the annual surveys, ISC shall check the following on board:

(1) Confirm that the ship's cyber security operation and maintenance management documents are available on board at any time and are the latest valid documents;

(2) Verify the *Ship's Cyber Security Assessment Report (Ships)*;

(3) Check the ship's cyber security operation and maintenance management organ and staff information as well as management records (including reports, logs, record forms, etc.), and confirm that security management activities meet the requirements of the management system.

(4) Ship cyber operation logs, to confirm that the operation is in good condition;

(5) Changes in assessment indicators of ship's cyber security;

(6) Since the last survey, if the topology of approved ship cyber has changed, in general, the shipowner/ship management company shall apply to ISC for an occasional survey of the ship's cyber security to confirm that the ship cyber meets the requirements herein.

5.3.1.4. If the survey results of the ship's cyber security fail to meet the requirements herein, ISC will suggest the rectification within a time limit or withdraw the ship's Cyber Security class notation.

5.3.1.5. If the ship's cyber security rectification is not completed within the time limit, ISC will withdraw the ship's Cyber Security class notation.

5.3.2. Occasional surveys

5.3.2.1. When the ship's cyber structure or system undergoes major changes, in general, the shipowner/ship management company shall apply to ISC for an occasional survey of ship's cyber security to confirm that the ship cyber meets the requirements herein.

5.3.2.2. During occasional surveys, ISC shall check the following:

(1) The ship's cyber security management documents and related data to confirm that the security management meets the requirements of the management system;

(2) The arrangement, installation and craftsmanship of network devices involved in the changes, such as servers, work stations, firewalls and cables, shall comply with approved drawings, diagrams, instructions, calculation sheets and other technical documents.

(3) Changes in assets list;

(4) The configuration of network devices such as firewalls and switches according to the configuration requirements stipulated in 3.6.1 of Chapter 3 in case that the changes involve backbone network adjustment;

(5) When necessary, the cyber system shall be tested in accordance with the requirements of 3.3.6 of Chapter 3;

(6) Determine whether to conduct on-site technical verification as appropriate.

5.3.2.3. If the survey results of the ship's cyber security fail to meet the requirements herein, ISC will suggest the rectification within a time limit or withdraw the ship's Cyber Security class notation.

5.3.2.4. If the ship's cyber security rectification is not completed within the time limit, ISC will withdraw the ship's Cyber Security class notation.

Appendix 1 Risk Analysis

Section 1 Risk analysis

1.1 Risk assessment

In accordance with relevant cyber security technology and management standards, the shipowner/ship management company shall assess the cyber system and the confidentiality, integrity, availability and other security attributes of the information it processes, transmits and stores. It is necessary to assess the threats to assets and the possibility of security incidents caused by the threats using vulnerability, and to judge the impact of a security incident once it occurs onboard the ship combining with the value of assets involved in the security incident.

1.2 Management requirements

1.2.1 The shipowner/ship management company shall determine the roles and responsibilities of the user, key personnel and the management personnel on shore and on board.

1.2.2 The shipowner/ship management company shall determine the ship's systems, assets, data and capabilities. The ship's operation and security may be exposed to risks if these systems, assets, data and capabilities are in danger.

1.2.3 The shipowner/ship management company shall implement technical measures to prevent network accidents and ensure the continuity of operation. This includes network configuration, network and system access control, communication and boundaries defense and protection, and the application of detection software.

1.2.4 The shipowner/ship management company shall implement procedural protective measures to provide capability to defend cyber security incidents.

1.3 Risk management process

1.3.1 Process

1.3.1.1 Risk assessment or risk disposal activities may be cyclically carried out for the risk management process of the ship's system security (Fig.1 Risk Management Flowchart). A cyclical risk assessment can make each cycle deeper and more specific. The cyclical approach can find a balance between ensuring that high risks are accurately identified and spending minimal time and effort on identifying control measures.

1.3.1.2 Determining the category first and then make a risk assessment. If the risk assessment has provided sufficient information to make an effective decision so as to determine the activities necessary for reducing the risk to an acceptable level, then the risk healing task is over and risk disposal begins. If the information is not sufficient, another cycle of revision category and risk assessment may be carried out, or part of the entire scope may be cycled.

1.3.1.3 Effective risk disposal depends on the results of risk assessment. Risk disposal may not immediately reduce residual risk to an acceptable level. In this case, change of risk category parameters (such as the criteria for risk assessment, risk acceptance or impact) may be required before a risk assessment cycle is carried out, and further risk disposal may be required.

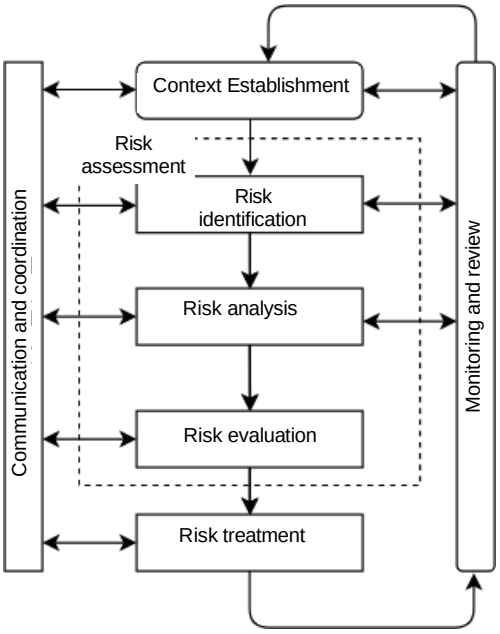

Fig.1 Risk Management Flowchart

1.3.2 Methodology

Specific ship risk management can be implemented with reference to *ISO/IEC27005: 2018 Information Technology - Security Technology - Information Security Risk Management* and *GB/T20984-2007 Information Security Technology - Risk Assessment Specification for Information Security*.

Section 2 Risk assessment process

2.1 Risk assessment process

The risk assessment process is shown in Fig. 2.

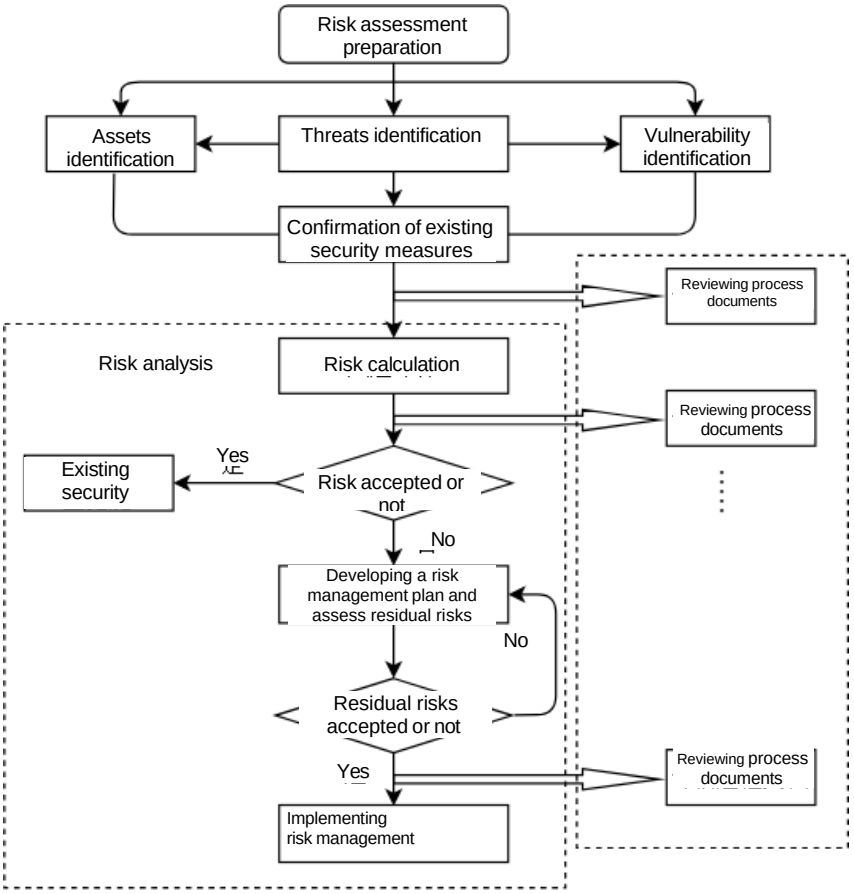

Fig. 2 Risk Assessment Process

2.2 Risk analysis

2.2.1 Risk assessment preparation

Risk assessment preparation is a guarantee of effectiveness of the entire risk assessment process. It is a strategic consideration to implement a risk assessment of the ship system. Its results will be affected by the ship system's business strategy, business process, security needs, system size and structure.

Identifing the deficiencies of the existing information system and management and the risk size that may be caused thereby according to the security needs and the provisions of laws and regulations to be satisfied for the sustainable development of the ship system business. The scope of risk assessment of the ship system shall be all the information thereof and various assets and management organs related to information processing.

2.2.1.1 Assets identification

(1) Assets classification

The shipowner/ship management company submits drawings, data, management procedures and others, sorts out the specific assessment objects and requirements reasonably based on the representation of assets, and classify the assets into IT room, network assets, computers, application assets, management assets, etc. See Table 1 for details.

Assets classification **Table 1**

Assets classification	Examples
IT room	A place where IT equipment and facilities such as Satcom cabinets, firewalls, switches and cabinets are stored in a centralized manner.

Network assets	Network communication and security devices, i.e.: routers, gateways, switches, firewalls, AC controllers, AP transmitters, CCTV cameras, IP phones, Satcom servers, etc.
Computer	IT and OT computers equipped onboard, i.e.: desktop/portable work computers, CCTV host, loading instruments, ECDIS host, liquid level telemetry terminal, centralized engine room monitoring alarm server, boiler manipulation terminal, etc
Application assets	Application system, i.e.: mail system, beacon system, CCTV system, stowage system, ECDIS system, liquid level telemetry system, centralized engine room monitoring alarm system, boiler manipulation system, etc. used for office work and ship manipulation/monitoring/operation.
Management assets	All kinds of management documents, administrative staff and users

(2) Asset assignment

Confidentiality, integrity and availability are the three security attributes of evaluating an asset. The assignment of an asset is determined by how well the asset achieves these three security attributes. The shipowner/ship management company carries out the following asset assignments based on the confirmed assets list under the three security attributes.

a) Assets can be classified into different levels according to their different requirements for confidentiality. For example, Class 1 to 3 (corresponding to: low, medium and high), respectively, corresponds to the degree of confidentiality held in an asset or the impact of the absence of confidentiality on the entire ship system;

b) Assets can also be classified into different levels according to their different requirements for integrity. For example, Class 1 to 3 (corresponding to: low, medium and high), respectively, corresponds to the impact of the absence of integrity on the entire ship system;

c) Assets can also be classified into different levels according to their different requirements for integrity. For example, Class 1 to 3 (corresponding to: low, medium and high), respectively, corresponds to the degree of availability held in an asset;

d) Rank of asset importance

The value of an asset is determined based on the level of assignment thereto in terms of confidentiality, integrity and availability. 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 divided into different levels. For example, level 1 to 3 (corresponding to: low, medium and high). According to the result of asset assignment, the scope of important assets is determined, and further risk assessment is made mainly surrounding the important assets.

2.2.1.2 Threats identification

(1) Threats classification

The factors that cause threats can be divided into human factors and environmental factors. They can be divided into malicious and non-malicious according to motivation. Environmental factors include force majeure factors and other physical factors in the nature. 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 events. The origins of threats shall be fully considered in the classification of threats, and threats classification shall be done according to the representation thereof. For the classification methods, please refer to *ISO/IEC27005: 2018 Information Technology - Security Technology - Information Security Risk Management*.

(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 combining with industry experience and relevant statistical data. Take into comprehensive consideration the following three aspects during the assessment:

a) Threats occurred in previous security incident reports and their frequency statistics;

b) Threats found by detection tools and their various logs in practical conditions and their frequency statistics;

c) Threats to the entire society or specific industries and their frequency statistics as well as threat warnings released by international organizations in recent years

Perform classified treatment of the frequency of threats, where different levels represent the scale of frequency of threats respectively. The bigger the level value, the higher the frequency of threat. For example, Level 1 to 3 (corresponding to: low, medium and high).

2.2.1.3 Vulnerability identification

(1) Contents identified in vulnerability

The vulnerability of the ship's cyber system is intrinsic to the assets. Unless it is used by corresponding threats, otherwise the vulnerability itself will not cause damage to the assets, and if the system is robust enough nor severe threats will cause any security incidents. That is, threats can cause hazards only when asset's vulnerability is used. The vulnerabilities of assets have a concealed property as some of them can only be revealed under certain conditions and circumstances, which is the most difficult part of vulnerability identification.

Vulnerability identification is the most important link in risk assessment. Vulnerability identification can center on assets against the vulnerability of assets and equipment protected by each agreement that may be threatened or used, and an assessment can be made on the severity of the vulnerability. It can also be done from physical, network, system and application levels, which then correspond to assets and threats. The basis of vulnerability identification can be either international or national standards, or the security requirements of industry norms.

a) Vulnerability identification shall be based on the data provided by the shipowner/ship management company and professionals in the relevant lines of business and hardware. The methods used for vulnerability identification mainly include: questionnaire survey, tool detection, manual verification, document query and penetration test.

b) Vulnerability identification is carried out mainly from technology and management aspects, of which technology vulnerability designs the security issues at physical, network, system and application levels. Management vulnerability can be divided into technology management vulnerability and organization management vulnerability, the former is related to specific technical activities and the latter is related to management environment.

(2) Vulnerability assignment

The severity of identified vulnerabilities can be assigned in a hierarchical manner based on the degree of vulnerability exposure to assets and the degree of difficulty in technology implementation. The levels represent the degree of severity of asset's vulnerability respectively. The bigger the level value, the higher the severity of vulnerability. For example, Level 1 to 3 (corresponding to: low, medium and high).

2.2.1.4 Confirmation of existing security measures

The effectiveness of security measures that have been taken shall be confirmed while identifying vulnerabilities. The confirmation of security measures will be made to assess their effectiveness, that is, if the system's vulnerabilities are truly reduced and if the threats are resisted. Effective security measures shall continue to be retained, and those identified as inappropriate shall be verified for cancellation, correction or replacement.

Security measures can be divided into preventive security measures and protective security measures.

The confirmation of existing security measures has a certain connection with vulnerability identification. The application of security measures will reduce the system's technology or management vulnerability. The confirmation of security measures needs not to be as specific to the vulnerability of each asset and component as the vulnerability identification process but the collective of a category of specific measures in order to provide a basis and reference for the development of a risk disposal plan.

2.2.1.5 Risk calculation

After the asset identification, threat identification, vulnerability identification and confirmation of security measures are completed, the shipowner/ship management company shall adopt appropriate methods and tools to determine the possibility of security incidents resulting from threatening to use vulnerabilities. The impact of the loss caused by security incidents on the ship's information system, that is, the security risk of the ship's cyber system, shall be judged based on the asset values and the severity of vulnerabilities affected by the security incidents.

The risk analysis of cyber security on board can be either qualitative or quantitative, or a combination of both:

(1) Identifying assets and assigning values to the assets;

(2) Identifying threats, describing the attributes of the threats, and assigning values to threat frequencies;

(3) Identifying vulnerabilities against specific assets and assigning values to the severity of the vulnerabilities;

(4) Calculating the possibility of security incidents against the severity of threats and vulnerabilities;

(5) Calculate the impact of security incidents on the system, i.e., the risk value , against the possibility of security incidents and consequential losses.

The risk calculation principle paradigm is as follow:

Risk value = R (A, T, V) = R (L (T, V), F (Ia, Va)) (1)

Where, *R* refers to the function of security risk calculation; *A* refers to asset; *T* refers to threat; *V* refers to vulnerability; I_a refers to the value of an assets affected by a security incident; V_a refers to the severity of vulnerability; *L* refers to the possibility of a security incident resulting from threatening to use vulnerabilities; *F* refers to the consequence of a security incident. Risk calculation can be made using matrix method and multiplication method. Refer to Appendix A of *GB/T20984-2007 Information Security Technology - Risk Assessment Specification for Information Security.* Fig. 3 shows the flow chart of on-board cyber security risk analysis and calculation.

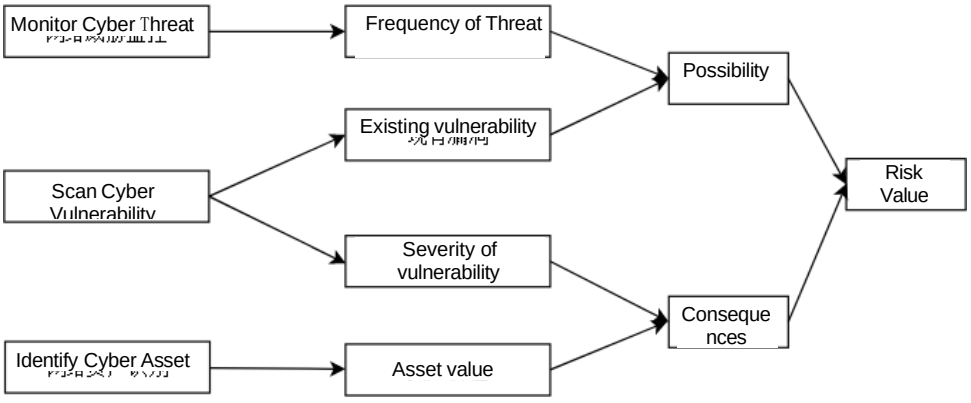

Fig. 3 Risk Analysis and Calculation Flowchart

2.2.1.6 Determination of risk results

To achieve risk control and management, the results of risk assessment shall be subject to a

classified treatment. The different levels represent the severity of asset risk respectively. The bigger the level value, the higher the severity of vulnerability. For example, Level 1 to 3 (corresponding to: low, medium and high).

The risk value faced by each asset shall be calculated with the adopted calculation methods, a range of risk valueshall be set for each level according to the distribution of risk values, and the results of all risk calculations shall be subject to a classified treatment. Each level represents the severity of relative risk. See Table 2 for details.

Risk Levels Table 2

Level	Logotype	Description
3	High	Where the risk level is high, severe economic or social influence will be exerted, if any.
2	Medium	Where the risk level is medium, certain economic or production and operation influence will be exerted if any, but the range and degree of influence are not large, for example, the ship's devices fail to operate in normal condition.
1	Low	Where the risk level is low, the influence exerted is almost non-existent if any, which can be remedied with simple measures or is provided with alternative measures, for example, the on-board office computers fail to operate in normal condition.

2.3 Risk disposal measures

2.3.1.1 Risk disposal plan

For unacceptable risks, a risk disposal plan shall be developed for the ship's cyber system based on the vulnerability causing the risks. The security measures taken for remediation of vulnerability, desired effect, implementation conditions, quarterly arrangement and responsible department shall be determined in the risk disposal plan. The selection of security measures will be considered from both management and technology aspects. The selection and fact of security measures shall be carried out with reference to relevant information security standards.

2.3.1.2 Residual risk assessment

After appropriate security measures are selected for unacceptable risks, in order to ensure the effectiveness of the security measures, a re-assessment can be made to judge if residual risks after the implementation of security measures have been reduced to an acceptable level. Given that the results of residual risks are still within an unacceptable range of risk after appropriate security measures have been taken, consideration shall be given as to whether to accept this risk or take further security measures.

Appendix 2 Pre-assessment Form of Ship Cyber Security

Form CYBER-P

Assessment applicant: Assessment system:

Assessor: Assessment date:

Category	Assessment items	Description	Score
Resources (Total score: 100 Baseline score: 60)	Is main system connected to the network protected by complex password (non-default, longer than 8-bit)? (10 points)		
	Is there a system supporting remote maintenance in the ship network? (-)		
	Can cyber security topology cover all systems and interfaces? (10 points)	Refer to network topology structure document.	
	Is the external communication of ship encrypted? (10 points)	Relevant encryption measures are taken to protect the data or message information in ship-shore or ship-ship communication.	
	Are encryption measures for file transmission and storage taken when mobile device (laptop, U disk, etc.) is connected to the network? (5 points)		
	Are unnecessary ports and services in the network disabled? (5 points)		
	Is the program regularly updated, patched and fixed? (10 points)		
	Are files regularly backed up and kept in a safe place? (10 points)	It is recommended to keep the backup files in device that is not connected to the Internet.	
	Are the system administrator account and user account in ship network subject to centralized storage and encryption management? (5 points)	All systems connected to the network are subject to the unified single sign-on, and account information and system data are stored separately with encryption measures.	
	Is an anonymous account or a general account able to log in to the ship network? (10 points)		

Category	Assessment items	Description	Score
	Is the log for login to ship network provided? (5 points)		
	Is the system configuration file stored validly with proper protection measures? (20 points)	The configuration file shall record the device and systems connected to the ship network and record the basic system parameters.	
Program (Total score: 120 Baseline score: 70)	Is ISO 27001 information security management system applied in the Company? (20 points)	The shipowner/ship management company has established the Information Security Management System (ISMS) and it is ISO 27001 certified.	
	Has the Company participated in a network risk assessment? (30 points)	The topology analysis, security risk auditing and other works are implemented, and relevant assessment reports can be provided.	
	Is a cyber security incident handler available? (15 points)	The Company's information management department has developed a clear code of conduct for cyber security incidents and specifically assigns the responsibilities in the procedural documents.	
	Is security level of the Company network reviewed regularly? (10 points)	The Company regularly assesses the level of cyber security, and adjusts corresponding management measures.	
	Has the developer of system connected to the ship network signed the confidentiality agreement? (5 points)		
	Does the Company emphasize the measures of setting the device password? (5 points)		
	Is the crew aware of the consequences of cyber attacks? (10 points)	Relevant information will be introduced in the Company's information security training.	
	Does the crew know the responsibilities of users and administrators in the cyber system? (5 points)	Ditto.	
	Is the crew aware of risks brought by using an unauthorized mobile data storage device? (5 points)	Ditto.	
	Does the crew realize the risks brought by opening e-mail attachments and accessing attachment links? (5 points)	Ditto.	
	Does the Company provide the cyber security training for the		

Category	Assessment items	Description	Score
	crew? (10 points)		
Risk (Total score: 60 Baseline score: 35)	Is the file received through the network or downloaded from e-mail set to be automatically opened? (10 points)		
	Is the host connected to the ship network installed with software for intrusion detection, virus defense and flow analysis? (15 points)		
	Is the host connected to the ship network able to monitor and record logs and alarms? (15 points)		
	Is the cyber system subject to the penetration test? (10 points)	The test is performed by using the professional penetration test system.	
	Is vulnerability scanning performed on the cyber system? (10 points)	The scanning is performed by using the professional vulnerability scanning system.	

* The baseline score in the table represents the basic score that should be reached in the pre-assessment phase for ships applying for ISC ship cyber security class notations.

Appendix 3 Ship cyber system/ Device Assessment Form

Form CYBER-K

Assessment applicant: Assessed ship:

Assessor: Assessment date:

Category	System/device	Other networks connected (Y/N)	Detailed assessment incorporated (Y/N)	Remarks
Communication system	Satellite communication equipment			
Bridge system	Voice of Internet phone (VOIP)			
	Wireless networks (WLANs)			
	General alarm system			
	Positioning system (GPS, etc.)			
	Electronic chart display system (ECDIS)			
	Dynamic positioning (DP) system			
	Systems associated with electronic navigation system and propulsion/ maneuvering system			
	Automatic identification system (AIS)			
	Global maritime distress and safety system (GMDSS)			
	Radar equipment			
	Voyage data recorder (VDR)			
	Inertial navigation system (INS)			
	Other monitoring and data collection systems			
Propulsion, mechanical equipment management and electric control systems	Diesel engine			
	Boiler control system			
	Auxiliary security system			
	Power station and power management system			
	Automatic monitoring system			
	Alarm system			
	Emergency system			
	Pollution prevention system			
	Steering control system			
Access control system	Monitoring systems, including CCTV system			
	Bridge navigational watch alarm system (BNWAS)			

Category	System/device	Other networks connected (Y/N)	Detailed assessment incorporated (Y/N)	Remarks
	Ship security alarm system (SSAS)			
	Embarking/ disembarking system			
	Public broadcasting and general alarm systems			
Cargo management system	Cargo control room and system equipment			
	Monitoring and alarm system for level, pressure and temperature of cargo			
	Level indication system			
	Valve remote control system			
	Gas liquefaction system			
	Loading calculation system			
	Inert gas control and monitoring system			
	Handling control and monitoring system			
	Crane control and monitoring system			
	Conditioning, temperature and ventilation system of cargo			
	Liquefied gas thermal oxidation system			
Stability in case of water ingress	Water ingress alarm system			
	Ballast water system			
	Watertight door			
	Watertight hatch cover			
	Bilge water system			
	Water ingress detection system of passenger ship			
Anchor	Anchor gear control and monitoring system			
	Mooring control system			
Engineering	Hoisting control system			
	Drilling control and monitoring system			
	Oil and gas monitoring and production system			
Fire and ignition source control	Fire monitoring system			
	Smoke detection system			
	Fire door control system			
	Fire pump control and monitoring system			
	Fire extinguishing system			
	Hazardous gas detection system			
	Hydrocarbon gas detection system			

Category	System/device	Other networks connected (Y/N)	Detailed assessment incorporated (Y/N)	Remarks
Passenger service management system	Asset management system			
	Medical records			
	Passenger boarding access system			
	Infrastructure supporting systems (e.g. domain name system, user identification/ authorization system)			
Passenger network	Passenger login into Wi-Fi or LAN			
	Entertainment system			
	Communication system			
Core infrastructure system	Router			
	Switch			
	Firewall			
	Virtual private network (VPN)			
	Virtual local area network (VLAN)			
	Intrusion prevention system			
	Security incident log system			
Information management system	Information management system (spare parts and materials management, PMS management, employee management and training systems)			
Individual equipment	Individual devices of crew, LAN or WiFi connected to the Internet			
Intelligent system	Intelligent navigation			
	Intelligent ship body			
	Intelligent cabin			
	Intelligent energy efficiency management			
	Intelligent cargo management			
	Intelligent integration platform			
Other systems	Other systems unspecified in the table and connected to the ship network			

Appendix 4 Detailed Assessment Form of Ship Cyber Security (Product)

Form CYBER-DD

Assessment applicant: Assessment system:

Assessor: Assessment date:

Notes: 1. Attention shall be paid to the assessment requirements if there is "×".

2. Numbering identifiers with "" are necessary items for detailed assessment (the assessment requirements have to be fully met).*

Category	Clauses	Details	Yes/No	Remark
Network redundancy	3.3.1.1.		☐	
	3.3.1.2.		☐	
Communication security	3.3.3.3.		☐	
	3.3.3.7.		☐	
	3.3.3.9.	(1) (2) (3) (4) (5) (6)	☐ ☐ ☐ ☐ ☐ ☐	
	3.3.3.15.	(1) (2) (3)	☐ ☐ ☐	
Wireless	3.3.4.1.			
	3.3.4.2.	(1) (2) (3) (4) (5)	☐ ☐ ☐ ☐ ☐	

Category	Clauses	Details	Yes/No	Remark
	3.3.4.3.	(1) (2) (3) (4)	□ □ □ □	
Boundary defense	3.4.1.5.		□	
	3.4.1.8.		□	
	3.4.1.9.		□	
Access control	3.4.5.1.		□	
	3.4.5.2		□	
	3.4.5.3.	(1) (2) (3) (4) (5) (6)	□ □ □ □ □ □	
	3.4.5.4.	(1) (2) (3) (4) (5) (6)	□ □ □ □ □ □	
	3.4.5.5.	(1) (2) (3) (4) (5) (6)	□ □ □ □ □ □	
	3.4.5.6.	(1) (2)	□ □	

Category	Clauses	Details	Yes/No	Remark
		(3) (4)	□ □	
	3.4.5.9.	(1) (2) (3) (4) (5) (6) (7) (8) (9) (10)	□ □ □ □ □ □ □ □ □ □	
Remote operation and maintenance	3.4.6.3.	(1) (2) (3) (4) (5) (6)	□ □ □ □ □ □	
	3.4.6.4	(1) (2)	□ □	
Authentication	3.5.1.1.		□	
Data security	3.5.2.2.	(1)	□	
	3.5.2.4.	(1) (2) (3) (4) (5)	□ □ □ □ □	
Backup	3.5.5.1.		□	
	3.5.5.2.		□	

Appendix 5 Detailed Assessment Form of Ship Cyber Security (Ship)

Form CYBER-DS

Assessment applicant: Assessment system:

Assessor: Assessment date:

Note: 1. Attention shall be paid to the assessment requirements if there is "×".

2. Numbering identifiers with "" are necessary items for detailed assessment (the assessment requirements have to be fully met).*

Category	Sub Category	Grade	Clauses	Details	Yes/No	Remark
Physical security	Location	P/S	3.2.1.1.		☐	
		P/S	3.2.1.2.		☐	
	Physical access control	P/S	3.2.2.1.		☐	
		P/S	3.2.2.2.		☐	
		P/S	3.2.2.3.	（1） （2） （3） （4）	☐ ☐ ☐ ☐	
		P/S	3.2.2.4.	（1） （2）	☐ ☐	
		P/S	3.2.2.5.	（1） （2） （3）	☐ ☐ ☐	
		P/S	3.2.2.6.		☐	
		P/S	3.2.2.7.		☐	
	Installation	P/S	3.2.3.1.		☐	
		P/S	3.2.3.3.		☐	
		P/S	3.2.3.4.		☐	
		P/S	3.2.3.4.		☐	
Network	Network	S	3.3.1.1.		☐	

Category	Sub Category	Grade	Clauses	Details	Yes/No	Remark
architecture	redundancy	S	3.3.1.2.		☐	
	Network segregation and segmentation	P/S	3.3.2.1.	（1） （2） （3）	☐ ☐ ☐	
		P/S	3.3.2.2.	（1） （2） （3）	☐ ☐ ☐	
		P/S	3.3.2.3.	（1） （2）	☐ ☐	
		P/S	3.3.2.4.	（1） （2） （3）	☐ ☐ ☐	
		P/S	3.3.2.5.		☐	
		P/S	3.3.2.6.		☐	
		P/S	3.3.2.7.	（1） （2） （3）	☐ ☐ ☐	
	Communication security	P/S	3.3.3.1.		☐	
		P/S	3.3.3.2.		☐	
		P/S	3.3.3.3.		☐	
		P/S	3.3.3.4.		☐	
		P/S	3.3.3.5.		☐	
		P/S	3.3.3.6.		☐	
		P/S	3.3.3.7.		☐	
		P/S	3.3.3.8.		☐	
		P/S	3.3.3.9.	（1） （2） （3） （4） （5） （6）	☐ ☐ ☐ ☐ ☐ ☐	
		P/S	3.3.3.10.		☐	

Category	Sub Category	Grade	Clauses	Details	Yes/No	Remark
		P/S	3.3.3.11.		☐	
		P/S	3.3.3.12.		☐	
		P/S	3.3.3.13.		☐	
		P/S	3.3.3.14.		☐	
		P/S	3.3.3.15.	（1） （2） （3）	☐ ☐ ☐	
	Wireless	P/S	3.3.4.1.			
		P/S	3.3.4.2.	（1） （2） （3） （4） （5）	☐ ☐ ☐ ☐ ☐	
		P/S	3.3.4.3.	（1） （2）	☐ ☐	
		P/S	3.3.4.4.		☐	
	Asset List	P/S	3.3.5.1	（1） （2）	☐ ☐	
		P/S	3.3.5.2.		☐	
	Network test	P/S	3.3.6.1.	（1） （2） （3） （4） （5） （6） （7） （8） （9）	☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐	
		P/S	3.3.6.2.		☐	
		P/S	3.3.6.3.		☐	
Network boundary	Boundary defense	P/S	3.4.1.1.	（1） （2）	☐ ☐	

Category	Sub Category	Grade	Clauses	Details	Yes/No	Remark
		P/S	3.4.1.2.		☐	
		P/S	3.4.1.3.		☐	
		P/S	3.4.1.4.		☐	
		P/S	3.4.1.5.		☐	
		P/S	3.4.1.6.		☐	
		P/S	3.4.1.7.		☐	
		P/S	3.4.1.8.		☐	
		P/S	3.4.1.9.		☐	
	Malicious code prevetion	P/S	3.4.2.1.		☐	
		P/S	3.4.2.2.		☐	
		P/S	3.4.2.3.		☐	
		P/S	3.4.2.4.	（1） （2） （3）	☐ ☐ ☐	
		P/S	3.4.2.5.		☐	
		P/S	3.4.2.6.		☐	
		P/S	3.4.2.7.		☐	
		P/S	3.4.2.8.		☐	
	Intrusion prevention	P/S	3.4.3.1.		☐	
		P/S	3.4.3.2.		☐	
		P/S	3.4.3.3.		☐	
		P/S	3.4.3.4.		☐	
		P/S	3.4.3.5.		☐	
		P/S	3.4.3.6.		☐	
		P/S	3.4.3.7.		☐	
		P/S	3.4.3.8.		☐	
		P/S	3.4.3.9.		☐	
		P/S	3.4.3.10.		☐	
	Monitoring and Alarm	S	3.4.4.1.		☐	
		S	3.4.4.2.		☐	
		S	3.4.4.3.		☐	

Category	Sub Category	Grade	Clauses	Details	Yes/No	Remark
		S	3.4.4.4.		☐	
		S	3.4.4.5.	（1） （2） （3） （4） （5） （6）	☐ ☐ ☐ ☐ ☐ ☐	
		S	3.4.4.6.	（1） （2） （3）	☐ ☐ ☐	
		S	3.4.4.7.		☐	
		S	3.4.4.8.		☐	
		S	3.4.4.9.	（1） （2） （3） （4） （5）	☐ ☐ ☐ ☐ ☐	
		S	3.4.4.10.		☐	
		S	3.4.4.11.	（1） （2） （3） （4） （5） （6）	☐ ☐ ☐ ☐ ☐ ☐	
	Acess control	P/S	3.4.5.1.		☐	
		P/S	3.4.5.2		☐	
		P/S	3.4.5.3.	（1） （2） （3） （4） （5） （6）	☐ ☐ ☐ ☐ ☐ ☐	

Category	Sub Category	Grade	Clauses	Details	Yes/No	Remark
		P/S	3.4.5.4.	(1) (2) (3) (4) (5) (6)	□ □ □ □ □ □	
		P/S	3.4.5.5.	(1) (2) (3) (4) (5) (6)	□ □ □ □ □ □	
		P/S	3.4.5.6.	(1) (2) (3) (4)	□ □ □ □	
		P/S	3.4.5.7.	(1) (2) (3)	□ □ □	
		P/S	3.4.5.8.	(1) (2) (3) (4) (5) (6) (7) (8) (9) (10)	□ □ □ □ □ □ □ □ □ □	
		P/S	3.4.5.9.	(1) (2) (3)	□ □ □	

Category	Sub Category	Grade	Clauses	Details	Yes/No	Remark
				（4） （5）	☐ ☐	
Network boundary	Remote operation and maintenance	P/S	3.4.6.1		☐	
		P/S	3.4.6.2		☐	
		P/S	3.4.6.3	（1） （2） （3） （4） （5） （6）	☐ ☐ ☐ ☐ ☐ ☐	
		P/S	3.4.6.4	（1） （2）	☐ ☐	
Compute environment	Authentication	P/S	3.5.1.1.		☐	
		P/S	3.5.1.2.			
	Data security	P/S	3.5.2.1.		☐	
		P/S	3.5.2.2.	（1） （2） （3） （4） （5） （6） （7） （8） （9）	☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐	
		P/S	3.5.2.3.		☐	
		P/S	3.5.2.4.	（1） （2） （3） （4） （5）	☐ ☐ ☐ ☐ ☐	
		P/S	3.5.2.5.		☐	
		P/S	3.5.2.6.		☐	

Category	Sub Category	Grade	Clauses	Details	Yes/No	Remark
		P/S	3.5.2.7.		☐	
		P/S	3.5.2.8.		☐	
	Software installation and update	P/S	3.5.3.1	（1） （2） （3） （4） （5）	☐ ☐ ☐ ☐ ☐	
		P/S	3.5.3.2	（1） （2） （3）	☐ ☐ ☐	
	Emergency response	P/S	3.5.4.1.	（1） （2） （3） （4） （5）	☐ ☐ ☐ ☐ ☐	
		P/S	3.5.4.2		☐	
		P/S	3.5.4.2.		☐	
		P/S	3.5.3.3.		☐	
	Backup	P/S	3.5.5.1.		☐	
		P/S	3.5.5.2.		☐	
Security audit	Configuration	P/S	3.6.1.1.		☐	
		P/S	3.6.1.2.	（1） （2） （3） （4） （5） （6） （7） （8） （9） （10） （11）	☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐	

Category	Sub Category	Grade	Clauses	Details	Yes/No	Remark
				（12） （13） （14） （15）	☐ ☐ ☐ ☐	
		P/S	3.6.1.3.	（1） （2） （3）	☐ ☐ ☐	
		P/S	3.6.1.4.	（1） （2） （3） （4） （5） （6） （7） （8） （9） （10） （11）	☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐	
	Security audit (log)	S	3.6.2.1.		☐	
		S	3.6.2.2.	（1） （2） （3） （4）	☐ ☐ ☐ ☐	
		S	3.6.2.3.		☐	
		S	3.6.2.4.		☐	
		S	3.6.2.5.		☐	
		S	3.6.2.6.		☐	
		S	3.6.2.7.		☐	
		S	3.6.2.8		☐	

Appendix 6 Additional Suggestions for Firewall Settings of Ship Industrial Control System

A two-port firewall instead of isolation zone is configured on the public server, rulemaking is particularly important. At least all rules shall contain IP addresses and port numbers. The rules for the address part shall prevent the communication between host from the office network address and some public servers (e.g., mass data recording system) in the control network, and any IP addresses that are intended to enter the control network and belong to the office network are not allowed. In addition, the rules for the port part shall focus on protocol security. Due to potential network interception and modification, it is a security risk to allow HTTP, FTP or other insecure protocols to traverse firewalls. While making rules, active connection initiated by host outside the control network to the network shall be rejected, and only connection actively initiated by host in the network is allowed.

If the architecture with isolation zone is used, the office network and control network can be configured to have no direct connection. Except in special circumstances, the terminal of any party will be the server in the isolation zone. “Combined” protocol can be used in the control network and office network communication. That is, when a protocol is used for the communication between the control network and the isolation zone, it cannot be used for the communication between the office network and the isolation zone preferably.

General rules are described as follows:

- Internal rules are prohibited, and devices connected to the control system must be operated through the isolation zone.
- External rules must be restricted, and used for necessary communications only.
- The connection from the control network to the office network must strictly control the sources and purposes through services and ports.

In addition to these rules, the firewall shall also be configured with outbound filtering rules to prevent fake IP packets escaping from the control network or isolation zone. This function is implemented by comparing interface addresses of the firewall with the source IP addresses of the outbound packets to prevent the control network from being deceived by communication (e.g., fake IP).

Special attention shall be paid to the following contents when firewall rules are made:

- The basic rule is to reject everything.
- Port communications and services between the control network environment and office network shall be approved on case-by-case basis. There must be business reasons for each data import or export, and there shall be documented risk analysis and responsible person.
- If the status is appropriate, all allowed rules shall contain IP addresses and TCP/UDP designated ports.
- All rules shall restrict IP addresses or address fields designated for the communication.
- The direct connection between all control networks and office networks shall be prohibited, and all communication terminals are isolation zones.
- When a protocol is used for the communication between the control network and the isolation zone, it cannot be used for the communication between the office network and the isolation zone.
- The connection from the control network to the office network must strictly control the sources and purposes through services and ports.
- The outbound packets of the control network and isolation zone must have correct IP addresses set for the control network or isolation zone.
- Devices in the control network cannot be connected to the Internet.
- Even if the protection of the firewall, the control network cannot be directly connected to the Internet.

All communications controlled by the firewall shall have an independent securely managed network or multi-factor authentication encryption network. In addition, for specific management situations, the communication can also be restricted through IP address.