April 2019

ClassNK

Cyber Security Management System for Ships

(Requirements and Controls) [First Edition]

[English]

ClassNK Cyber Security Approach

ClassNK has compiled the "ClassNK Cyber Security Approach" as a basic way of thinking about onboard cyber security based on trends in international institutions and maritime bodies.

1. Ensuring navigational safety is of the highest priority

The most important goal of onboard cyber security controls is to ensure navigational safety. To achieve it, it is of high priority to ensure availability of systems in terms of operation technology (OT) as well as information technology (IT) systems, which support operation of ships.
To mitigate cyber risks in both IT and OT, we will propose controls based on a balanced combination of physical, technical, and organizational approaches, such as designing ships and onboard equipment with security by design, constructing management systems during service, etc.

2. Setting layers of cyber security controls

We will classify cyber security controls into different layers, and clarify what each of stakeholders should do for each layer by adopting requirements from the existing standards on cyber security that are considered applicable to ships.

3. Ongoing revisions and updates

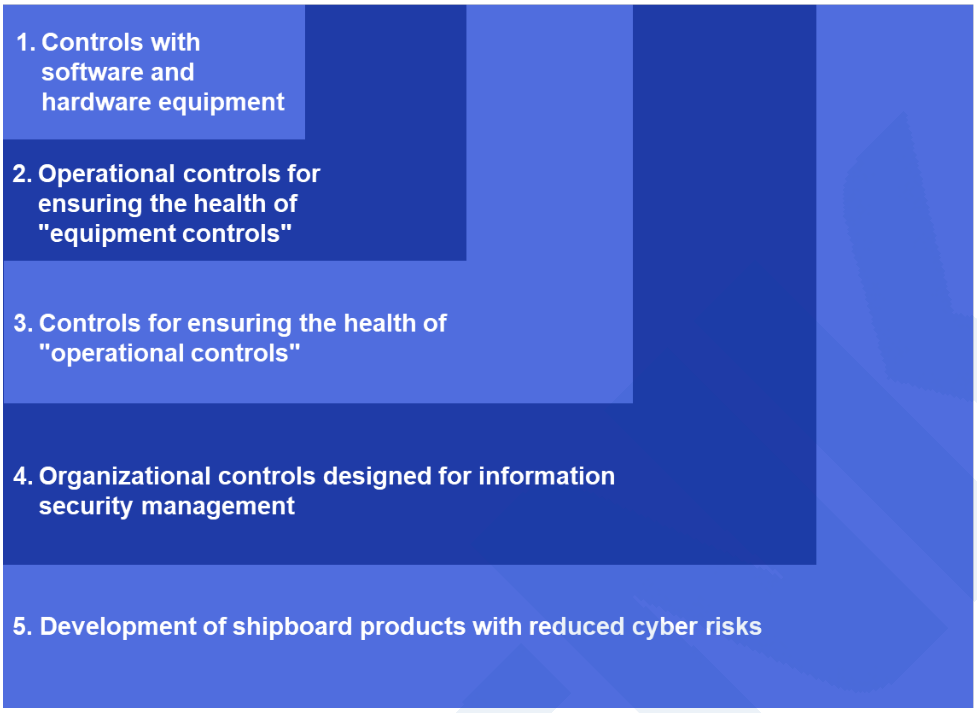
In light of the increased use of IT for the operation of ships and international trends in cyber security, we will analyze the latest information with experts and propose current best practices in cyber security controls for ships.

Based on these concepts, we will continually publish guidelines and standards that specify the parties responsible for implementing cyber security controls and the details thereof as part of the "ClassNK Cyber Security Series".

For the first edition of the Guidelines, we tried to extract minimum required controls for ships from standards on cyber security. However, cyber security controls implemented in accordance with the Guidelines may be insufficient or excessive. Therefore, we will continually revise and optimize the Guidelines for ships.

ClassNK Cyber Security Approach

Layers of Cyber Security Controls



1. Controls with software and hardware equipment

2. Operational controls for ensuring the health of "equipment controls"

3. Controls for ensuring the health of "operational controls"

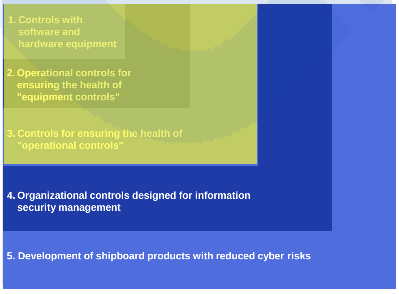
4. Organizational controls designed for information security management

5. Development of shipboard products with reduced cyber risks

ClassNK Cyber Security Series

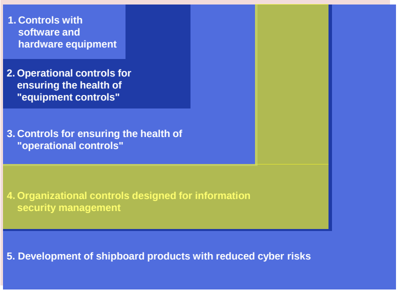
Guidelines for Designing Cyber Security Onboard Ships

- Target: Shipyards and shipowners
- Extract controls applicable to ships from NIST SP800-53 using NIST SP800-82 as a reference
- Examine the IACS Recommendations



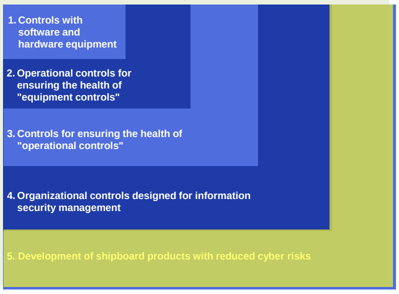
Cyber Security Management System for Ships

- Target: Ship management companies and ships
- Management system aimed at compatibility with the ISM Code system using the basic structures of ISO 27001 and ISO 27002



Software Security Guidelines

- Target: Shipboard equipment manufacturers
- Verify development process and functional requirements based on guidelines with elements required for ships extracted from relevant ISO/IEC standards



Revision History

No.	Date	Category	Details of revision
1	April 1, 2019	New	First issue

CONTENTS

INTRODUCTION

1 Background and context

"Cyber Security Management System for Ships" (NK-CSMS) provides guidelines for activities to establish, maintain, and continually improve a management system for cyber security so that the company and ship can ensure safety of the ship in operation. Integrating NK-CSMS into the processes and management structure of the company and ship will be helpful in properly evaluating and managing cyber risks. When applying NK-CSMS, the needs, goals, and capabilities of the organization should be taken into account in addition to the cyber security controls provided in this document.

This document consists of the following 2 parts.

"PART 1 REQUIREMENTS" defines the requirements for a Cyber Security Management System (CSMS). The requirements apply to the company and ship.

"PART 2 CONTROLS" defines cyber security controls in shipbuilding and operation. The controls are implemented for the company and ship.

			Target	
			Company	Ship
PART 1	REQUIREMENTS		○	○
Part 2	CONTROLS	Shipbuilding	○ Chapter 2	-
		Operation	○ Chapter 3	○ Chapter 4

2 Definitions

The following definitions apply to Parts 1 and 2 of this document.

2.1 Cyber Security

"Cyber Security" means the activities performed in the company and onboard the ship to ensure the safety of operation and maintain proper implementation of shipboard operations by protecting equipment, information communication devices, networks, and information related to operation from threats.

2.2 Company

"Company" means the owner of the ship or any other organization or person such as the manager, or the bareboat charterer, who has assumed the responsibility for operation of the ship from the shipowner and who, on assuming such responsibility, has agreed to take over all the duties and responsibility imposed by the NK-CSMS.

2.3 Administration

"Administration" means the Government of the State whose flag the ship is entitled to fly.

2.4 Cyber Security Management System (CSMS)

"Cyber Security Management System" means a structured and documented management system enabling Company personnel to implement effectively the Company cyber security policy.

2.5 Cyber Security Management Certificate

"Cyber Security Management Certificate" means a document issued to a ship which signifies that the Company and its shipboard management operate in accordance with the approved CSMS.

2.6 Objective Evidence

"Objective Evidence" means quantitative or qualitative information, records or statements of fact pertaining of cyber security or to the existence and implementation of a CSMS element, which is based on observation, measurement or test and which can be verified.

2.7 Non-Conformity

"Non-conformity" means an observed situation where objective evidence indicates the non-fulfillment of a specified requirement.

2.8 Major Non-Conformity

"Major non-conformity" means an identifiable deviation that poses a serious threat to the cyber security of personnel or the ship or a serious risk to the environment that requires immediate corrective action or the lack of effective and systematic implementation of a control of the CSMS.

2.9 Convention

"Convention" means the International Convention for the Safety of Life at Sea, 1974 as amended.

PART 1: REQUIREMENTS

Chapter 1 GENERAL

1.1 Objectives

1.1.1 General

The objective of Part 1 is to ensure cyber security in ship operation.

1.1.2 Cyber security management objectives of the company

Cyber security management objectives of the Company should, inter alia:

-1. Provide for safe practices in ship operation and a safe working environment;

-2. Assess all identified cyber risks to its ships, personnel and the environment and establish appropriate safeguards; and

-3. Continuously improve cyber security management skills of personnel ashore and aboard ships, including preparing for emergencies related both to cyber security.

1.1.3 Compatibility with relevant rules, regulations, codes, and guidelines

The CSMS should ensure:

-1. Compliance with mandatory rules and regulations; and

-2. That applicable codes, guidelines and standards recommended by the Organization, Administrations, classification societies and maritime industry organizations are taken into account.

1.2 Application

The controls defined in Part 2 may be applied to all ships and companies.

1.3 Functional Requirements for a Cyber Security Management System (CSMS)

Every Company should develop, implement and maintain a cyber security management system (CSMS) which includes the following functional requirements:

-1. A cyber security policy;

-2. Instructions and procedures to ensure cyber security of ships in compliance with relevant international and flag State legislation;

-3. Defined levels of authority and lines of communication between, and amongst, shore and shipboard personnel;

-4. Procedures for reporting accidents and non-conformities with the provisions of the Requirements;

-5. Procedures to prepare for and respond to emergency situations; and

-6. Procedures for internal audits and management reviews.

Chapter 2 CYBER SECURITY POLICY

2.1 Establishment of the Cyber Security Policy

The Company should establish a cyber security policy which describes how the objectives given in paragraph **1.1** will be achieved.

2.2 Implementation and Maintenance of the Cyber Security Policy

The Company should ensure that the policy is implemented and maintained at all levels of the organization both, ship-based and shore-based.

Chapter 3 COMPANY RESPONSIBILITIES AND AUTHORITY

3.1 Reporting of the Entity Who Is Responsible for the Operation of the Ship

If the entity that is responsible for the operation of the ship is other than the owner, the owner must report the full name and details of such entity to the Administration.

3.2 Definition of Responsibilities for Work Relating to Cyber Security

The Company should define and document the responsibility, authority and interrelation of all personnel who manage, perform and verify work relating to and affecting cyber security.

3.3 Company's Responsibility for Support

The Company is responsible for ensuring that adequate resources and shore-based support are provided to enable the designated person or persons to carry out their functions.

Chapter 4 DESIGNATED PERSONS

4.1 Appointment of Designated Persons and their Responsibility and Authority

To ensure the cyber security of each ship and to provide a link between the Company and those on board, every Company, as appropriate, should designate a person or persons ashore having direct access to the highest level of management. The responsibility and authority of the designated person or persons should include monitoring the cyber security aspects of the operation of each ship and ensuring that adequate resources and shore-based support are applied, as required.

Chapter 5 MASTER'S RESPONSIBILITY AND AUTHORITY

5.1 Master's Responsibility

The Company should clearly define and document the master's responsibility with regard to:

-1. Implementing the cyber security policy of the Company;

-2. Motivating the crew in the observation of that policy;

-3. Issuing appropriate orders and instructions in a clear and simple manner;

-4. Verifying that specified requirements are observed; and

-5. Periodically reviewing the CSMS and reporting its deficiencies to the shore-based management.

5.2 Master's Authority

The Company should ensure that the CSMS operating on board the ship contains a clear statement emphasizing the master's authority The Company should establish in the CSMS that the master has the overriding authority and the responsibility to make decisions with respect to cyber security and to request the Company's assistance as may be necessary.

Chapter 6 RESOURCES AND PERSONNEL

6.1 Requirements for the Master

The Company should ensure that the master is:

-1. Properly qualified for command;

-2. Fully conversant with the Company's CSMS; and

-3. Given the necessary support so that the master's duties can be safely performed.

6.2 Requirements for Manning

The Company should ensure that each ship is:

-1. Manned with qualified, certificated and medically fit seafarers in accordance with national and international requirements; and

-2. Appropriately manned in order to encompass all aspects of maintaining cyber security operation on board.

6.3 Familiarization

The Company should establish procedures to ensure that new personnel and personnel transferred to new assignments related to cyber security are given proper familiarization with their duties. Instructions which are essential to be provided prior to sailing should be identified, documented and given.

6.4 Ensuring of Understanding by Personnel Involved

The Company should ensure that all personnel involved in the Company's CSMS have an adequate understanding of relevant rules, regulations, codes and guidelines.

6.5 Training

The Company should establish and maintain procedures for identifying any training which may be required in support of the CSMS and ensure that such training is provided for all personnel concerned.

6.6 Establishment of Procedures for Providing Information

The Company should establish procedures by which the ship's personnel receive relevant information on the CSMS in a working language or languages understood by them.

6.7 Ensuring of Communication with the Ship's Personnel

The Company should ensure that the ship's personnel are able to communicate effectively in the execution of their duties related to the CSMS.

Chapter 7 SHIPBOARD OPERATIONS

7.1 Establishment of Shipboard Operations

The Company should establish procedures, plans and instructions, including checklist as appropriate, for key shipboard operations concerning the cyber security of the personnel and ship. The various tasks should be defined and assigned to qualified personnel.

Chapter 8 EMERGENCY PREPAREDNESS

8.1 Establishment of Procedures to Respond to Emergency Situations

The Company should identify potential emergency shipboard situations, and establish procedures to respond to them.

8.2 Establishment of Programs to Respond to Emergency Situations

The Company should establish programs for drills and exercises to prepare for emergency actions.

8.3 Provision of Measures Ensuring Response to Emergency Situations

The CSMS should provide for measures ensuring that the Company's organization can respond at any time to hazards, accidents and emergency situations involving its ships.

Chapter 9 REPORTS AND ANALYSIS OF NON-CONFORMITIES, ACCIDENTS AND HAZARDOUS OCCURRENCES

9.1 Reports of Non-Conformities, Accidents and Hazardous Situations

The CSMS should include procedures ensuring that non-conformities, accidents and hazardous situations are reported to the Company, investigated and analyzed with the objective of improving cyber security.

9.2 Measures to Prevent Recurrence

The Company should establish procedures for the implementation of corrective action, including measures intended to prevent recurrence.

Chapter 10 MAINTENANCE OF THE SHIP AND EQUIPMENT

10.1 Establishment of Maintenance Procedures

The Company should establish procedures to ensure that the ship is maintained in conformity with the provisions of the relevant rules and regulations and with any additional requirements which may be established by the Company.

10.2 Requirements for Maintenance Procedures

In meeting these requirements the Company should ensure that:

-1. Inspections are held at appropriate intervals;
-2. Any non-conformity is reported, with its possible cause, if known;
-3. Appropriate corrective action is taken; and
-4. Records of these activities are maintained.

10.3 Ensuring of the Continuity of Maintenance Procedures

The Company should identify equipment and technical systems the sudden operational failure of which may result in hazardous situations. The CSMS should provide for specific measures aimed at promoting the reliability of such equipment or systems. These measures should include the regular testing of stand-by arrangements and equipment or technical systems that are not in continuous use.

10.4 Relationship with the Maintenance Routine

The inspections mentioned in **10.2** as well as the measures referred to in **10.3** should be integrated into the ship's operational maintenance routine.

Chapter 11 DOCUMENTATION

11.1 Establishment and Maintenance of Document Control Procedures

The Company should establish and maintain procedures to control all documents and data which are relevant to the CSMS.

11.2 Requirements for Document Control Procedures

The Company should ensure that:

-1. Valid documents are available at all relevant locations;

-2. Changes to documents are reviewed and approved by authorized personnel; and

-3. Obsolete documents are promptly removed.

11.3 Cyber Security Management Manual

The documents used to describe and implement the CSMS may be referred to as the Cyber Security Management Manual. Documentation should be kept in a form that the Company considers most effective. Each ship should carry on board all documentation relevant to that ship.

Chapter 12 COMPANY VERIFICATION, REVIEW AND EVALUATION

12.1 Audits of the Cyber Security Management System

The Company should carry out internal cyber security audits on board and ashore at intervals not exceeding twelve months to verify whether cyber security activities comply with the CSMS. In exceptional circumstances, this interval may be exceeded by not more than three months.

12.2 Supplier Relationships

The Company should periodically verify whether all those undertaking delegated CSMS-related tasks are acting in conformity with the Company’s responsibilities under the CSMS.

12.3 Evaluation of the Cyber Security Management System

The Company should periodically evaluate the effectiveness of the CSMS in accordance with procedures established by the Company.

12.4 Implementation of Audits and Corrective Actions

The audits and possible corrective actions should be carried out in accordance with documented procedures.

12.5 Independence of Audits

Personnel carrying out audits should be independent of the areas being audited.

12.6 Calling Attention to the Results of Reviews

The results of the audits and reviews should be brought to the attention of all personnel having responsibility in the area involved.

12.7 Implementation of Corrective Actions

The management personnel responsible for the area involved should take timely corrective action on deficiencies found.

Part 2 CONTROLS

Chapter 1 GENERAL

1.1 Objectives

Part 2 defines cyber security controls (hereafter called "controls") to be implemented in the company and onboard the ship in order to properly respond to cyber risks in operation.

1.2 Application

Part 2 applies to the company and ship.

1.3 Relationships Between Risk Management and Controls for Cyber Security

1.3.1 Cyber security threats in ships

Onboard equipment related to operation of the ship includes the main engine, steering gear, navigation support systems, generators, equipment for cargo handling management, information systems and terminals, communication devices, and equipment for responding to emergencies, etc. These devices utilize ICT for control, communication, and human interface. Especially, they are connected externally and to each other via networks. For example, the main engine is remotely controlled from the bridge. Steering instructions are sent to the steering gear via onboard networks. Also, the rudder status is displayed on the navigation support system. The ship's position, speed, distance from other ships are captured by devices including the GPS compass, gyro compass, and radars, and displayed on the navigation support system. ICT is also used for cargo control and onboard/outboard communication.

With the introduction of ICT, there are a wide variety of potential cyber security threats in operation of ships, including:

-1. If onboard equipment is connected externally via networks, the equipment is subject to cyber attacks. In case of an actual cyber attack, the equipment stops operating or its operation becomes faulty, which may disrupt normal operation of the ship;

-2. The navigation support system does not operate normally radio communications interference or DoS attacks via communication, which may pose problems for operation;

-3. The remote control functions of the main engine, rudder, or other device are damaged due to various cyber attacks, which may jeopardize the safety of operation;

-4. Terminals and information systems may be infected by a virus (malware) or opportunities for external attacks may be created due emails;

-5. If the shore information communication system receives cyber attacks, data stored in the shore system is leaked or stolen, or onboard systems receive attacks via the shore system, which may disrupt normal operation of the ship;

-6. Inappropriate configuration changes are made in onboard systems due to human errors, or the ship's personnel unintentionally embed cyber attacks, which may disrupt normal operation of the ship.

1.3.2 Cyber risk management

In operation of ships, cyber security means the activities performed in the company and onboard the ship to ensure the safety of operation and maintain proper implementation of shipboard operations by protecting equipment, information communication devices (including information systems, terminals, and network devices), networks, and information related to operation from threats.

An incident means a situation where a threat manifests as a specific phenomenon and disrupts the safety of operation or proper implementation of shipboard operations. Measures should be taken to ensure safety in case of each of the potential incidents.

Cyber risk management in operation of the ship is a series of activities to set and achieve goals regarding the safety of operation and proper implementation of shipboard operations. Cyber risk management includes the following processes:

- Understanding of the context
- Risk assessment
- Risk treatment

-1. Understanding of the context

The following context should be understood and documented about the ship.

(1) Onboard equipment and its specifications

Such equipment includes the main engine, steering gear, navigation support systems, generators, equipment for cargo handling management, and equipment for responding to emergencies, etc. Information to be understood and documented includes:

(a) Use of ICT in each equipment;

(b) Support of remote control functions and automatic control functions.

(2) Onboard information communication devices (including information systems, terminals, and network devices) and their specifications

(3) Network configuration and use of communication

Equipment and information communication devices connected to networks, communication protocol and messages communicated, ship-to-shore network connections via the internet, etc. should be included.

[Reference: IACS Recommendations, No. 156 (Sep 2018) Network Architecture, No. 159 (Sep 2018) Network security of onboard computer based systems]

-2. Risk assessment

For risk assessment processes, JIS Q 31000:2010 Risk management-Principles and guidelines should be referred to.

(1) Cyber risk identification

Cyber risks that may affect equipment, information communication devices, and information related to operation of the ship should be identified and described. When identifying cyber risks, information about the latest cyber security in the industry should be obtained, and persons with accurate knowledge about cyber security should participate. "Annex 2 Applications of ICT and Cyber Risks in the Maritime Field" provides examples of risk identification in typical information systems.

(2) Cyber risk analysis

For each of the identified cyber risks, its probability and effects should be examined. Analysis results may vary significantly depending on the business circumstances of the target, such as the type of the ship/cargo, scheduled course, etc. In addition, dependencies between cyber risks should be clarified to organize information for cyber risk evaluation.

(3) Cyber risk evaluation

Based on the analysis results, risks that need to be treated and their priorities should be examined. The Company should clarify the differences from the pre-defined risk criteria and examine the need for treatment of each of the risks. The risk criteria include the guidelines for evaluating the severity of risks (ISO/IEC 31000). Effects from standards and laws should also be taken into account.

-3. Risk treatment

The Company should determine the details of risk treatment based on the result of risk assessment. For risk treatment, all controls that are required must be selected and implemented. Part 2 describes the controls and implementation procedures. Part of the controls should be implemented during shipbuilding because they involve equipment and information communication devices related to operation of the ship. Therefore, the controls are divided into those to be implemented in shipbuilding and those to be implemented in operation. Chapter 2 lists the controls in shipbuilding. In addition to the organizational controls for the company, shore-based controls for supporting operation of the ship are also essential for the operation of the ship. Therefore, Chapter 3 lists the controls for the company in operation, and Chapter 4 lists the controls for the ship in operation.

Chapter 2 CONTROLS IN SHIPBUILDING

2.1 Functions and Operation for Cyber Security

Objective

To protect the ship from threats including cyber attacks by implementing controls selected in "Risk treatment" (1.3.2 -3) for cyber security in shipbuilding.

2.1.1 Design of functions and operation for cyber security

-1. Control

The Company should design and document functions and operation for total cyber security for onboard equipment, information communication devices (including information system, terminals, and network devices), and networks, as well as areas where they are sited.

[Reference: IACS Recommendations, No. 160 (Nov 2018) Vessel System Design]

-2. Implementation guidance

Functions and operation to deal with cyber risks should be designed and documented for the entirety of onboard equipment, information communication devices, and networks. The document is called the Design Philosophy Document (DPD).

The Company should conduct the processes of risk assessment and risk treatment for cyber security in shipbuilding and determine required controls (1.3). Requirements related to system configuration, such as device redundancy and network segregation, should be determined as controls. In addition, measures for each of equipment, information communication devices, and networks should be substantiated as controls (1.3, 2.2, 2.3, and 2.4). The processes of risk assessment and risk treatment for cyber security constitute the process of designing functions and operation for total cyber security in shipbuilding.

The Design Philosophy Document should include, for example:

(1) Onboard equipment, information communication devices, and networks;

(2) System categories of equipment and information communication devices (see "Annex D18.1.1 System categories" in Part D of the Guidance for the Survey and Construction for Steel Ships (2018)).

(3) Safety requirements determined taking into account system categories;

(4) Requirements based on treaties, rules, and regulations;

(5) Presumptions about the knowledge and skills of the ship's personnel;

(6) Presumptions about system architecture, e.g. avoidance of single point of failure;

(7) Functions and operation for cyber security that are consistent with the requirements and presumptions and determined through risk assessment and risk treatment.

Functions and operation for cyber security should be substantiated further by examining the controls listed below in this chapter and other controls.

The Company may delegate this control to the system integrator, etc.

2.1.2 Implementation of functions for cyber security

-1. Control

The Company should implement functions for total cyber security for onboard equipment, information communication devices, and networks, as well as areas where they are sited.

[Reference: IACS Recommendations, No. 160 (Nov 2018) Vessel System Design]

-2. Implementation guidance

The functions designed based on "2.1.1 Design of functions and operation for cyber security" should be implemented in equipment, information communication devices, and networks.

2.1.3 Inventory list of equipment, etc.

-1. Control

The Company should create and maintain an inventory list of onboard equipment, information communication devices, and networks.

[Reference: IACS Recommendations, No. 161 (Sep 2018) Inventory List of computer based systems]

-2. Implementation guidance

In shipbuilding, an inventory list of onboard equipment, information communication devices, and networks should be created and maintained as they are determined. The inventory list should include information that identifies them, location, and network configuration. Such information provides the basis to determine related controls and their implementation methods.

If equipment and information communication devices have software installed, information that identifies software, version, and updates and patches applied should be recorded. The information is used to manage the application of patches when software vulnerabilities are released and patches are distributed.

2.2 Equipment

Objective

To ensure cyber security controls for equipment to defend against threats including cyber attacks to onboard equipment.

2.2.1 Equipment selection

-1. Control

The Company should select onboard equipment with cyber security controls.

-2. Implementation guidance

Onboard equipment includes the main engine, steering gear, navigation support systems, generators, equipment for cargo handling management, and equipment for responding to emergencies, etc. If such equipment has remote operation or automation functions, communication and software control for such functions may pose vulnerabilities to external attacks.

The networks for communication channels for remote operation and automation should be properly segmented and isolated from networks used for other purposes.

For equipment with software (including firmware), the need for application of software updates and security patches should be determined. Equipment for which required updates and security patches will be provided and applicable on an ongoing basis should be selected. Upon selection, when and who will apply updates and patches should be determined. For example, the application of updates and patches may be performed by a contract maintenance service for the equipment while the ship is in port.

[Reference: IACS Recommendations, No. 153 (Sep 2018) Recommended procedures for software maintenance of computer based systems on board]

Functions for cyber security controls to be employed may vary depending on the equipment and include:

(1) Selecting security configuration according to the use of the equipment;

(2) Having anti-virus functions or allowing anti-virus software to be installed;

(3) Performing monitoring useful for detection of anomalies, detection of incidents, and understanding of the context;

(4) Collecting logs useful for detection of anomalies, detection of incidents, and understanding of the context;

(5) Allowing for the implementation of isolation of the equipment from networks and contingency plans if detected anomalies or incidents are serious for operation of the ship.

2.2.2 Equipment configuration

-1. Control

The Company should identify and implement security configuration required for onboard equipment.

-2. Implementation guidance

Required security configuration may vary depending on the equipment and include:

(1) Adopting the latest version of software and applying security patches;

(2) Selecting embedded system configuration that ensures security according to the use of the equipment;

(3) Taking vulnerability measures including blocking unused communication ports;

(4) Employing anti-virus measures;

(5) Enabling monitoring useful for detection of anomalies, detection of incidents, and understanding of the context;

(6) Enabling collection of logs useful for detection of anomalies, detection of incidents, and understanding of the context;

(7) Enabling functions for the implementation of contingency plans to respond to serious anomalies or incidents detected.

2.2.3 Equipment siting

-1. Control

The Company should site equipment to reduce the risks from environmental threats, and opportunities for unauthorized access.

-2. Implementation guidance

The following examples should be considered to site equipment properly:

(1) Equipment should be sited to minimize unnecessary access into work areas;

(2) Storage facilities should be secured to avoid unauthorized access;

(3) Items requiring special protection should be sited and protected separate from other items;

(4) Controls should be adopted at the equipment location to minimize the risk of potential physical and environmental threats, e.g. water (or water supply failure), dust, vibration, electrical supply interference, communications interference, electromagnetic radiation and vandalism;

(5) Environmental conditions, such as temperature and humidity, should be monitored for conditions which could adversely affect the operation of the equipment location;

(6) The use of special protection methods, such as keyboard membranes, should be considered for equipment in industrial environments.

2.2.4 Implementation of manual control functions in equipment

-1. Control

For onboard equipment controlled remotely or automatically, manual control functions should be implemented in case that the control becomes impossible.

-2. Implementation guidance

The main engine, rudder, and other equipment are controlled by management systems in distant areas such as the bridge, or automatically controlled by the software embedded in the equipment. To ensure the operation of such equipment, manual control functions that are independent of the management systems or embedded software should be implemented in the equipment.

[Reference: IACS Recommendations, No. 154 (Sep 2018) Recommendation concerning manual / local control capabilities for software dependent machinery systems]

2.3 Information Communication Devices

Objective

To ensure cyber security for information communication devices to defend against threats including cyber attacks that exploit the vulnerabilities of onboard information communication devices.

2.3.1 Information communication device selection

-1. Control

The Company should select onboard information communication devices including information systems and terminals that have functions for cyber security controls and allow for the configuration and implementation of cyber security controls.

-2. Implementation guidance

Information communication devices include information systems, terminals, and network devices.

Onboard information communication devices for which software updates and security patches will be provided and applicable on an ongoing basis should be selected. Upon selection, when and who will apply updates and patches should be determined. For example, the application of updates and patches may be performed by a contract maintenance service for the information communication device while the ship is in port.

[Reference: IACS Recommendations, No. 153 (Sep 2018) Recommended procedures for software maintenance of computer based systems on board]

Functions for cyber security controls to be employed include:

(1) Selecting security configuration according to the use of the information communication device;

(2) Having anti-virus functions or allowing anti-virus software to be installed;

(3) Allowing for monitoring useful for detection of anomalies, detection of incidents, and understanding of the context;

(4) Collecting logs useful for detection of anomalies, detection of incidents, and understanding of the context;

(5) Allowing for the implementation of termination of network connections and contingency plans if detected anomalies or incidents are serious for operation of the ship.

2.3.2 Information communication device configuration

-1. Control

The Company should identify and implement security configuration required for onboard information communication devices.

-2. Implementation guidance

Required security configuration includes:

(1) Adopting the latest version of software and applying updates and security patches;

(2) Taking vulnerability measures including blocking unused communication ports;

(3) Employing anti-virus measures;

(4) Enabling monitoring useful for detection of anomalies, detection of incidents, and understanding of the context;

(5) Enabling collection of logs useful for detection of anomalies, detection of incidents, and understanding of the context;

(6) Enabling functions for the implementation of contingency plans to respond to serious anomalies or incidents detected.

2.3.3 Information communication device siting

-1. Control

The Company should site information communication devices to reduce the risks from environmental threats, and opportunities for unauthorized access.

-2. Implementation guidance

The following examples should be considered to site information communication devices properly:

(1) Information communication devices should be sited to minimize unnecessary access into work areas;

(2) Storage facilities should be secured to avoid unauthorized access;

(3) Controls should be adopted at the device location to minimize the risk of potential physical and environmental threats, e.g. water (or water supply failure), dust, vibration, electrical supply interference, communications interference, electromagnetic radiation and vandalism;

(4) Environmental conditions, such as temperature and humidity, should be monitored for conditions which could adversely affect the operation of the device location;

(5) The use of special protection methods, such as keyboard membranes, should be considered for information communication devices in industrial environments.

2.4 Networks

Objective

To ensure cyber security controls for networks to defend against threats including cyber attacks that exploit the vulnerabilities of onboard networks.

2.4.1 Network design

-1. Control

The Company should design cyber security controls for onboard networks.

-2. Implementation guidance

Cyber security controls for onboard networks should be designed based on risk management taking into account:

(1) Equipment and information communication devices connected to networks and their functions;

(2) Need for and content of communication between equipment and information communication devices;

(3) Need for and content of outboard communication of equipment and information communication devices;

(4) Threats and vulnerabilities related to communication.

Controls for networks include:

(5) Physical protection of networks and information communication devices;

(6) Encryption of communication;

(7) Partitioning of networks and network segments;

(8) Communication filtering and communication channel control with firewalls, switches, etc.;

(9) Anti-virus measures;

(10) Authentication for network access;

(11) Prevention, notification, and logging of unauthorized intrusions by intrusion prevention systems (IPSs).

[Reference: IACS Recommendations, No. 156 (Sep 2018) Network Architecture, No. 159 (Sep 2018) Network security of onboard computer based systems, No. 162 (Sep 2018) Integration]

Especially for the following equipment related to navigational safety, controls should be determined by carefully examining cyber risks associated with ship-shore communication and communication for control:

(12) Bridge systems/navigation support systems

(13) Main engine control system

(14) Bridge maneuvering

(15) Steering gear/heading control systems

(16) Electronic chart display systems

(17) Cargo control

(18) Ballast control

[Reference: IACS Recommendations, No. 164 (Nov 2018) Communication and Interfaces]

2.4.2 Implementation of networks

-1. Control

The Company should implement cyber security controls for onboard networks.

-2. Implementation guidance

Cyber security controls for onboard networks should be implemented based on the design (2.4.1).

2.5 Information

Objective

To provide protection for information related to operation control/management and shipboard operations according to the use and importance of information to defend against threats including cyber attacks.

2.5.1 Protection of information

-1. Control

The Company should determine requirements for protection of information (Note) related to operation of the ship, and design and implement safeguards.

[Reference: IACS Recommendations, No. 157 (Sep 2018) Data assurance]

Note: "Data" in the IACS Recommendation No. 157 is referred to as "information" in 2.5.

-2. Implementation guidance

The Company should determine requirements for protection of information related to operation of the ship, and design and implement safeguards that meet the requirements. The target information is handled in onboard equipment, information communication devices, and networks.

The impact of each requirement for protection of information can be expressed as, for example, High, Moderate, or Low, in terms of confidentiality, integrity, and availability of information. Requirements for protection of information relate to system categories as defined in "Annex D18.1.1 System categories" in Part D of the Guidance for the Survey and Construction for Steel Ships (2018). The IACS Recommendations No. 157 (Sep 2018) Data assurance shows the relations between system categories I, II, and III and confidentiality, integrity, and availability as shown below. The categorization may be used when determining requirements for protection of each type of information onboard the ship.

System category	Confidentiality	Integrity	Availability
I	Low	Moderate	Low
II	Moderate	High	Moderate
III	Moderate	High	High

Information safeguards should be implemented with functions and operation for cyber security for onboard equipment, information communication devices, and networks that handle the information (2.2, 2.3, and 2.4).

Information includes information at rest in equipment or information communication device and information in transit depending on the status. Controls such as access control and encryption should be determined and implemented for each type.

2.6 Access Control

Objective

To restrict access to information related to operation control/management and shipboard operations, as well as onboard equipment, information communication devices, and networks.

2.6.1 Access control policy

-1. Control

The Company should establish, document, and review an access control policy based on business security requirements.

-2. Implementation guidance

Access controls are both logical and physical (2.7) and these should be considered together. The Company should give a clear statement of the business requirements to be met by access controls.

The access control policy should take into account the following:

(1) Security requirements of business applications;

(2) Consistency between the access rights and information classification policies of different information systems and networks;

(3) Management of access rights in a networked environment;

(4) Segregation of access control roles, e.g. access request, access authorization, access administration;

(5) Requirements for formal authorization of access requests;

(6) Removal of access rights;

(7) Archiving of records of all significant events concerning the use and management of user identities and access authentication information;

(8) Roles with privileged access.

2.6.2 Access to networks

-1. Control

The Company should provide users with access to the network (including network services) that they have been specifically authorized to use.

-2. Implementation guidance

A policy should be formulated concerning the use of networks. This policy should cover:

(1) The networks which are allowed to be accessed;

(2) Authorization procedures for determining who is allowed to access which networks;

(3) Management controls and procedures to protect access to network connections;

(4) The means used to access networks (e.g. use of VPN or wireless network);

(5) User authentication requirements for accessing various network services;

(6) Monitoring of the use of network services.

2.6.3 User registration and de-registration

-1. Control

A formal user registration and de-registration process should be implemented to enable assignment of access rights.

-2. Implementation guidance

The process for managing user IDs should include:

(1) Using unique user IDs to enable users to be linked to and held responsible for their actions; the use of shared IDs should only be permitted where they are necessary for business or operational reasons and should be approved and documented;

(2) Immediately disabling or removing user IDs of users who have left the organization;

(3) Periodically identifying and removing or disabling redundant user IDs;

(4) Ensuring that redundant user IDs are not issued to other users.

2.6.4 Management of privileged access rights

-1. Control

The Company should restrict and control the allocation and use of privileged access rights.

-2. Implementation guidance

The allocation of privileged access rights should be controlled through a formal authorization process in accordance with the relevant access control policy (2.6.1).

2.6.5 Management of access authentication information of users

-1. Control

The Company should control the allocation of access authentication information through a formal management process.

-2. Implementation guidance

The allocation of access authentication information should take into account the following:

(1) When users are required to maintain their own access authentication information they should be provided initially with secure temporary access authentication information, which they are forced to change on first use;

(2) Procedures should be established to verify the identity of a user prior to providing new, replacement or temporary access authentication information;

(3) Temporary access authentication information should be given to users in a secure manner; the use of external parties or unprotected (clear text) electronic mail messages should be avoided;

(4) Temporary access authentication information should be unique to an individual and should not be guessable;

(5) Users should acknowledge receipt of access authentication information;

(6) Default vendor access authentication information should be altered following installation of systems or software.

2.6.6 Removal or adjustment of access rights

1. Control

The Company should remove the access rights to information, information communication devices, and networks upon termination of employment, contract or agreement, or adjust upon change.

-2. Implementation guidance

Upon termination, the access rights of an individual to information and assets associated with information communication devices and networks should be removed or suspended. Changes of employment should be reflected in removal of all access rights that were not approved for the new employment. The access rights that should be removed or adjusted include those of physical and logical access. Removal or adjustment can be done by removal, revocation or replacement of keys, identification cards, information processing facilities or subscriptions. Any documentation that identifies access rights of employees and contractors should reflect the removal or adjustment of access rights. If a departing employee or external party user has known access authentication information for user IDs remaining active, it should be changed upon termination or change of employment, contract or agreement.

2.6.7 Secure log-on procedures

-1. Control

Where required by the access control policy, the Company should control access to information, equipment, information communication devices, and networks by a secure log-on procedure.

-2. Implementation guidance

A suitable authentication technique should be chosen to substantiate the claimed identity of a user. Where strong authentication and identity verification is required, authentication methods such as cryptographic means, smart cards, token devices or biometric means should be used in combination with passwords.

The log-on procedure should be designed to minimize the opportunity for unauthorized access. The log-on procedure should therefore disclose the minimum of information about the system or application, in order to avoid providing an unauthorized user with any unnecessary assistance.

2.6.8 Remote access and remote update

-1. Control

The Company should create a cyber security policy and implement controls for remote access and remote update for onboard equipment and information communication devices.

-2. Implementation guidance

Equipment and information communication devices may be accessed remotely to:

(1) Monitor the states of the equipment and information communication devices;

(2) Diagnose the states of the equipment and information communication devices;

(3) Update software and data in the equipment and information communication devices.

Such accesses and processes involve the following threats:

(4) Communication channels used for access may be exploited, resulting in intrusions or other attacks;

(5) Administrative rights assigned for monitoring and diagnosis or other access rights may be exploited, or erroneous operations may be performed with the access rights, impairing normal operations of the equipment or information communication device;

(6) Software or data update process may fail, impairing normal processing of the equipment or information communication device;

(7) Updated software or data may contain errors or other problems, impairing normal processing after the update;

(8) The equipment or information communication device may be infected by a virus as a result of an update of software or data.

To counter these threats, cyber security controls for remote update and remote access should be created and implemented.

Controls include:

(9) Identification of the target equipment and information communication devices and processes to be implemented;

(10) Authentication for access and communication as well as encryption of access control and communication;

(11) Identification of parties/persons and specification of the responsible person;

(12) Operational management for implementation, such as advanced application and training;

(13) Collection and checking of implementation records.

[Reference: IACS Recommendations, No. 163 (Sep 2018) Remote Update / Access]

2.7 Physical Controls

Objective

To ensure physical cyber security controls including control of areas to defend against erroneous operation, destruction, damage, and other threats to onboard equipment, information communication devices, and networks.

2.7.1 Areas

-1. Control

The Company should specify areas onboard the ship for cyber security controls and implement physical controls for the areas.

[Reference: IACS Recommendations, No. 158 (Oct 2018) Physical Security of onboard computer based system]

-2. Implementation guidance

A policy for physical controls for areas should be created. The policy should define, for example:

(1) Specification of areas appropriate for equipment, information communication devices, and networks;

(2) Who has permission to access areas and when they can access.

Physical controls for areas should be determined and implemented. Physical controls for areas include:

(3) Building perimeter walls around the areas to restrict access;

(4) Installing a lock on the doors into the areas to restrict access;

(5) Collecting logs related to the use of keys to record entries;

(6) Managing access to the records to protect them.

2.7.2 Physical protection of equipment, information communication devices, and networks

-1. Control

The Company should determine and implement physical controls to protect equipment, information communication devices, and networks.

[Reference: IACS Recommendations, No. 158 (Oct 2018) Physical Security of onboard computer based system]

-2. Implementation guidance

Physical controls to protect equipment, information communication devices, and networks include:

(1) Siting equipment, information communication devices, and networks in areas with appropriate physical controls;

(2) Duplicating power systems, communication facilities, and air conditioning systems as required to ensure their operations;

(3) Prohibiting unauthorized removal of equipment.

2.8 Contingency Plan

Objective

To reduce damage caused by emergency situations by planning response in preparation for emergency situations relating to cyber security.

2.8.1 Development of the contingency plan

-1. Control

The Company should develop a contingency plan for cyber security.

[Reference: IACS Recommendations, No. 155 (Sep 2018) Contingency plan for onboard computer based systems]

-2. Implementation guidance

The Contingency Plan should include the following information:

(1) List of systems and information communication devices covered by the Contingency Plan;

(2) Incident response plan;

(3) Recovery plan;

When developing a contingency plan, target equipment and information communication devices should be determined and a list should be created. The determination should be based on the importance of the equipment or information communication device in safety of operation and the effects of potential incidents. In addition, the provisions of industry guidelines should be taken into account.

The incident response plan should include the following information:

(1) Types and descriptions of potential incidents;

(2) Shore and onboard contact systems and messages;

(3) Coordination with external entities including service providers;

(4) Measures taken in case of an incident;

The recovery plan should include the following information:

(1) Procedures for restoring systems and information communication devices;

(2) Procedures for restoring information;

(3) Coordination with external entities including service providers;

The developed contingency plan should be tested and verified in the Company and onboard the ship. In addition, necessary improvements should be reflected.

The contingency plan should be kept in the Company and onboard the ship.

2.9 Supplier Relationships

Objective

To ensure enforcement and implementation of cyber security controls to defend against threats including cyber attacks to operation related to outsourced operations and procured equipment and devices in shipbuilding.

2.9.1 Provision of cyber security requirements in supplier relationships

-1. Control

The provider should require the supplier to comply with the requirements for cyber security when outsourcing or procuring operations for shipbuilding.

-2. Implementation guidance

The Company, the owner or manager of the ship, outsources shipbuilding to a system integrator. The system integrator procures onboard equipment, information communication devices, and networks from suppliers and outsources construction of them to suppliers.

This control applies to the Company and system integrator which outsource and/or procure part of operations in shipbuilding. The Company, as the owner of the ship, should require the system integrator to implement this control via contracts with the system integrator.

For outsourcing of operations for shipbuilding, the outsourcing contract may include the following as the requirements for cyber security:

(1) Functions for cyber security provided in equipment, information communication devices, and networks;

(2) Requirements related to the work structure and work environment of the outsourcing contractor.

When determining the requirements for cyber security for the outsourcing contractor, the controls and implementation procedures related to equipment, information communication devices, and networks (2.2, 2.3, and 2.4) may be consulted.

The system integrator may procure equipment, information communication devices, and/or networks externally. In such a case, the system integrator should procure items that comply with the required cyber security requirements.

The requirements related to the work structure and work environment of the outsourcing contractor ensure the appropriateness of work at the outsourcing contractor. Appropriate structure and management are required at the outsourcing contractor to ensure the implementation and quality of the functions required in deliverables. In addition, the outsourcing contractor may be required to separate the work environment from other operations.

The provider should determine, and include in the outsourcing contract, specification documents and inspection reports to be delivered for cyber security when outsourcing shipbuilding operations.

2.9.2 Ensuring of cyber security requirements in supplier relationships

-1. Control

The provider should verify that deliverables satisfy the requirements for cyber security when procuring operations and equipment for shipbuilding.

-2. Implementation guidance

The supplier should verify that deliverables satisfy the requirements for cyber security during a receiving inspection.

Chapter 3 CONTROLS FOR THE COMPANY IN OPERATION

3.1 Preparation of Operation Rules

Objective

To ensure that the ship's personnel can implement cyber security controls against threats including cyber attacks in operation of the ship.

3.1.1 Development of operation rules

-1. Control

The Company should develop rules for cyber security in operation that are applicable to the ship's personnel.

-2. Implementation guidance

The operation rules applicable to the ship's personnel should be developed according to the implementation methods of the controls of Operation (2.1.1), Equipment (2.2), Information Communication Devices (2.3), Networks (2.4), and Physical Controls (2.5) for cyber security.

3.2 Support and Management in Operation

Objective

To ensure that the ship's personnel can implement cyber security controls against threats including cyber attacks in operation of the ship.

3.2.1 Support of operation

-1. Control

The Company should support the ship's personnel in relation to cyber security in operation.

-2. Implementation guidance

Support of the ship's personnel includes:

(1) Preparing and providing documentation required by the ship's personnel about cyber security controls for onboard equipment, information communication devices, and networks, as well as physical controls for cyber security;

(2) Developing operation rules for cyber security in operation, as well as providing and explaining the operation rules to the ship's personnel (related controls include "4.1.1 Development of operation rules");

(3) Developing a contingency plan for cyber security in operation, as well as providing and explaining the plan to the ship's personnel (related controls include "4.2.1 Implementation of the contingency plan");

(4) Preparing and providing information about cyber security that needs to be provided to the ship's personnel in addition to the operation rules and contingency plan;

(5) Communication related to cyber security in operation.

3.2.2 Management of operation

-1. Control

The Company should understand and manage the context in relation to cyber security in operation.

-2. Implementation guidance

The Company should understand and manage the context by:

(1) Understanding and managing the implementation status of controls for cyber security in operation;

(2) Understanding and managing especially the implementation status of the application of software updates and security patches to onboard equipment and information communication devices;

(3) Understanding the context of cyber security that may affect operation of the ship, including general trends of cyber attacks and cyber incidents.

3.3 Security Controls in Shore Information Communication Devices

Objective

To ensure the implementation of cyber security controls for shore information communication devices related to operation to defend against threats including cyber attacks in operation of the ship.

3.3.1 Identification of shore information communication devices

-1. Control

The Company should identify shore information communication devices including information systems and terminals related to cyber security in operation of the ship.

-2. Implementation guidance

Companies have information communication devices including information systems and terminals for various operations. Among the information communication devices, the Company should identify the ones related to cyber security in operation of the ship. Such information communication devices include:

(1) Devices that manage documents on the functions and operation for cyber security onboard the ship, including the specifications of onboard equipment, information communication devices, and networks;

(2) Devices that manage the status of cyber security controls in operation of the ship;

(3) Devices for communications between the ship and Company in operation.

3.3.2 Configuration of shore information communication devices

-1. Control

The Company should implement security controls including identification and implementation of security configuration required for shore information communication devices related to cyber security in operation of the ship.

-2. Implementation guidance

Security controls should be designed and implemented for the shore information communication devices identified above.

Especially, security configuration required for information communication devices includes:

(1) Adopting the latest version of software and applying updates and security patches;

(2) Taking vulnerability measures including blocking unused communication ports;

(3) Employing anti-virus measures;

(4) Performing monitoring useful for detection of anomalies, detection of cyber incidents, and understanding of the context;

(5) Collecting logs useful for detection of anomalies, detection of cyber incidents, and understanding of the context;

(6) Allowing for the implementation of contingency plans to respond to serious anomalies or incidents detected.

3.4 Logging and Monitoring

Objective

To detect and properly respond to events relating to cyber security in early stages and secure information for post-investigations

3.4.1 Monitoring of cyber security in operation

-1. Control

The Company should monitor events related to cyber security for the ship in operation.

-2. Implementation guidance

The Company should record events defined in Equipment (2.2), Information Communication Devices (2.3), Networks (2.4), and Physical Controls (2.5) onboard the ship in operation. Logs recording events should be protected from tampering and unauthorized access.

3.5 Contingency Plan

Objective

To reduce damage caused by emergency situations by ensuring that the Company responds to emergency situations relating to cyber security onboard the ship in operation according to a contingency plan.

3.5.1 Implementation of the contingency plan

-1. Control

The Company should take actions according to the defined contingency plan in case of an incident onboard the ship in operation.

[Reference: IACS Recommendations, No. 155 (Sep 2018) Contingency plan for onboard computer based systems]

-2. Implementation guidance

The Company should take actions according to the defined contingency plan when detecting an incident that may affect operation of the ship during event monitoring.

The Company should conduct training timely according to the incident response and recovery plans to ensure the implementation of these plans.

Chapter 4 CONTROLS FOR SHIPS IN OPERATION

4.1 Management of Equipment, Information Communication Devices, and Networks

Objective

To defend against threats including cyber attacks by ensuring the implementation of operations for cyber security onboard the ship in operation.

4.1.1 Development of operation rules

-1. Control

The ship's personnel should implement the defined operation rules for cyber security in operation.

-2. Implementation guidance

The ship's personnel should carry out operations relating to cyber security in equipment, information communication devices, and networks according to the defined operation rules (3.1.1).

4.1.2 Application of software updates and security patches

-1. Control

The Company or the ship's personnel should apply software updates and security patches to onboard equipment and information communication devices according to the defined procedures.

-2. Implementation guidance

The application of software (including firmware) updates and security patches may be performed while the ship is in port, where a required transmission speed can be ensured. The application of updates and patches may be performed by a contract maintenance service, for example, according to the defined procedures. Even when updates and/or patches with a particularly high need to be applied are issued, an extremely careful decision should be made about the application onboard the ship, and it should be avoided in principle. It should be considered that no expert support is available for application, the operation of the equipment or information communication device must be stopped for application, and the transmission speed for communication to obtain updates or patches is limited.

[Reference: IACS Recommendations, No. 153 (Sep 2018) Recommended procedures for software maintenance of computer based systems on board]

The persons who perform the updating of software and application of security patches should be specified in advance. It may be outsourced to external services by the Company.

4.2 Contingency Plan

Objective

To reduce damage caused by emergency situations by ensuring that the ship's personnel respond to emergency situations relating to cyber security onboard the ship in operation according to a contingency plan.

4.2.1 Implementation of the contingency plan

-1. Control

The ship's personnel should take actions according to the defined contingency plan in case of an incident onboard the ship in operation.

[Reference: IACS Recommendations, No. 155 (Sep 2018) Contingency plan for onboard computer based systems]

-2. Implementation guidance

The ship's personnel should take actions according to the defined contingency plan in case of an incident.

The ship's personnel should be trained timely according to the incident response and recovery plans to ensure the implementation of these plans.

Annex

1 Reference

(1) IACS Recommendations, No. 153 (Sep 2018) Recommended procedures for software maintenance of computer based systems on board

(2) IACS Recommendations, No. 154 (Sep 2018) Recommendation concerning manual / local control capabilities for software dependent machinery systems

(3) IACS Recommendations, No. 155 (Sep 2018) Contingency plan for onboard computer based systems

(4) IACS Recommendations, No. 156 (Sep 2018) Network Architecture, No. 159 (Sep 2018) Network security of onboard computer based systems

(5) IACS Recommendations, No. 157 (Sep 2018) Data assurance

(6) IACS Recommendations, No. 158 (Oct 2018) Physical Security of onboard computer based system

(7) IACS Recommendations, No. 159 (Sep 2018) Network security of onboard computer based systems

(8) IACS Recommendations, No. 160 (Nov 2018) Vessel System Design

(9) IACS Recommendations, No. 161 (Sep 2018) Inventory List of computer based systems

(10) IACS Recommendations, No. 162 (Sep 2018) Integration

(11) IACS Recommendations, No. 163 (Sep 2018) Remote Update / Access

(12) IACS Recommendations, No. 164 (Nov 2018) Communication and Interfaces

(13) JIS Q 27001:2014 Information technology-Security techniques-Information security management systems-Requirements

(14) JIS Q 31000:2010 Risk management-Principles and guidelines

2 Applications of ICT and Cyber Risks in the Maritime Field

	I. Applications of ICT	II. Equipment	III. Communication	IV. Event 1: Action, equipment state, natural phenomenon, etc.	V. Event 2: Direct cause of results	VI. Risk
1. Navigation systems						
1-1	Bridge systems, navigation support systems - Display of maps, position, course, and other ships - Navigation instruction - Navigation control	GPS Compass	Obtains GPS position information.	GPS position information is disrupted	Radio waves interfering with high-frequency transmission of the Doppler speed log and signals from GPS satellites (Protection from armed attacks using GPS signals)	Correct position information cannot be used Correct direction information cannot be used Heading control cannot be performed
1-2		Gyro Compass	Makes corrections with the ship's speed information from the Doppler speed log and GPS position information.	High-frequency transmission of the Doppler speed log or GPS position information is disrupted		
1-3		Heading Control System	Obtains GPS position information. Obtains direction information from the gyro compass.	High-frequency transmission of the Doppler speed log or GPS position information is disrupted		
1-4		Voyage Data Recorder	Records voyage data such as GPS position, speed, data from heading control systems, etc.	(1) High-frequency transmission of the Doppler speed log or GPS position information is disrupted (2) Accumulated data is exploited	Radio waves interfering with high-frequency transmission of the Doppler speed log and signals from GPS satellites Intrusion via the real time monitor (optional function)	Correct voyage data cannot be accumulated
1-5		Echo Sounder	Measures water depth by sending and receiving sound waves from the ship's bottom.	Sound waves are disrupted	Sound wave interference	Correct water depth cannot be measured, resulting in an increase risk of grounding
1-6		Doppler Speed Log	Measures the ship's speed by sending and receiving high-frequency waves.	High-frequency transmission is disrupted	High-frequency transmission interference	Correct speed cannot be measured, affecting ship handling
1-7		Radar	Measures the bearing and distance of the target by sending and receiving radar waves.	Radar waves are disrupted	Radar wave interference	Ship's surroundings cannot be assessed
1-8		Electronic Chart Display and Information System (ECDIS)	(1) Displays GPS position information on the electronic chart. (2) Uses the internet and USB for installing and updating electronic charts.	GPS position information is disrupted Malware infection	Radio waves interfering with signals from GPS satellites Virus infection due to internet connection or USB use	Ship's position becomes unknown, affecting ship handling
1-9		GPS (Global Positioning System)	Receives position information from satellites.	GPS position information is disrupted	Radio waves interfering with signals from GPS satellites	Ship's position becomes unknown, affecting ship handling

	I. Applications of ICT	II. Equipment	III. Communication	IV. Event 1: Action, equipment state, natural phenomenon, etc.	V. Event 2: Direct cause of results	VI. Risk
1-10		AIS (Automated Identification System)	Automatically sends information including ship name, ship position, course, etc. to other ships in the vicinity and land stations via international VHF frequencies.	International VHF frequencies are disrupted	VHF wave interference	Information about other ships becomes unknown, affecting ship handling
1-11		BNWAS (Bridge Navigational Watch Alarm System)	Optionally connects with navigation facilities such as ECDIS.	Virus infection occurs via ECDIS.	Virus infection occurs via ECDIS.	Officer falling asleep on duty may be overlooked, which may cause a dangerous situation
2. Engine systems						
2-1	Automation of engine operation	Main Engine Control System Boilers	Performs automatic monitoring and sends information via the internet by interfacing with the fuel management system.	An attacker hacks into the system and steals information for attacks	Fraudulent information is fed to the engine control system as input	Normal operation of the engine is disrupted
2-2			Connects with the main engine control system.			
2-3		Bridge Maneuvering	Connects to networks for remote maneuvering from the bridge.			
3. Steering						
3-1	Computerized steering instructions	Steering Gear	Connection with the heading control system	Invalid steering signals are entered	Connection with the heading control system	Accurate steering cannot be performed
4. Cargo handling management						
4-1	Cargo loading	Loading Computer	Communicates ship-to-shore via the internet.	An attacker hacks into the system and steals information for attacks Malware infection	Fraudulent information is fed to the system as input Malware infection	Cargo information is leaked Ship's conditions become off balance and stability is lost, resulting in an increased risk of rollover
4-2	Maintenance of the ship's conditions	Ballast Water Management System	Communicates ship-to-shore via the internet.			Movement and spreading of aquatic organisms increase
4-3		Cargo Control	Controls temperature and pressure of liquefied gas bulk carriers. Controls temperature and atmosphere of cold storage warehouses.	Boil off gas increases Perishable cargoes are spoiled	Increased temperature and pressure of liquefied gas cargoes Increased temperature and oxygen concentration of cold storage warehouses	Cargo volume decreases Cargo value decreases
4-4		Ballast Control	Obtains information regarding the ballast tank, such as water level, draft, inclination, etc.	Wrong information is entered	Virus infection	Ship's conditions become off balance and stability is lost, resulting in an increased risk of rollover

	I. Applications of ICT	II. Equipment	III. Communication	IV. Event 1: Action, equipment state, natural phenomenon, etc.	V. Event 2: Direct cause of results	VI. Risk
5. Information communication						
5-1	Transmission and reception of information via email, etc.	VSAT (Very Small Aperture Terminal) /INMARSAT	Sends/receives emails and accesses the web via satellite communications (Inmarsat, etc.).	Malware, ATP attacks, etc. (same as potential attacks and abnormal states in outboard use of the internet)	PCs/servers are infected by malware PCs/servers are hacked or operated by an attacker	Information is leaked Communication with the company and other ships is lost or delayed Operations using PCs or servers are disrupted
6. Emergency response						
6-1	Distress response	GMDSS (Global Maritime Distress and Safety System)	Establishes internet connections via Inmarsat.	An attacker sends a fraudulent distress signal	Fraudulent information is fed to the system as input	Fraudulent distress signals are sent Distress signals from other ships cannot be received
6-2	Fire response	Fire Detection System	Does not connect with communication systems.	Fire	Malware infection	Fire detection system malfunctions
7. Software systems						
7-1	Email software	Onboard LAN	Communication via the internet	Potential cyber attacks	Communication via the internet	Information is leaked
7-2	Chart revision software	ECDIS				Ship handling is affected
7-3	Weather information software	Onboard LAN				Ship operation plans are affected
7-4	Loading computer software	Loading Computer	Connects with the onboard LAN.	Potential malware infection	Connection with the onboard LAN	Maintenance of seaworthiness is affected
7-5	Stowage planning software	Office PC connected to onboard LAN				Maintenance of seaworthiness is affected
7-6	Maintenance programs	Engine control room/ office PC connected to onboard LAN				Normal operation of the engine is affected
7-7	Fuel control programs	Engine control room/office PC connected to onboard LAN	Communication via the internet	Potential cyber attacks	Communication via the internet	Fuel-efficient operation is affected

Acknowledgments

We would like to express our deepest appreciation to the following committee members and working group members for their guidance and support in the preparation of the Guidelines.

List of Development Committee Members

(titles omitted; in no particular order)

Chairman:

Ken Takagi	Professor, Department of Ocean Technology, Policy and Environment, Graduate School of Frontier Sciences, The University of Tokyo

Committee members:

Shoji Kawano	Chief Security Officer, CISSP, Microsoft Japan Co., ltd.
Koji Nakao	Distinguished Researcher, Cybersecurity Research Institute, National Institute of Information and Communications Technology
Shin Yamashita	Technical Researcher, Cybersecurity Laboratory, Cybersecurity Research Institute, National Institute of Information and Communications Technology
Hirofumi Takano	Senior Corporate Officer, Director of Innovation Development Division, ClassNK
Toshiro Arima	Corporate Officer, Director of Rule Development and ICT Division, ClassNK
Yasuhiro Ikeda	Representative Director and President, Ship Data Center

List of Working Group Members

(titles omitted; in no particular order)

Koji Nakao	Distinguished Researcher, Cybersecurity Research Institute, National Institute of Information and Communications Technology
Shin Yamashita	Technical Researcher, Cybersecurity Laboratory, Cybersecurity Research Institute, National Institute of Information and Communications Technology
Rina Goto	Patner Dev Manager, Managed Service Providers, One Commercial Partner, Microsoft Japan Co., Ltd.
Yasuhiro Ikeda	Representative Director and President, Ship Data Center

Maritime Education and Training Certification Team,
Innovation Development Division, Nippon Kaiji Kyokai

4-7, Kioi-cho, Chiyoda-ku, Tokyo 102-8567, Japan
Tel: 03-5226-2177
Fax: 03-5226-2179
E-mail: met@classnk.or.jp

www.classnk.or.jp

April 2019