

CHARTING THE FUTURE 

ClassNK

Guidelines for Cyber resilience of ships
(Edition 1.1)

[English]



Cyber
Resilience of **SHIPS**

ClassNK

Revision History

No.	Date	Revised part	Revision details
1.0	2024.7.26	---	First issue
1.1	2025.8.29	All	Revised following items: <ul style="list-style-type: none">- Application- Explanation of each document to submit

Introduction

Traditional marine systems primarily relied on physical connections and controls without considering threats such as cyber attacks. However, in recent years, these systems have become digitally interconnected through computers and the Internet. As a result, marine systems are now exposed to cyberspace, increasing the risk of cyber attacks, and some ships have already experienced actual damage. This background has brought significant attention to cybersecurity.

In April 2022, the International Association of Classification Societies (IACS) issued two new Unified Requirements (UR) for cybersecurity: UR E26 and UR E27. These URs specify requirements related to the capability to reduce the occurrence and mitigate the effects of cyber incidents due to cyber attacks and to recover quickly if such incidents occur (hereinafter referred to as "cyber resilience"). UR E26 covers ships, while UR E27 covers on-board systems and equipment. The aim of these URs is to ensure minimum cyber security of ships by providing a set of baseline requirements for cyber resilience of ships, on-board systems, and equipment. Following the publication of UR E26 and UR E27, the Nippon Kaiji Kyokai (hereinafter referred to as "the Society") has decided to incorporate these requirements into Part X of the *Rules for the Survey and Construction of Steel Ships* (hereinafter referred to as "Part X").

For the first time, cybersecurity measures have been incorporated as mandatory requirements for new ships. In response, the Society has decided to issue this Guidelines to help stakeholders understand these new requirements better in July 2024. Subsequently, following the official publication of the Rules and based on knowledge gained through their implementation, this Guidelines has been revised. The current revision aims to enhance explanations with more practical examples and implementation approaches to better support compliance with the Rules.

This *Guidelines for Cyber resilience of ships* (hereinafter referred to as "Guidelines") is [a commentary on Chapter 5, Part X \(UR E26\)](#). It primarily targets [systems integrators \(mainly shipyards\) and shipowners \(or ship management companies\)](#). Specifically, it provides guidance on the following:

- **Scope and approval process**

This Guidelines describes the procedures for obtaining approval from the Society, including the scope of application for ships and systems.

- **Requirements for documents and surveys**

This Guidelines explains in detail the requirements for cyber resilience of ships, including the specifics of documents to submit and survey items.

[Although this Guidelines contains highly specialized content on cybersecurity, the "Chapter 1 Overview" section provides a summary of basic information and the overall perspective to help you grasp the entirety.](#)

Outline

This Guidelines is intended for the following stakeholders:



Systems integrator: Refers to those responsible for security design and network construction, typically the shipyard unless otherwise contracted or designated.



Shipowner: Refers to the shipowner or the ship management company.



Chapter 1 Overview

This chapter explains the overall picture of Chapter 5, Part X (UR E26). Chapter 5, Part X (UR E26) aims to achieve the overall goal of "building ships with cyber resilience" by breaking down this goal into five functional elements, each with its own requirements. [This chapter provides a detailed explanation of the purpose and content of each of the five functional elements \(Identify, Protect, Detect, Respond, Recover\) to make them easier to understand.](#) By understanding the purpose and content of each element, the overall goal of Chapter 5, Part X (UR E26) becomes clear, and the objectives that ships need to achieve are clarified.



Systems integrator and Shipowner: Understand the overall picture of Chapter 5, Part X (UR E26).



Chapter 2 Application

This chapter explains the scope of application of Chapter 5, Part X (UR E26). Chapter 5, Part X (UR E26) defines the scope of application for ships and systems. [This chapter provides specific examples to make it clearer which ships and systems are subject to Chapter 5, Part X \(UR E26\).](#) The scope of systems and networks under Chapter 5, Part X (UR E26) is determined by network design. An example is provided to help correctly understand the scope of application.



Systems integrator: Obtain information to support network and security design by understanding the scope of application for ships and systems.



Shipowner: Understand which ships and systems are subject to Chapter 5, Part X (UR E26), particularly regarding IT equipment that may be provided (such as servers used in ECDIS and VDR. [See 2-2.2 of the Guidelines.](#)) and how it relates to Chapter 5, Part X (UR E26).



Chapter 3 Process for Compliance

This chapter explains the process of Chapter 5, Part X (UR E26). Chapter 5, Part X (UR E26) lists the stakeholders as suppliers, systems integrators, shipowners, and the Society, and requires their engagement in four phases (design, construction, commissioning, and operation). [This chapter outlines the actions that systems integrators and shipowners should take at each phase \(design, construction,](#)

[commissioning, and operation\) based on the documents to be prepared.](#) This chapter provides information on the required submission documents and surveys during the process of Chapter 5, Part X (UR E26).



Systems integrator: Clearly understand the submission documents and surveys required at each phase (especially design, construction, and commissioning) and take appropriate actions.



Shipowner: Clearly understand the submission documents and surveys required at each phase (especially during operation) and take appropriate actions.



Chapter 4 Explanation of Submission of Plans and Documents

[This chapter provides a detailed explanation of the submission documents.](#) Systems integrators are required to submit the relevant plans and documents during the registration survey during construction, and shipowners are required to submit them by the first annual survey. This chapter provides a detailed explanation of the submission of plans and documents.



Systems integrator: Understand the details of the submission plans and documents required at each phase (especially design, construction, and commissioning).



Shipowner: Understand the details of the submission plans and documents required during the operation phase.



Chapter 5 Explanation of Surveys

[This chapter provides a detailed explanation of the surveys.](#) Systems integrators are required to conduct relevant surveys during the commissioning phase, and shipowners are required to conduct them during periodic surveys. This chapter provides a detailed explanation of the surveys.



Systems integrator: Understand the details of the surveys required during the commissioning phase.



Shipowner: Understand the details of the surveys required during periodical surveys.

Contents

Chapter 1	Overview	1
Chapter 2	Application	7
2-1.	Ships in scope of Chapter 5, Part X (UR E26)	7
2-2.	Systems in scope of Chapter 5, Part X (UR E26)	8
2-2.1	Operational Technology (OT) Systems Onboard Ships	8
2-2.2	Applicable Systems other than OT Systems, Network Devices	11
2-2.3	Communication Interface Between Networks Within the Scope of Chapter 5, Part X (UR E26) and Untrusted Networks (Network Devices)	17
2-2.4	OT Systems Excluded from Application based on Risk Assessment for Exclusion of Computer-Based System from the Application of Requirements	17
Chapter 3	Process for Compliance	20
3-1.	Design and Construction Phase	20
3-2.	Commissioning Phase	23
3-3.	Operation Phase	24
Chapter 4	Explanation of Submission of Plans and Documents	26
4-1.	Vessel asset inventory	27
4-1.1	Overview	27
4-1.2	Explanation	27
4-2.	Zones and conduit diagram	32
4-2.1	Overview	32
4-2.2	Explanation	32
4-3.	Cyber security design description	39
4-3.1	Overview	39
4-3.2	Explanation	39
4-3.3	Explanation of Each Requirement in Functional Elements	39
4-4.	Risk assessment for the exclusion of computer-based systems	58
4-4.1	Overview	58
4-4.2	Explanation	58
4-5.	Description of compensating countermeasures	61
4-5.1	Overview	61
4-5.2	Explanation	61
4-6.	Ship cyber resilience test procedure	63
4-6.1	Overview	63
4-6.2	Explanation	63
4-6.3	Explanation of Each Requirement in Functional Elements	64
4-7.	Ship cyber security and resilience program	89
4-7.1	Overview	89
4-7.2	Explanation	89

4-7.3 Explanation of Each Requirement in Functional Elements	91
Chapter 5 Explanation of Surveys	126
5-1. Survey during the Commissioning Phase	127
5-2. First Annual Survey	130
5-3. Subsequent Annual Surveys / Intermediate Survey	132
5-4. Special Survey	133



Chapter 1 Overview

This chapter provides an overview to understand the entirety of Chapter 5, Part X (UR E26).

Chapter 5, Part X (UR E26) outlines the requirements for cyber resilience of ships. Cyber resilience refers to the capability to reduce the occurrence of and mitigate the effects of operational technology (OT) disruptions on ships caused by cyber attacks or other threats, thereby safeguarding human and ship safety as well as the environment. Additionally, it includes the ability to quickly recover from such disruptions when they occur. The aim of Chapter 5, Part X (UR E26) is to [equip ships with these capabilities, making them resistant to cyber attacks or other threats](#).

To ensure cyber resilience on ships, Chapter 5, Part X (UR E26) is divided into [five functional elements: Identify, Protect, Detect, Respond, and Recover](#), each with its specific requirements.

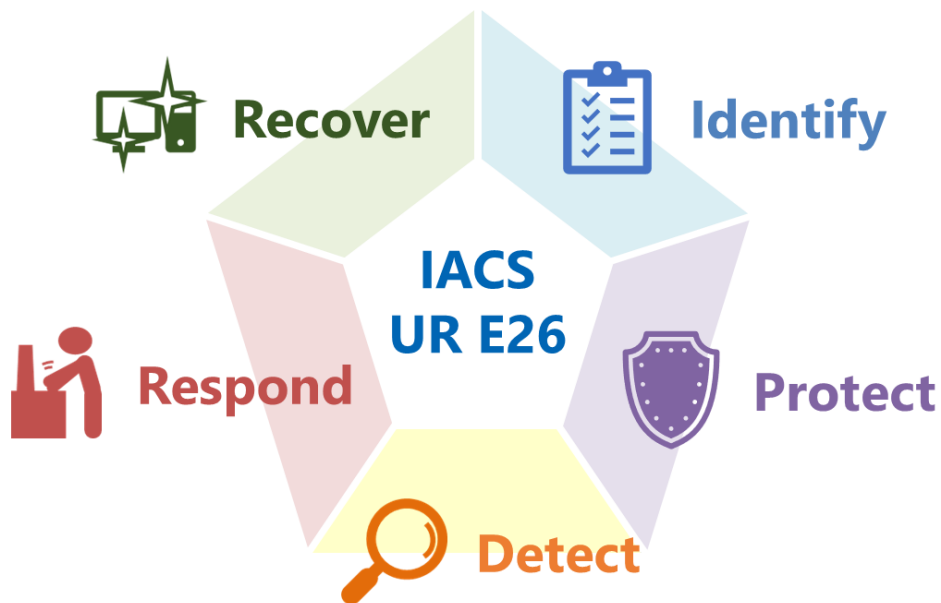


Figure 1.1 Conceptual figure of Chapter 5, Part X (UR E26)



Identify

The main purpose of "Identify" is to provide visibility into the assets owned by the ship, such as systems and network devices. Specifically, this involves creating and updating an inventory of the ship's assets. This inventory, called the vessel asset inventory, clarifies what computer-based systems and equipment are currently onboard.

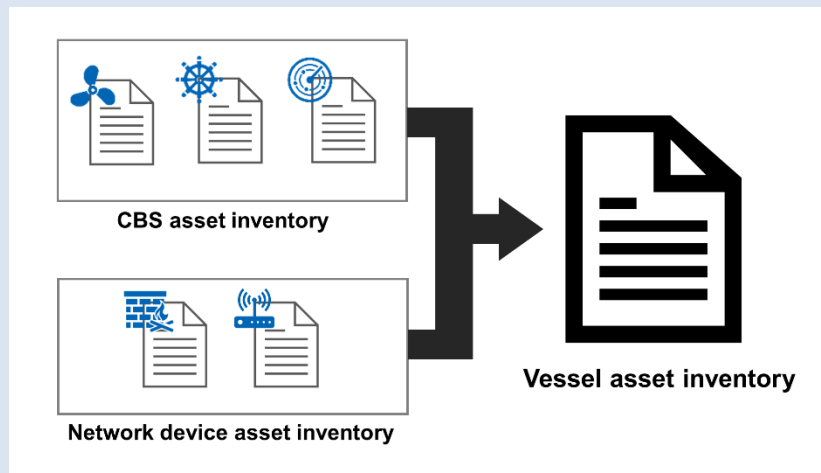


Figure 1.2 Vessel asset inventory

The vessel asset inventory is compiled by gathering product information such as OS and software from the manufacturer for each product supplied, and then summarizing it as an inventory, along with information on the onboard systems' purposes and interfaces.

By keeping the vessel asset inventory up to date, it becomes easier to grasp the assets, leading to the following effects:

- Enables understanding of the security risks of the ship's assets by cross-referencing manufacturer-provided information on security vulnerabilities and patches with the vessel asset inventory.
- Enables quick response to cyber incidents by making detailed information about the ship's assets visible in advance.
- Serves as reference documentation when managing changes to computer-based systems.

What to do?



The systems integrator is required to collect and list product information such as OS and software for the systems.



The shipowner is required to maintain and update this list as needed.



Protect

The main purpose of "Protect" is to minimize the scale and frequency of potential cyber incidents. The requirements related to implementing necessary safeguards are specified. The significant aspect is "segmenting" the networks connected to the ship's assets. Segmentation means dividing computer-based systems based on their purpose and criticality in network design.

It is also required to implement the necessary security measures (e.g., disabling unnecessary functions and services, providing only essential functions) for each device within the same segment. This design approach reduces the likelihood of being affected by cyber attacks or other threats and limits the impact on systems.

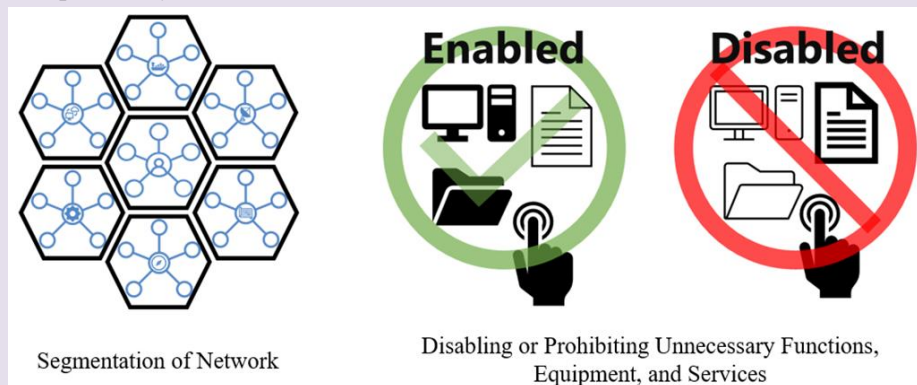


Fig.1.3 Significant safeguards required by these requirements

Effects of implementing the above safeguards:

- Security measures for each device minimize the risk of the ship being affected by cyber attacks or other threats.
- Network segmentation prevents the propagation and minimizes damage when a cyber attack occurs.

What to do?



The systems integrator is required to design the ship's network and properly configure the computer-based systems onboard, e.g., disabling unnecessary functions.



The shipowner is required to manage the systems and records to maintain the implemented safeguards.

Detect

The main purpose of "Detect" is to identify anomalies. Specifically, it involves network operation monitoring and ensuring the effectiveness of onboard security functions. During normal operations, periodic functional verification is carried out, and in the event of anomalies, alarms are triggered to enable early detection of cyber attacks affecting the ship.

- **Network operation monitoring:** Many cyber attacks involve network activities (such as increased communication traffic, changes in communication partners, etc.) during or before and after the attack. By recording these network-related activities as audit records (logs) and triggering alarms for unintended network activities that are suspected to be attacks, anomalies can be identified.



Figure 1.4 Alarms triggered by unintended network activities

- **Verification of security capabilities:** During normal operations, it is necessary to establish verification procedures, methods, and timings for verifying that the security functions related to cyber resilience, including the above-mentioned network operation monitoring, are functioning correctly. This enables the ship's security capabilities to be maintained effectively at all times.

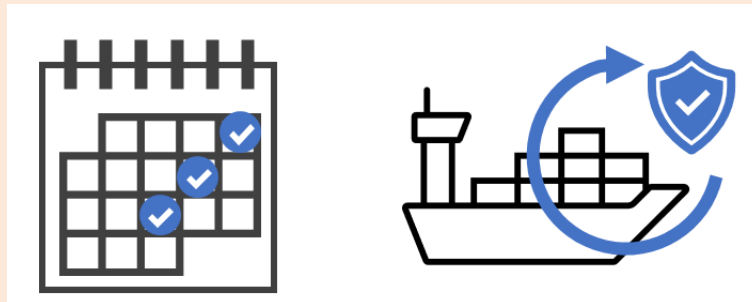


Figure 1.5 Protection through periodic verification of security functions

What to do?



The systems integrator is required to compile the network operation monitoring functions and methods for verifying security functions.



The shipowner is required to document the procedures for using network operation monitoring functions and verify the effectiveness of security functions.

Respond

The main purpose of "Respond" is to examine and implement means to minimize the impact of detected cyber incidents. Specifically, it requires creating an incident response plan that specifies how to respond to incidents and act according to that plan.

The plan must include the following information:

- **Local, independent and/or manual operation:** Detailed procedures on who will implement local or manual control over main engines, controllable pitch propellers, other propulsion equipment, and electricity generation systems as required in the event of a cyber incident.
- **Network isolation:** Detailed procedures on who will implement network isolation and how it will be done in the event of a cyber incident.
- **Fallback to a minimal risk condition:** "Fallback to a minimal risk condition" means a safe, stable condition that reduces safety risks in the event of a cyber incident. The plan should create specific procedures for how to achieve a safe, stable condition for each computer-based system provided by the systems integrator, referring to information on each system.

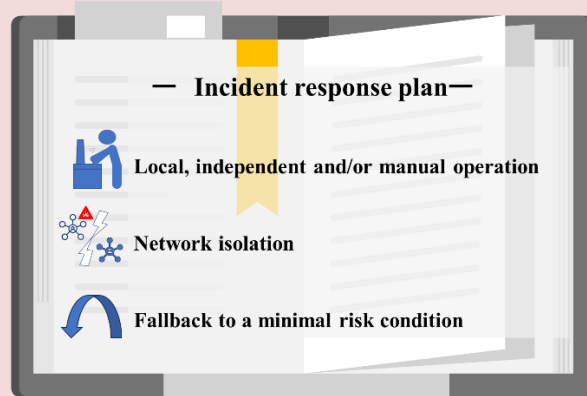




Figure 1.6 Incident response plan

By creating an incident response plan, when a cyber incident occurs, the person in charge onboard can give instructions to each crew member, and each crew member can perform their respective roles quickly and accurately. As a result, damage can be minimized.

What to do?

-  The systems integrator is required to compile and document information to assist the shipowner in creating incident response plans.
-  The shipowner is required to create an incident response plan. When a cyber incident occurs, the person responsible is to give instructions according to the plan, and each crew member is required to perform their respective roles quickly and accurately.

Recover

The main purpose of "Recover" is to restore computer-based systems to an operational state after a disruption or failure caused by a cyber incident. By planning and implementing a recovery plan according to these requirements, computer-based systems and networks can be quickly restored.

In the recovery plan, "roles and procedures for personnel in recovering from a cyber incident" and "backup management, including maintenance and testing" are to be developed based on the shipowner's policy. Additionally, when creating the recovery plan for each computer-based system, it is necessary to refer to the "information supporting incident response and recovery plans" provided by suppliers.

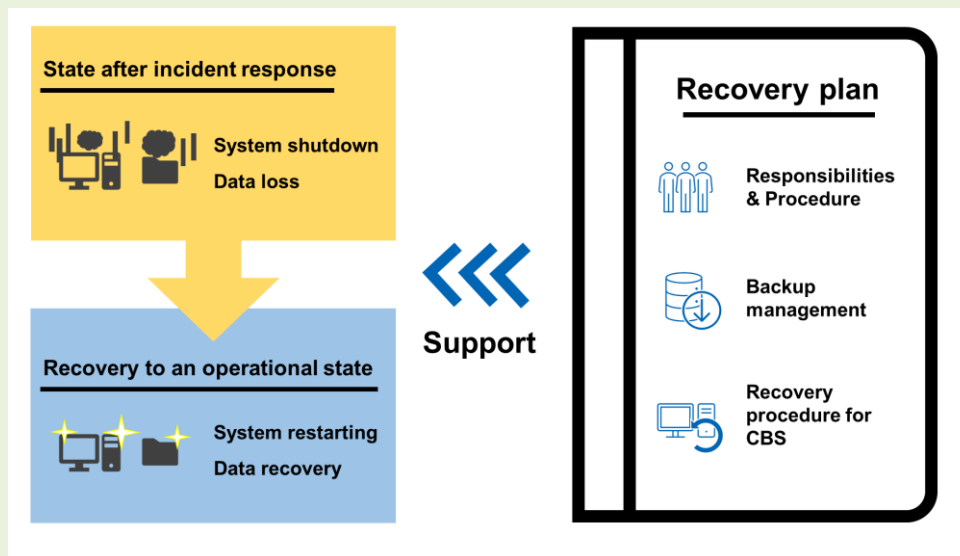




Figure 1.7 Recovery plan

By creating a recovery plan, the following benefits are achieved:

- Each personnel member's responsibilities and tasks for incident recovery are clarified.
- Recovery can be performed using procedures appropriate for each computer-based system.

What to do?

-  The systems integrator is required to compile and document information to assist the shipowner in creating recovery plans for each computer-based system.
-  The shipowner is required to manage backups, including maintenance and testing, and ensure that recovery work is performed quickly and accurately according to the plan's procedures.

Chapter 2 Application

This chapter explains the scope of application of Chapter 5, Part X (UR E26). The scope of Chapter 5, Part X (UR E26) is determined as follows. The key points are the determination of applicability to ships and the determination of applicability for each onboard system. Firstly, applicability is determined for each ship, and then applicability is determined for each system on the ship that has been determined to be applicable as shown in Figure 2.1. In determining the applicability of systems, the network configuration of the systems requires particular consideration. The applicable systems are represented as blue, green, or orange in the “Applicable systems” area in Figure 2.1. They will be explained in detail in Section 2-2.2. The collection of systems that become applicable in this manner constitutes the scope of application.

Systems subject to Chapter 5, Part X (UR E26) must be approved based on Chapter 4, Part X (UR E27) and require network design and management based on Chapter 5, Part X (UR E26).

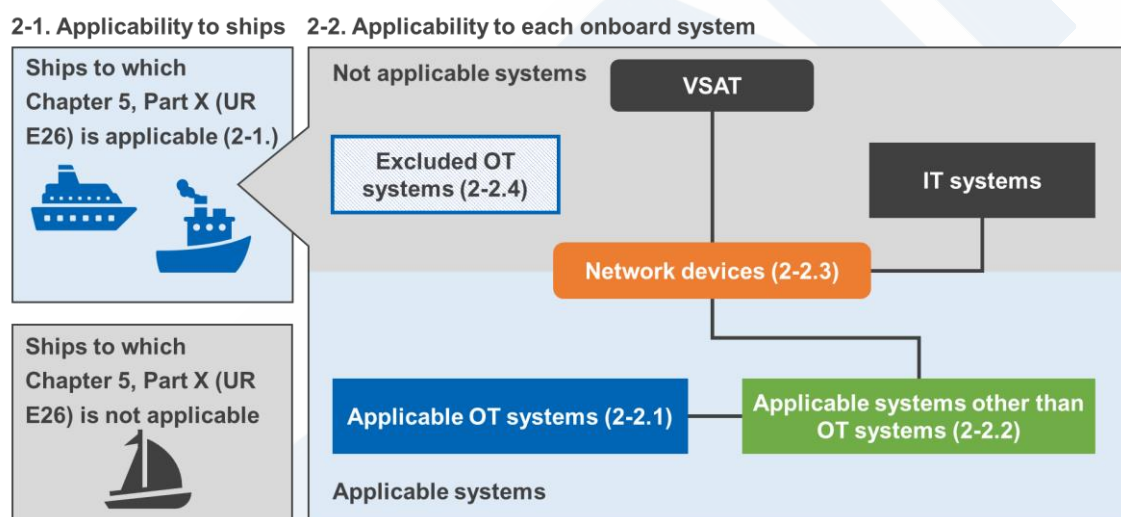


Figure 2.1 Scope of Application of Chapter 5, Part X (UR E26)

2-1. Ships in scope of Chapter 5, Part X (UR E26)

Chapter 5, Part X (UR E26) applies to the following ships contracted for construction on or after July 1, 2024, registered with the Society:

- Passenger ships (including passenger high-speed craft) engaged in international voyages
- Cargo ships of 500 GT and upwards engaged in international voyages
- High speed craft of 500 GT and upwards engaged in international voyages
- Mobile offshore drilling units of 500 GT and upwards
- Self-propelled mobile offshore units engaged in construction (i.e. wind turbine installation maintenance and repair, crane units, drilling tenders, accommodation, etc.)

Computer-based systems installed on ships other than the above are not applicable, and do not need to be approved in accordance with Chapter 5, Part X (UR E26).

2-2. Systems in scope of Chapter 5, Part X (UR E26)

Chapter 5, Part X (UR E26) applies not to all systems installed on ships, but to systems related to ship operations. Figure 2.2 shows a flowchart for determining the applicability of each system. This section provides detailed descriptions of applicable systems based on these determination criteria for applicability.

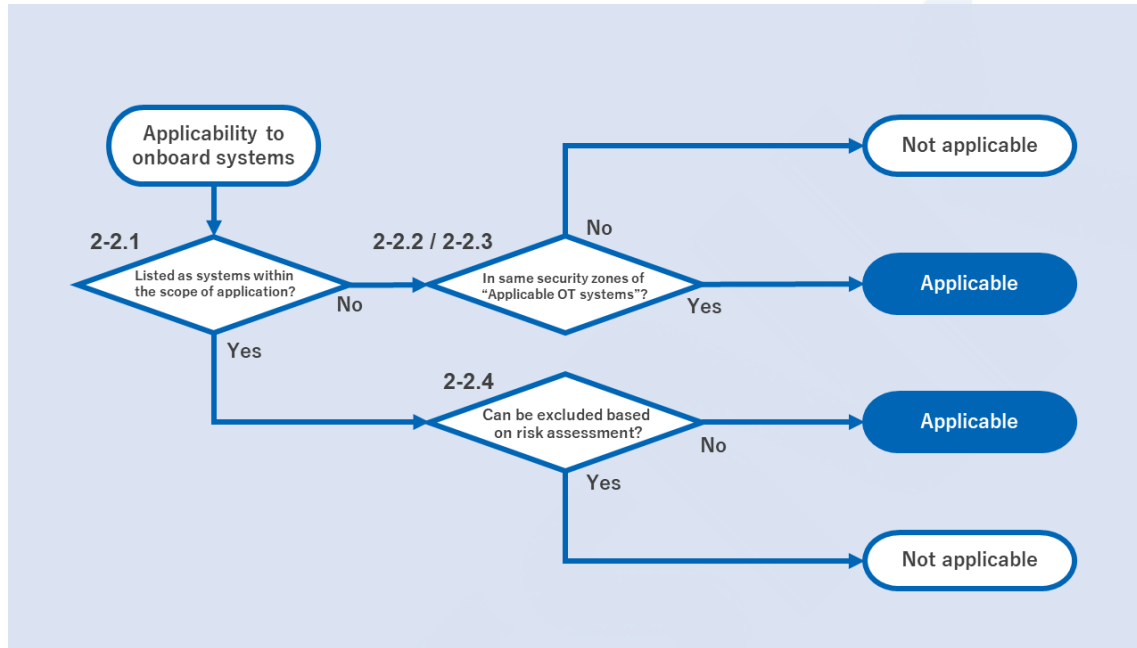


Figure 2.2 Flowchart of applicability of systems

2-2.1 Operational Technology (OT) Systems Onboard Ships

Operational Technology (OT) systems onboard ships are subject to application. OT systems are computer-based systems that use data to control or monitor physical processes*. In other words, OT systems onboard ships refer to systems that control or monitor the ship's navigation, propulsion, power generation, safety, etc., and may pose safety concerns if compromised. Furthermore, these systems require approval in accordance with Chapter 4, Part X (UR E27).

*Physical Process: A series of operations that utilize physical phenomena, such as pressure and temperature, to perform work or transformations.

Below are examples of systems considered to be within the scope of application. Please note that these are merely examples and do not conclusively determine the application of Chapter 5, Part X (UR E26).

**Propulsion**

Engine control systems

Main boiler control systems

Electric propulsion control systems

Machinery alarm and monitoring systems
(including data loggers)

Engine telegraph

Engine remote control systems

CPP control systems

Fuel supply system control unit (e.g., FGSS
control systems)

Waterjet propulsion control systems

**Steering**

Steering system control systems

Azimuth thruster control systems

**Anchoring and mooring**

Windlass control systems

Mooring winch control systems

**Electrical power generation and distribution**

Generator engine control systems
(including power management systems)

Battery management systems
(consisting of lithium-ion batteries with total
capacities of 20 kWh or more, and associated
equipment)

Electric power converters
(for electric propulsion ship)

**Fire detection and extinguishing systems**

Fire detection and alarm systems

Fixed CO₂ fire extinguishing systems

Fixed local application fire-fighting systems

Dry chemical fire-extinguishing equipment

Fixed foam fire extinguishing systems

Fixed deck foam systems

Water-spraying systems

**Bilge and ballast system, loading computer**

Ballast transfer valve remote control systems

Loading computers



Watertight integrity and **flooding detection**

Watertight door power opening/closing devices

Water level detection and alarm systems



Lighting (e.g. emergency lighting, low locations, navigation lights, etc.)

Emergency lighting

Low location lighting

Navigation lighting control systems



Any required **safety system** whose disruption or functional impairing may pose risks to ship operations (e.g. emergency shutdown system, cargo safety system, pressure vessel safety system, gas detection system, etc.)

Inert gas systems

Cargo monitoring control systems

Liquefied gas emergency shutdown systems

Flammable gas detection systems

Reliquefaction plants

Auxiliary boiler control systems

GCU control systems

Gas fuel tank monitoring and control systems



Navigational systems required by statutory regulations

Radar

Transmitting heading devices (THD)

Electronic plotting aids (EPA)

Automatic identification systems (AIS)

Automatic tracking aids (ATA)

Voyage data recorders (VDR)

Target Track (TT) (ARPA)

Heading control systems (HCS)

Echo sounding devices

Track control systems (TCS)

Global navigation satellite systems (GNSS)

Long range identification and tracking systems (LRIT)

Sound reception systems

Bridge navigational watch alarm systems (BNWAS)

Speed and distance measuring devices

Electronic chart display and information systems (ECDIS)

Electronic Inclinometer

Rate-of-turn indicator



Internal and external communication systems required by class rules and statutory regulations

General emergency alarm

Public addressor

NAVTEX receiver

VHF DSC device

EGC receiver

DSC device

VHF DSC continuous watch device

DSC continuous watch device



Others

Dynamic positioning systems (DPS)

2-2.2 Applicable Systems other than OT Systems, Network Devices

In addition to Section 2-2.1, modern ships may have systems other than OT systems that connect to OT systems by IP connection. For example, electronic chart data servers connected to ECDIS for obtaining chart data via external networks, or data servers that collect operational data from VDRs and telegraph loggers and transfer it to computers on business networks. (See Figure 2.3) In addition, if the system is connected to a satellite communication device, L3 switches and routers connected to the firewall may also be applicable.

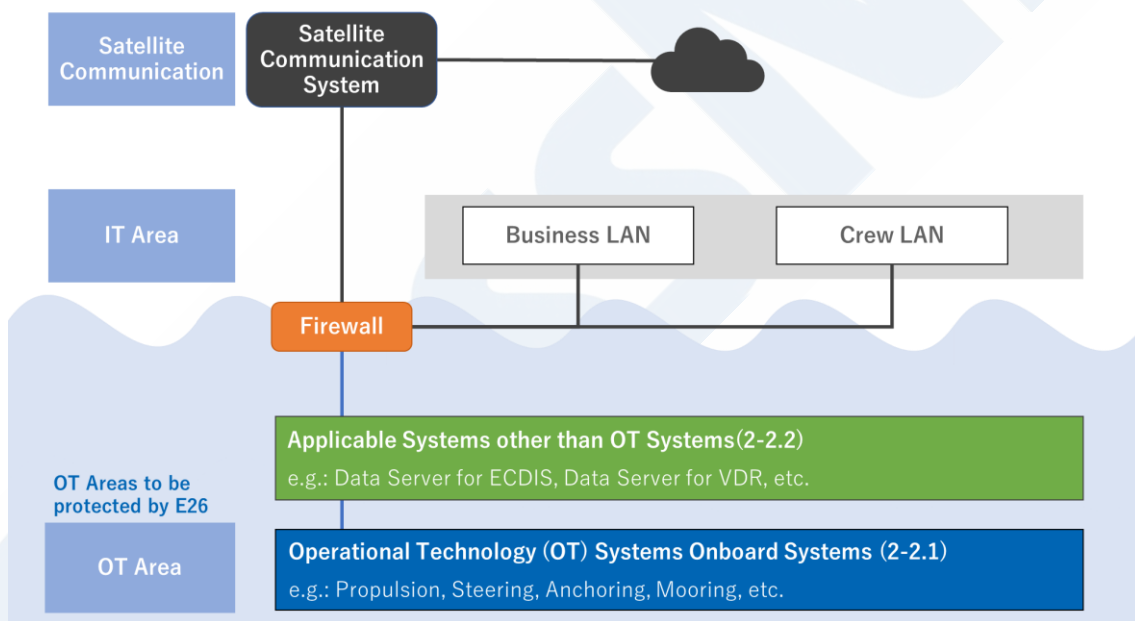


Figure 2.3 Outline diagram of Ship Network

Whether these devices are within the scope of the application depends on the network design method. Here, we explain whether these systems are included in the scope using some representative network design examples. [In any network design, it is necessary to protect the safety-related systems mentioned in 2-2.1.](#)

2-2.2.1 Terminology

This section explains the terminology used in section 2-2.2.

- **Network segment**

A network segment refers to a section or division of a network that is separated by routers or switches. It defines the scope where the same broadcast communication (communication transmitted simultaneously to all devices) can reach. Essentially, devices within the same network segment can communicate directly with each other without going through routers or similar devices.

- **Zone Boundary Device**

A zone boundary device is equipment used to separate network sections, including routers and firewalls. This device inspects and controls communication data passing through it, and permits or denies communication based on security policies (predetermined rules). This prevents unauthorized communication and ensures the security of inter-zone communication.

According to the regulations, these are also referred to as:

- Components providing protection of the security zone boundary
- Means providing control of data communicated between the zones
- (Security) zone boundary devices

- **Security Zone**

A security zone is a group of onboard networks, consisting of one or more network segments that satisfying the same security policy. Zone boundary devices must be placed between different security zones.

- **Untrusted Network**

This refers to networks to which Chapter 5, Part X (UR E26) is not applied. Examples include external networks outside the ship, as well as business networks and crew networks. Zone boundary devices are required between untrusted networks and security zones.

2-2.2.2 Case with No Connections between Applicable OT Systems and IT Systems

This case involves scenarios where there are no direct IP connections between OT system networks and IT system networks. In this case, the scope of application is limited to the OT systems mentioned in 2-2.1. The representative network configuration for this scenario is as follows:

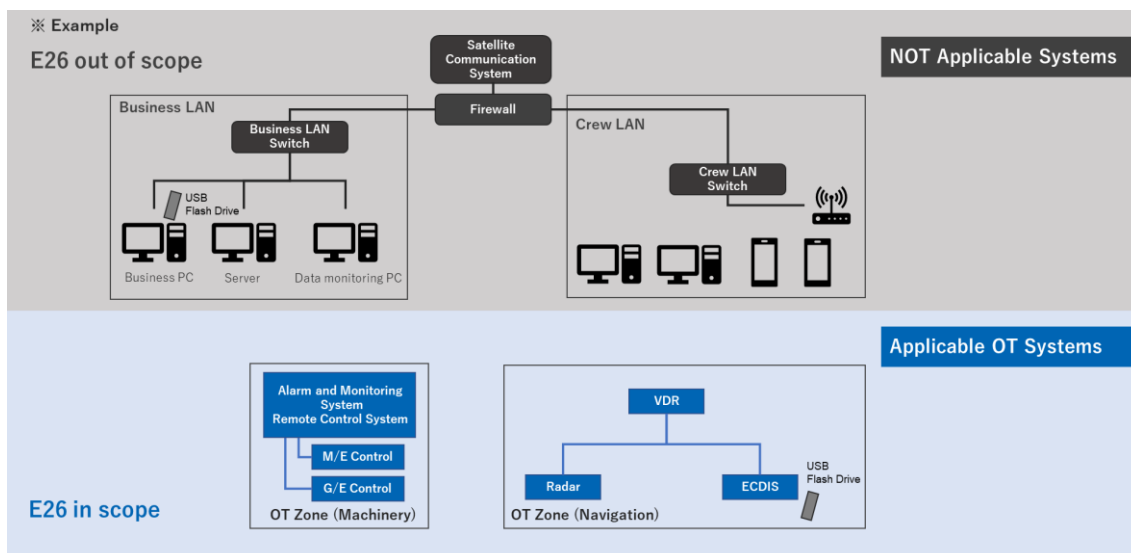


Figure 2.4 Network Configuration Diagram for the Case with No Connections between Applicable OT Systems and IT Systems

- Assumed Operation:

Electronic chart updates are obtained on a computer on the IT network, and the data is copied to a medium such as a USB flash drive and transferred to the ECDIS on the OT network.

- Explanation of Network Configuration:

Since the OT network within the scope of application and the IT network are completely isolated with no connection points, there is no change in the applicable scope regarding network design. However, there are cyber risks through media and personnel, so access management and media management must be implemented based on Chapter 5, Part X (UR E26).

Additionally, when examining the connection status of the OT systems, it can be observed that they are separated into engine room systems (such as machinery monitoring systems and remote control systems) and navigation equipment systems (such as ECDIS and VDR). "Security zones" can be established for each group based on the security policy. Each security zone is to be segmented from the others. In this example, the engine room systems are grouped as "OT Zone (Machinery)" and the navigation equipment systems are grouped as "OT Zone (Navigation)".

This diagram illustrates a configuration where there are no IP connections between OT zones or between OT zones and IT zones. In this case, no systems other than those indicated above are connected to the same security zone as the applicable computer-based systems.

2-2.2.3 Case with Systems other than Applicable OT Systems within OT Zones

This case involves scenarios where systems other than the applicable OT systems are included within the OT zone. In this situation, such systems are also within the scope of application. Therefore, these systems are allocated to the same zone as the OT systems mentioned in 2-2.1, and equivalent measures are required for each device, necessitating compliance with Chapter 4, Part X (UR E27).

The representative network configuration for this scenario is as follows:

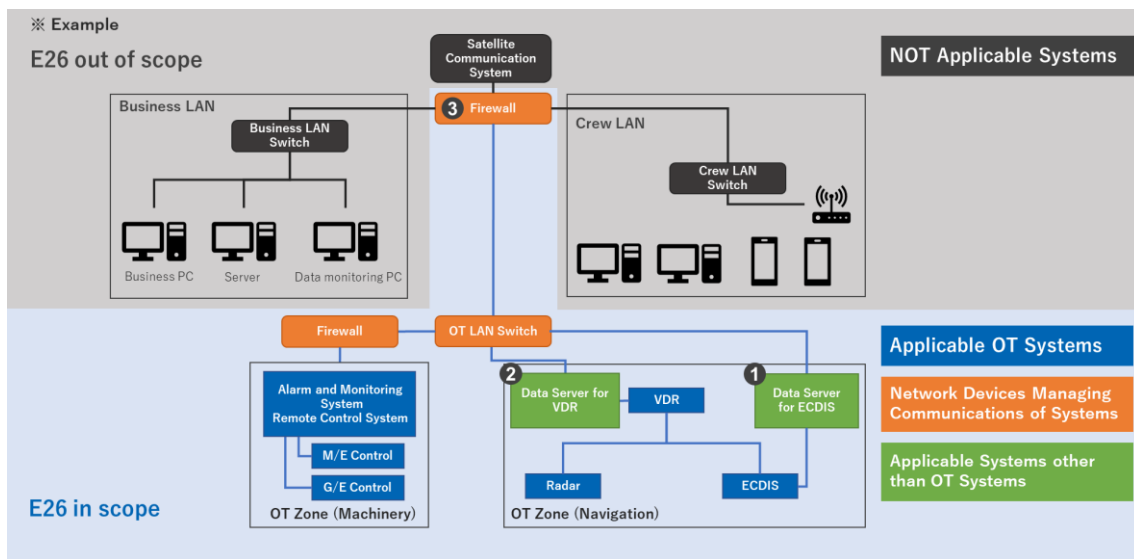


Figure 2.5 Network Configuration Diagram for the Case with Systems other than Applicable OT Systems within OT Zones

- Assumed Operation:

Electronic chart updates are delivered from an onshore server (such as a server owned by an electronic chart provider) via the ECDIS data server with external connection capabilities at point ① in Figure 2.5 and then transferred to the ECDIS. Operational data from the VDR is transferred to a computer on the IT network or an external computer via the VDR data server at point ② in Figure 2.5.

- Explanation of Network Configuration:

Since there is communication between the network within the scope of application and the IT network, zone boundary devices such as firewalls at point ③ in Figure 2.5 are to be introduced to ensure physical separation.

Additionally, all systems included in the security zone within the scope of application must be approved in accordance with Chapter 4, Part X (UR E27). In this case, among these zone boundary devices and network equipment, those positioned up to the boundary between applicable networks or untrusted networks also fall within the scope of applicability.

- Explanation of Network Configuration:

Applicable systems need to receive approval based on Part X Chapter 4 (UR E27). Part X Chapter 4 (UR E27) contains functional requirements that systems must satisfy, but the requirements to be addressed differ depending on whether there is communication with untrusted networks.

When there is no communication with untrusted networks, compliance with the basic 30 security capabilities is required. On the other hand, when there is communication with untrusted networks, compliance with 11 additional requirements is required in addition to the basic 30 security capabilities.

For detailed information, please refer to the "Guidelines on Cyber Resilience of On-board Systems and Equipment."

2-2.2.4 Case with Systems other than Applicable OT Systems within the DMZ

This case involves systems with IP connections to OT systems being included in a DMZ (Demilitarized Zone). Generally, in network design, a DMZ is a zone allocated between external and internal networks to accept access from the external network while preventing direct access to the internal network. In ship networks, systems connected to OT systems in the DMZ reduce threats to OT systems from unauthorized access via the IT network even if unauthorized access to the DMZ occurs through the IT network. It also enables relatively easy adaptation to various network configuration changes throughout the ship's lifecycle. In this case, since the network in the DMZ is allocated outside the zone containing OT systems, compliance with Chapter 4, Part X (UR E27) for devices in the DMZ is not mandatory and it can be treated as an untrusted network.

However, there are considerations when treating devices in the DMZ as an untrusted network by making them non-applicable to Chapter 4, Part X (UR E27).

Firstly, the representative network configuration for the scenario where the DMZ is treated as an untrusted network is shown as follows:

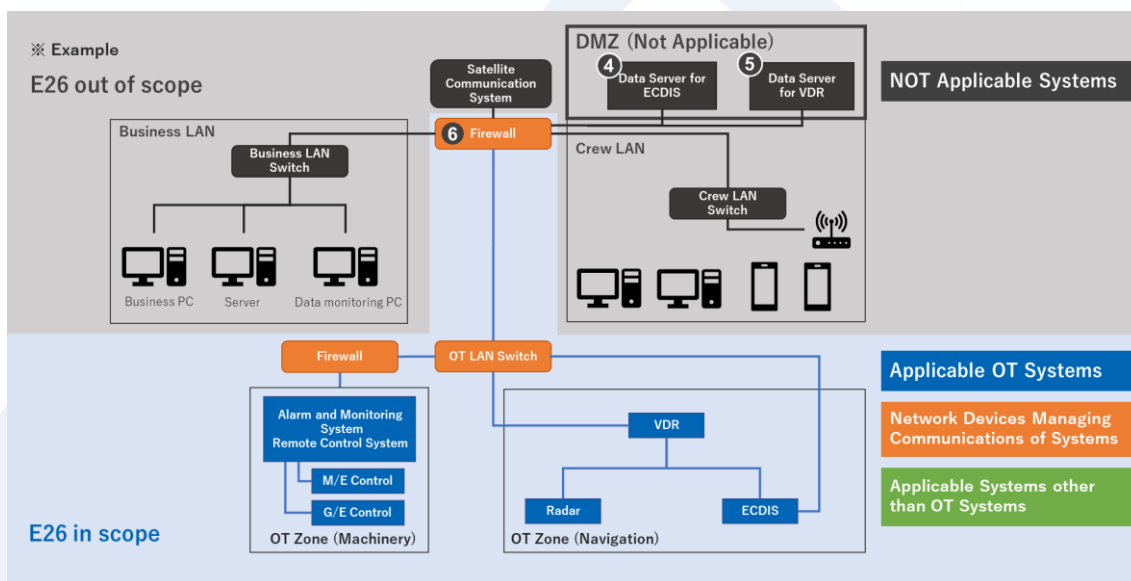


Figure 2.6 Network Configuration Example for Systems Connected to OT Systems Included in the DMZ

- Assumed Operation:

The electronic chart updates are delivered from an onshore server (such as a server owned by an electronic chart provider) via the shipboard ECDIS data server with external connection capabilities at point ④ in Figure 2.6, and then transferred to the ECDIS. Operational data on the VDR is transferred to a computer on the IT network or an external computer via the VDR data server at point ⑤ in Figure 2.6.

- Explanation of Network Configuration:

Since there is communication between the network within the scope of the application and the DMZ network, zone boundary devices such as firewalls at point ⑥ in Figure 2.6 are to be introduced to ensure physical separation. While systems within the DMZ can comply with the rules without being designated as applicable as described above, when determining whether they should be designated as applicable in actual design, it is recommended to consider the following advantages and disadvantages.

- When the DMZ is Not Designated as an Applicable Security Zone:

With this network configuration, systems such as the ECDIS data server and the VDR data server fall outside the scope of systems under Chapter 5, Part X (UR E26), thus approval according to Chapter 4, Part X (UR E27) is not required. However, since the DMZ becomes an untrusted network, as explained in the case of including systems other than applicable OT systems within OT zones, each OT system that communicates with the DMZ must comply with the additional 11 security capabilities for untrusted networks, in addition to the basic 30 security capabilities. In this example, the additional requirements apply to ECDIS and VDR.

- When the DMZ is Designated as an Applicable Security Zone:

When the DMZ is included within the scope of applicability in the network configuration, the network structure becomes as shown below. In this case, systems within the DMZ require compliance with Chapter 4, Part X (UR E27). In this case, while systems within the DMZ are subject to the additional requirements, ECDIS and VDR do not need to comply with the additional requirements since they communicate with applicable systems.

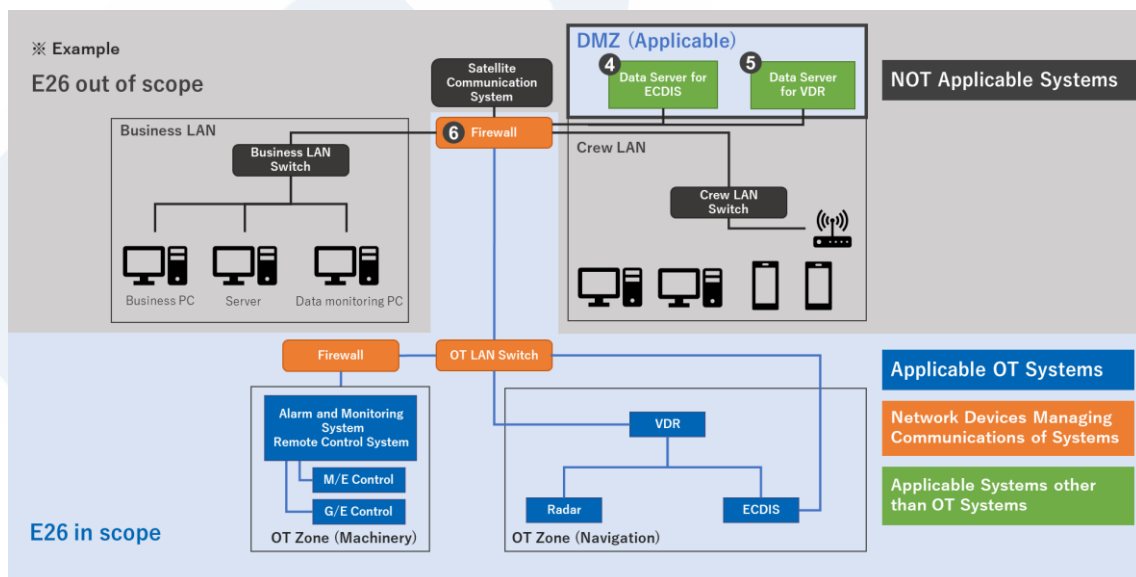


Figure 2.7 Network Configuration Diagram in case the DMZ is applicable.

The following summarizes the advantages and disadvantages of the total 4 network designs mentioned in sections 2-2.2.2 through 2-2.2.4 (including whether the DMZ is applicable or not).

Table 2.1 Comparison of Advantages and Disadvantages of Each Network Design

		Advantages	Disadvantages
Case where OT and IT systems are not connected		- Low risk of intrusion via IT networks	- Data collection/updates of OT systems through network connections cannot be performed
Case where systems other than OT systems are included in OT zones		- Data collection/updates of OT systems through network connections become easier	- Risk of intrusion such systems are compromised - Approval in accordance with Chapter 4, Part X (UR E27) is required for such systems
Case where systems other than OT systems are included in the DMZ	Non-applicable DMZ	- Data collection/updates of OT systems through network connections become easier - Equivalent systems can be segmented, which reduces risk compared to including them in OT zones - Approval in accordance with Chapter 4, Part X (UR E27) is not required for such systems	- Additional requirements of Chapter 4, Part X (UR E27) apply to OT systems
	Applicable DMZ	- Data collection/updates of OT systems through network connections become easier - Such systems can be segmented, which reduces risk compared to including them in OT zones - Additional requirements of Chapter 4, Part X (UR E27) do not apply to OT systems	- Approval in accordance with Chapter 4, Part X (UR E27) is required for such systems

2-2.3 Communication Interface Between Networks within the Scope of Chapter 5, Part X (UR E26) and Untrusted Networks (Network Devices)

The scope of Chapter 5, Part X (UR E26) is determined based on 2-2.2. For IP-based communication between networks within the scope of application and other networks, such communication is also included within the scope of Chapter 5, Part X (UR E26), and the following measures are required:

- Network devices (such as switches and firewalls) connected to the networks within the scope of application are to be properly configured.
- Network devices are to be appropriately managed and maintained.
- Data flowing through the network is to be properly encrypted.

Additionally, the network devices themselves are to be placed within the scope of Chapter 5, Part X (UR E26), requiring approval in accordance with Chapter 4, Part X (UR E27). These correspond to “Network Devices Managing Communications of Systems” in Figure 2.5 to Figure 2.7.

2-2.4 OT Systems Excluded from Application based on Risk Assessment for Exclusion of

Computer-Based System from the Application of Requirements

For the applicable OT systems described in **2-2.1 Operational Technology (OT) Systems Onboard Ships**, applying Chapters 5 and 4, Part X (UR E26 and E27) to all systems is not realistic considering the large number of requirements, and cases where the effectiveness would be small are anticipated.

These rules establish a mechanism for individually excluding such OT systems from the scope of application. Figure 2.8 shows a network that includes OT systems that have been excluded from application in this manner.

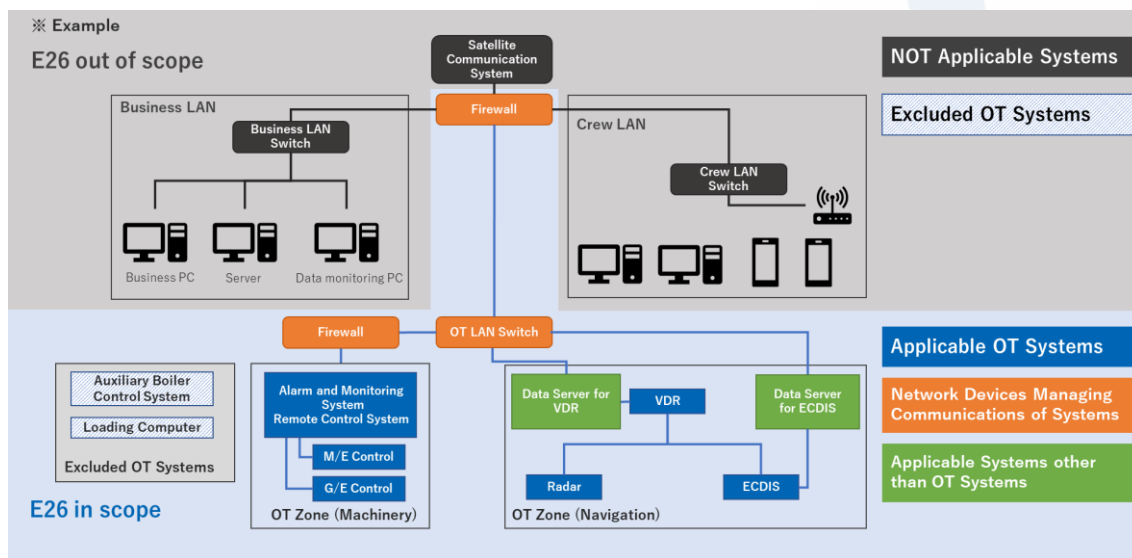


Figure 2.8 Network Diagram Including OT Systems Excluded from Application

As shown above, even systems listed as applicable OT systems in **2-2.1 Operational Technology (OT) Systems Onboard Ships** can be considered outside the scope of application if they meet the criteria shown below. The conditions for exclusion include mandatory criteria and additional criteria that should be met. The mandatory criteria must be satisfied as specified in the regulations. However, additional criteria that should be met may allow for exclusion even when not fully satisfied, if a rational explanation is provided and accepted by the Society. These criteria are presented below, but for details, please refer to "4-4. Risk Assessment for Exclusion of Computer-Based Systems from Application Requirements" in this guideline.

Firstly, the mandatory criteria are as follows:

Rule 5.5.4-2, Part X of the Rules

The following criteria are to be met to exclude a system from the scope of applicability of this Chapter:

- (1) The computer-based system is to be isolated (i.e, have no IP-network connections to other systems or networks).
- (2) The computer-based system is to have no accessible physical interface ports. Unused interfaces are to be logically disabled. It is not to be possible to connect unauthorised devices to the computer-based system.

- (3) The computer-based system is to be located in areas to which physical access is controlled.
 - (4) The computer-based system is not to be an integrated control system serving multiple ship functions as specified in the scope of applicability of this Chapter.
-

Then, the additional criteria are as follows:

Rule 5.5.4-3, Part X of the Rules

The following additional criteria are to be considered for the evaluation of risk level acceptability:

- (1) The computer-based system should not serve ship functions of category III.
 - (2) Known vulnerabilities, threats, potential impacts deriving from a cyber incident affecting the computer-based system have been duly considered in the risk assessment.
 - (3) The attack surface for the computer-based system is minimized, having considered its complexity, connectivity, physical and logical access points, including wireless access points.
-

Chapter 3 Process for Compliance

This chapter explains the process of Chapter 5, Part X (UR E26). Specifically, it outlines the actions that systems integrators and shipowners should take at each phase of a ship's lifecycle, based on the documents to be created.

Firstly, Chapter 5, Part X identifies systems integrators and shipowners as stakeholders. This Guidelines defines systems integrators and shipowners as follows:



Systems integrator: Refers to the person in charge of security design and network construction. Except when contracted or designated otherwise, this is the shipyard.



Shipowner: Refers to the shipowner or ship management company. (In Chapter 5, Part X, this is defined as "shipowner/company.")

Table 3.1 Actions to be Taken by Systems integrators and Shipowners at Each Phase

	Design / Construction Phase	Commissioning Phase	Operation Phase
Systems Integrator	P. 20	P. 23	
Shipowner	P. 23	P. 23	P. 24

3-1. Design and Construction Phase

During the design and construction phase, systems integrators are required to design the ship's network, including computer-based systems, and then actually construct the network accordingly. Systems integrators are also required to submit relevant materials related to the ship's network to the Society. Although shipowners are not directly subject to specific requirements, it is recommended that they share information about the ship's network with the systems integrators in advance.



Systems integrator

The role of the systems integrator during the design and construction phase includes the following:

1) Identify computer-based systems within the Scope of Chapter 5, Part X (UR E26)

Systems integrators are first required to identify the computer-based systems that fall within the scope of Chapter 5, Part X (UR E26). This involves listing the necessary computer-based systems for the

ship and assessing whether each system falls within the scope of Chapter 5, Part X (UR E26). The scope of application is explained in detail in Chapter 2 "Application" of this Guidelines.



Chapter 2 Application

P. 8

2-2. Systems in scope of Chapter 5, Part X (UR E26)

When identifying computer-based systems, [it is recommended to prepare the following documents prior to other submission materials at this stage.](#)



4-1. Vessel asset inventory

P. 27



4-2. Zones and conduit diagram

P. 32



4-4. Risk assessment for the exclusion of computer-based systems

P. 58

Preparing these documents allows for the accurate identification of computer-based systems and network devices within the scope of Chapter 5, Part X (UR E26). Failure to accurately identify the scope of Chapter 5, Part X (UR E26) may result in the following issues:

- Concerns about the installation of computer-based system or network devices within the scope of Chapter 5, Part X (UR E26) but not approved under Chapter 4, Part X (UR E27).
- Concerns about computer-based system connected to untrusted networks but lacking "additional security features" as required by Chapter 4, Part X (UR E27).

Such cases could lead to [reordering computer-based systems or network devices, causing setbacks](#), so it is important to prepare the documents early.

Additionally, [it is necessary to identify the equipment provided by the shipowner in advance](#). These shipowner-supplied items may be integrated into the ship's network and directly connected to OT systems. In such cases, there is a possibility that these shipowner-supplied items fall within the scope of Chapter 5, Part X (UR E26), so attention is required. Therefore, it is important for systems integrators to promptly receive information about these shipowner-supplied items from the shipowner.

2) Obtain Approval Documents for computer-based systems from Each Supplier

The computer-based systems identified in 1) are subject to Chapter 4, Part X (UR E27), and therefore, computer-based systems approved by the Society based on these regulations are to be installed. Systems integrators are required to obtain approval documents for these computer-based systems from the suppliers. The documents required by Chapter 4, Part X (UR E27) are as follows:






Approval documents for computer-based systems (see Chapter 4, Part X (UR E27))	
<input type="checkbox"/>	Computer-based system asset inventory
<input type="checkbox"/>	Topology diagrams
<input type="checkbox"/>	Description of security capabilities

<input type="checkbox"/>	Test procedure of security capabilities (Including Test reports)
<input type="checkbox"/>	Security configuration guidelines
<input type="checkbox"/>	Secure development lifecycle documents
<input type="checkbox"/>	Plans for maintenance and verification of the computer-based system
<input type="checkbox"/>	Information supporting the owner's incident response and recovery plan
<input type="checkbox"/>	Management of change plan

Additionally, when obtaining these documents, it is essential to verify the descriptions of compensating countermeasures described in the "Description of security capabilities". Compensating countermeasures are alternative measures implemented when the required security capabilities for the computer-based system cannot be implemented. Some of the compensating countermeasures proposed by the computer-based system may require additional network equipment. Therefore, it is recommended to determine the necessity of purchasing such additional equipment at this phase.

3) Prepare and Submit Required Documents to the Society's Machinery Department

During the design phase, the systems integrator is to prepare and submit documents related to security and network for approval. The necessary documents are as follows. Detailed explanations of each document can be found in Chapter 4, "Explanation of Submission Plans and Documents" of this Guidelines.

	4-1. Vessel Asset Inventory	P. 27
	4-2. Zone and Conduit Diagram	P. 32
	4-3. Cybersecurity Design Description	P. 39
	4-4. Risk Assessment for the Exclusion of Computer-based Systems	P. 58
	4-5. Description of Compensating Countermeasures	P. 61

Additionally, [it is anticipated that information necessary for the design of drawings related to shipowner-supplied equipment may not be shared.](#) In such cases, please indicate the relevant information as "TBD" (To Be Determined) and proceed to prepare and obtain approval for the necessary documents by the "Survey at the commissioning phase."

4) Update Approved Documents as Necessary

During the construction phase, if design modifications occur, it is required to update the documents approved in 3). Design modifications are to be carried out in accordance with the systems integrator's management of change plan.

Additionally, as indicated in 3), if information about shipowner-supplied equipment was marked as "TBD" at the time of plan approval, update the relevant documents once the information is obtained from the shipowner and seek approval from the Society.



Shipowner

During the design and construction phase, it is necessary to consider the following point:

Share Equipment to be Integrated into the Ship's Network with the Systems Integrator

Equipment supplied by the shipowner during the design and construction phase may be integrated into the ship's network and directly connected to OT systems. Since these shipowner-supplied items may fall within the scope of Chapter 5, Part X (UR E26), attention is required. Therefore, [it is important for the shipowner to promptly share information about these shipowner-supplied items with the systems integrator.](#)

- Regarding Equipment Supplied by the Shipowner

Among shipowner-supplied equipment, systems that may be subject to application including the following:

- Network devices (switches, routers, firewalls, etc.)
- Applicable Systems other than applicable OT systems (see Chapter 2 "Application" of this Guidelines)



Chapter 2 Application

2-2. Systems in scope of Chapter 5, Part X (UR E26)

P. 8

In conventional shipbuilding, these devices are often installed in the final stages of construction (from sea trials to delivery) and it has been common for information about these devices to not be shared with the systems integrator during the design phase. However, in the future, it will be important to provide the systems integrator with information about these devices from the design phase.

3-2. Commissioning Phase

During the commissioning phase, the systems integrator is required to conduct tests to ensure that the security capabilities of the computer-based system and network are functioning correctly after constructing the ship's network.



Systems Integrator

The systems integrator's roles during the commissioning phase are as follows:

1) Submit the latest design documents to our machinery department if necessary

If there have been any changes to the documents approved during the design phase (see 3-1.4 above), the latest versions must be submitted for approval by the Society before conducting tests during the commissioning phase.

2) Prepare and submit the "Ship Cyber Resilience Test Procedure" to the Society's machinery department

Before conducting tests during the commissioning phase, it is necessary to prepare a test procedure (Ship Cyber Resilience Test Procedure) that outlines the test environment, test procedures, expected results, and pass criteria. This document is to be approved by the Society.



4-6. Ship Cyber Resilience Test Procedure

P. 63

3) Conduct the tests in accordance with the approved Ship Cyber Resilience Test Procedure under the Society's survey

As a verification test of the security of the ship's computer-based system and network, the tests during the commissioning phase are to be conducted under the supervision of the Society's surveyor. These tests are to be performed in accordance with the aforementioned "Ship Cyber Resilience Test Procedure."



5-1. Survey at the commissioning phase

P. 127

Additionally, please note that this survey is a verification test targeting computer-based system and networks within the scope of Chapter 5, Part X (UR E26). If the shipowner-supplied items are included as systems within this scope, they will also be subject to the survey.

3-3. Operation Phase

After the delivery of the ship, the documents created during the design, construction, and commissioning phases are handed over to the shipowner. During the operation phase, the shipowner is required to maintain the security as designed. To ensure continued compliance with Chapter 5, Part X (UR E26), change management of these documents is necessary throughout the ship's operational life. Properly managing these changes allows for the maintenance of the security established during the design phase throughout the ship's lifetime. Therefore, the shipowner is to create and implement documents that outline procedures for proper operation and change management.

**Shipowner**

The roles of the shipowner during the operation phase are as follows:

1) Prepare and submit the "Ship cyber security and resilience program" to our machinery department

The shipowner is to prepare the "Ship cyber security and resilience program," including operations and procedures, based on the information provided by the systems integrator. This program is to be approved by the Society.



4-7. Ship cyber security and resilience program

P. 89

2) Conduct the first annual survey

During the first annual survey, the operational status based on the approved "Ship cyber security and resilience program" will be verified. Therefore, the shipowner is to implement the program in practice and complete the entire process, including the creation of records, [by the first annual survey](#). Details on the "First Annual Survey" are provided below.



5-2. First Annual Survey

P. 130

3) Operate the approved "Ship cyber security and resilience program" and update approved documents as necessary

During operation, if there are any changes affecting the security capabilities, such as updates to computer-based system or network configuration changes, these are to be implemented and recorded based on the program. Additionally, if there are any changes to the approved documents, including materials from the systems integrator, they are to be re-approved by the Society.

4) Conduct the required surveys during periodical surveys

During periodical surveys, the corresponding surveys (annual, intermediate, special) are to be conducted to ensure ongoing compliance with the requirements of Chapter 5, Part X (UR E26).



5-3. Subsequent Annual Surveys / Intermediate Survey

P. 132



5-4. Special Survey

P. 133

Chapter 4 Explanation of Submission of Plans and Documents

This chapter explains the details of the submission documents specified in Chapter 5, Part X (UR E26)

Chapter 5, Part X (UR E26) specifies the requirements for seven submission documents related to the cyber resilience of ships. The requirements for each document are as follows:



Submission Plans and Documents Requirements



4-1. Vessel asset inventory

P. 27



4-2. Zones and conduit diagram

P. 32



4-3. Cyber security design description

P. 39



4-4. Risk assessment for the exclusion of computer-based systems

P. 58



4-5. Description of compensating countermeasures

P. 61



4-6. Ship cyber resilience test procedure

P. 63



4-7. Ship cyber security and resilience program

P. 89

In addition to the above documents, Table X2.4 of Chapter 5, Part X (UR E26) requires "Approved supplier documentation". These are the documents that the manufacturer is required to submit to the Society for approval in accordance with Chapter 4, Part X (UR E27). These documents are required to be submitted by the supplier to the integrator during the construction phase. For further details, please refer to the "Guidelines for Cyber resilience of on-board systems and Equipment".

4-1. Vessel asset inventory

Rule Table X2.4 No. 4, Part X of the Rules



Systems integrator: Submit, maintain until completion



Shipowner: Maintain

4-1.1 Overview

The vessel asset inventory is a list of assets owned by the ship, such as computer-based systems and network devices. (For the purpose of the vessel asset inventory, please refer to "Identify" in Chapter 1.)

Specifically, by combining the information of network devices including security devices with the computer-based system Asset Inventory submitted by each supplier based on Part X, Chapter 4 (UR E27) into one table, you can create a vessel asset inventory.

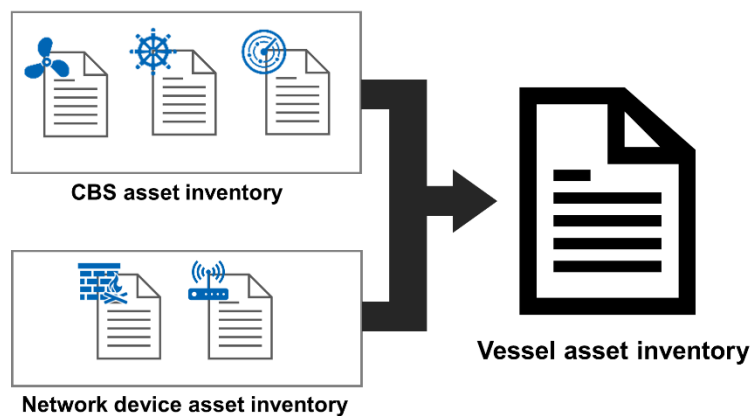


Figure 4.1 Vessel asset inventory

The vessel asset inventory provides efficient change management by making it possible to overview information of the computer-based systems on the ship in a list.

4-1.2 Explanation

Rule 2.2.3-3(6), Part X of the Rules

The content of "Vessel asset inventory" is specified in 5.4.2(1).

The requirements for this document are specified in 5.4.2(1), Part X of the Rules. This requirement, including related requirements, is explained below.

Rule 5.4.2(1)(c), Part X of the Rules

The vessel asset inventory is to include at least the computer-based systems indicated in 5.1.2-1., if present onboard. The inventory is to be kept updated during the entire life of the ship. Software and hardware modifications potentially introducing new vulnerabilities or modifying functional dependencies or connections among systems are to be recorded in the inventory. If confidential information is included in the inventory (e.g. IP addresses, protocols, port numbers), special measures are to be adopted to limit the access to such information only to authorized people.

i) Hardware

- 1) For all hardware devices in the scope of applicability of this Chapter, the vessel asset inventory is to include at least the information in 4.4.1(1).
- 2) In addition, the vessel asset inventory may specify system category and security zone associated with the computer-based system.

ii) Software

- 1) For all software in the scope of applicability of this Chapter (e.g., application program, operating system, firmware), the vessel asset inventory is to include at least the information in 4.4.1(1).
- 2) The software of the computer-based systems in the scope of applicability of this Chapter are to be maintained and updated in accordance with the shipowner's process for management of software maintenance and update policy in the Ship cyber security and resilience program (see 2.2.3-5(7))

The vessel asset inventory should include the following information:

Table 4.1 Example of vessel asset inventory

System	Detailed Machinery / Systems	Updated Log	Security Zone	System Category	Location	Trusted network connected to	Untrusted network connected to	IP address / Port No.	Hardware	Software
								
(1)			(2)						(3)	

The items to be included in the vessel asset inventory are largely divided into the following three parts:

- (1) Information about the system in the ship's network (System, Updated Log, etc.) (See Table 4.2)
- (2) Information about the location and connections of the systems (See Table 4.3)
- (3) Information about the system's hardware and software (See Table 4.4)

Firstly, for the computer-based systems planned to be installed on the ship, list the "System (system name)", "Detailed Machinery / Systems", and "Updated Log".

Table 4.2 (1) Example of information about the computer-based system in the ship's network

System	Detailed Machinery / Systems	Updated Log
Main propulsion systems	Main engine control system (ECS)	
	Main engine remote control system (RCS)	
	Machinery alarm and monitoring systems (AMS, including data loggers)	
Steering system control systems	Steering system	

Additionally, it is recommended to include information about the location and connections of the systems in the inventory. Although there is no requirement to include these details in the inventory itself, this information can be useful for managing ship assets. Please note that this information constitutes confidential information and requires information management based on confidential information requirements. Please refer to "Access Control" in the "Ship Cyber Security and Resilience Plan" for confidential information requirements.



4-7. Ship cyber security and resilience program

5.4.3(4), Part X of the Rules / Access control

P. 100

Additionally, by including "System Category"* in the ship asset inventory, it is possible to use it concurrently with the "list of computer-based systems" required under Part X, Chapter 3 (UR E22).

*The categorization based on the potential severity of the consequences if the system serving the function fails, as determined by the integrator in accordance with Chapter 3, Part X (UR E22).

Table 4.3 (2) Example of information about the computer-based system in the ship's network

Security Zone	System Category	Location	Trusted network connected to	Untrusted network connected to	IP address / Port No.
Main propulsion Zone	III	E/R (E/S)	VDR, RCS	Shore	192.168.xx.x: xxx
		C/R	-	-	192.168.xx.x: xxx
		W/H	-	-	192.168.xx.x: xxx
	II	C/R	VDR, WIAS	Data server	192.168.xx.x: xxx
		W/H Accommodations	-	-	-
Navigation Zone	NA	W/H	-	-	-
		W/H	VDR Radar	ECDIS data server	192.168.xx.x: xxx

For computer-based systems that has obtained approval based on Part X, Chapter 4 (UR E27), the information in (3) of Table 4.1 is basically included in the "Computer-based system asset inventory" provided by the supplier. Therefore, the systems integrator's task is to reflect this information in the vessel asset inventory and, if necessary, refer to the document.

Table 4.4 (3) Example of information about the computer-based system's hardware and software

Detailed Machinery/ Systems	Hardware						Software					
	Name	Brand/ manufacturer	Model/ type	Short description of functionality/ Purpose	Physical interfaces	Supported communication protocols	Brand/ manufacturer	Model/ type	Short description of functionality/ Purpose	Version of Software	OS Version	Firmware Version
XXX	Main Unit	ABC Electronics	MU-01	Control system functions and integrate their subsystems.	LAN (2/2) USB (0/4) Serial (1/1)	TCP/IP USB3.0 Modbus	ABC Electronics	MU-01-LNG	Main engine control system which serves gas fuel (LNG) injection function	1.00	Windows 10 22H2(19045.XXXX)	-
	Wheelhouse panel	NK Display	TFT10.4TP	Control panel for main engine which is located in the W/H	LAN (1/2) USB (1/2)	TCP/IP USB3.0	ABC Electronics	TP-WH-LNG	W/H control of the main engine control system	1.00	Windows 10 22H2(19045.XXXX)	-
	Control room panel	NK Display	TFT10.4TP	Control panel for main engine which is located in the C/R	LAN (1/2) USB (1/2)	TCP/IP USB3.0	ABC Electronics	TP-CR-LNG	C/R control of the main engine control system	1.10	Windows 10 22H2(19045.XXXX)	-
	...											

Rule 5.4.2(1)(d)i)2), Part X of the Rules

The vessel asset inventory is to incorporate the asset inventories of all individual computer-based systems falling under the scope of this Chapter. Any equipment in the scope of this Chapter delivered by the systems integrator is also to be included in the vessel asset inventory.

For network devices (switches, firewalls, routers, etc.) and security devices (IDS, SIEM, etc.) additionally installed by the systems integrator, the systems integrator should fill in the information in (1) to (3) above.

Also, for assets whose information required in this section is unknown at the design phase (e.g., data servers provided by the shipowner), the systems integrator should ask the shipowner for the information shown in Table 4.2 ("System (system name)", "Detailed Machinery / Systems", and

“Updated Log”) and include it in the vessel asset inventory, and fill in the other information as much as possible. If any information cannot be filled in at the time of initial submission, fill in "TBD" and update them as soon as the information is available. This document needs to be finalized by the time of the tests in the commissioning phase.

In any case, the vessel asset inventory needs to be created considering that it must be updated and maintained throughout the ship's lifecycle. If the asset inventory is managed manually, the updating process may be cumbersome. Therefore, systematization is recommended to streamline the updating of the asset inventory and improve its accuracy.

4-2. Zones and conduit diagram

Rule Table X2.4 No.2, Part X of the Rules



Systems integrator: Submit, maintain until completion



Shipowner: Maintain

4-2.1 Overview

The Zones and Conduit Diagram illustrates how systems within the scope of Chapter 5, Part X (UR E26) and other systems are grouped when constructing the network on the ship, and how communication between different groups is controlled, providing both physical and logical information.

This diagram can be drawn by identifying the systems included in the same zone on the ship's network and specifying whether physical or logical separation measures (such as firewalls, VLANs, etc.) required by E26 are in place for communication between zones.

This diagram allows for an easy understanding of the ship's network configuration, thereby enabling efficient maintenance after the ship's delivery.

4-2.2 Explanation

Rule 2.2.3-3(4), Part X of the Rules

The content of “Zones and conduit diagram” is specified in 5.4.3(1)(d)i).

The requirements for this diagram are specified in 5.4.3(1)(d)i), Part X of the Rules. The following explains these requirements, including related ones.

Rule 5.4.3(1)(d)i)2), Part X of the Rules

The Zones and conduit diagram is to illustrate the computer-based systems in the scope of applicability of this Chapter, how they are grouped into security zones, and include the following information:

- clear indication of the security zones,
- simplified illustration of each computer-based system in scope of applicability of this Chapter, and indication of the security zone in which the computer-based system is allocated, and indication of physical location of the computer-based system/equipment,
- reference to the approved version of the computer-based system topology diagrams provided by the suppliers (4.4.1(2)),
- illustration of network communication between systems in a security zone
- illustration of any network communication between systems in different security zones

- (conduits), and
- illustration of any communication between systems in a security zone and untrusted networks (conduits).

The sample diagram explaining the above requirements is as follows:

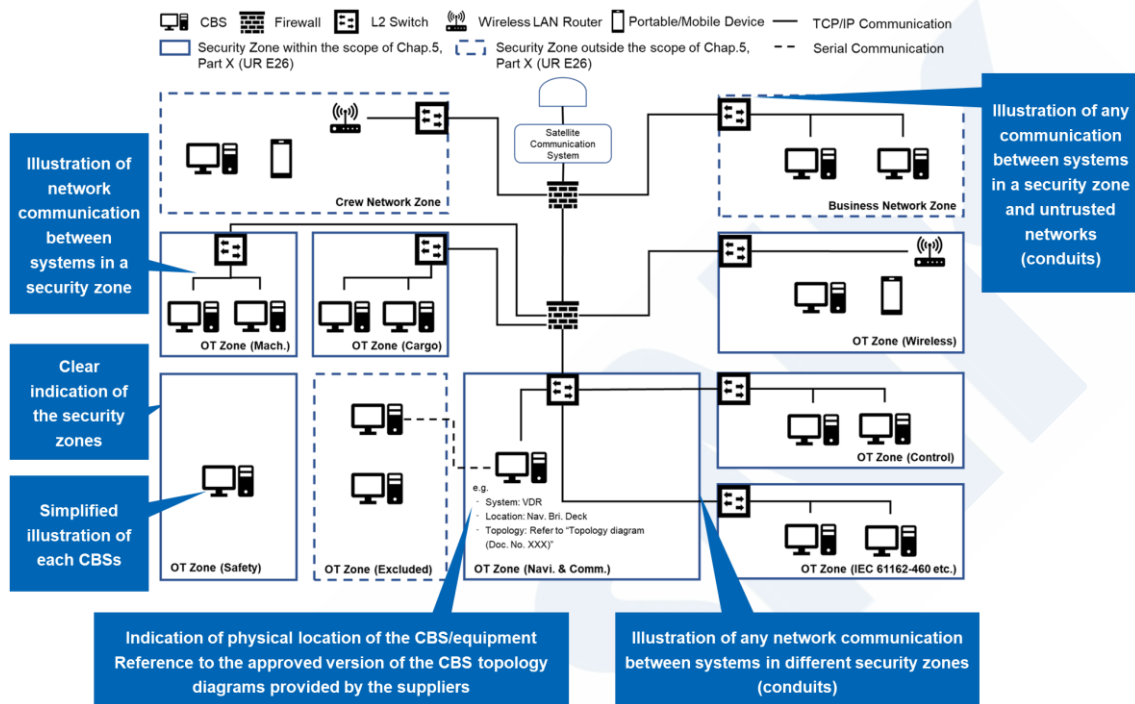


Figure 4.2 Sample Diagram of Zones and Conduits

The following points are crucial for meeting these requirements:

- **Clear Display of Security Zones**

To clarify the scope of Chapter 5, Part X (UR E26), it is necessary to distinctly show the security zones within and outside the scope. In Figure 4.2, zones within the scope are indicated by solid lines, while zones outside the scope are shown by dotted lines. It is important to depict these clearly.

- **Reference to the Approved Version of the System Topology Diagram for computer-based system**

For computer-based system approved under Chapter 4, Part X (UR E27), the supplier provides the topology diagram of the system. The zones and conduit diagram must include references to the diagram names and numbers to allow easy access to the topology diagrams for each computer-based system.

- **Illustration of network communication**

Illustration of network communication must also be included in the zones and conduit diagram.

Network communication that crosses zone boundaries is called a conduit.

The types of communication that need to be documented are determined by whether they cross zone boundaries and whether there is communication with untrusted networks. Specifically, network communication within zones and network communication between applicable security zones (conduits) require documentation of IP communication. On the other hand, communication with untrusted networks requires documentation of discrete signals (ON/OFF contact signals and others, hereinafter referred to as digital signals) and serial communication in addition to IP communication.

Additionally, the zones and conduit diagram must be created to meet the following requirements:

Rule 5.4.3(1)(c), Part X of the Rules

- i) A security zone may contain multiple computer-based systems and networks, all of which are to comply with applicable security requirements given in this Chapter and Chapter 4.
 - ii) The network(s) of a security zone are to be logically or physically segmented from other zones or networks (see also 5.4.3(6)(c)).
 - iii) Computer-based systems providing required safety functions are to be grouped into separate security zones and are to be physically segmented from other security zones.
 - iv) Navigational and communication systems are not to be in same security zone as machinery or cargo systems. If navigation and/or radiocommunication systems are approved in accordance with other equivalent standard(s) (see 4.1.2-2(1)(k)), these systems should be in a dedicated security zone.
 - v) Wireless devices are to be in dedicated security zones (see also 5.4.3(5)).
 - vi) Systems, networks or computer-based systems outside the scope of applicability of this Chapter are considered untrusted networks and are to be physically segmented from security zones required by this Chapter. Alternatively, it is accepted that such systems are part of a security zone if these OT- systems meet the same requirements as demanded by the zone.
 - vii) It is to be possible to isolate a security zone without affecting the primary functionality of the computer-based systems in the zone (see also 5.4.5(3)).
-

Rule 5.4.5(2)(c), Part X of the Rules

- ii) If communication to the remote control system or other computer-based system's is arranged by networks, segmentation and protection safeguards as described in 5.4.3(1) and 5.4.3(2) are to be implemented. This implies that the local control and monitoring system are to be considered a separate security zone. Notwithstanding the above, special considerations can be given to computer-based systems with different concepts on case by case basis.
-

The sample diagram explaining the above requirements is as follows:

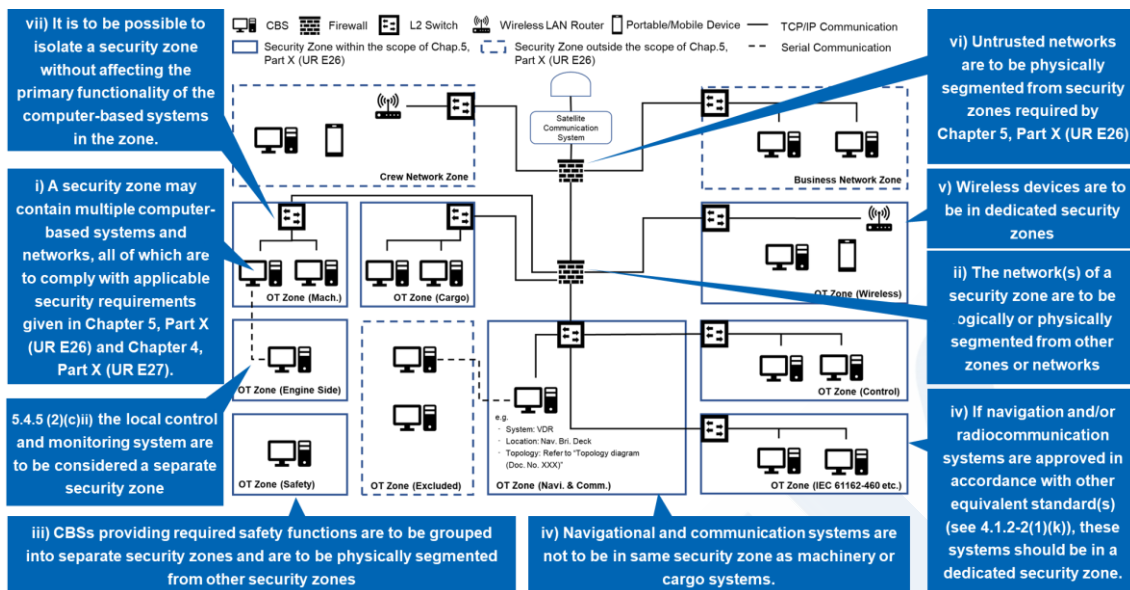


Figure 4.3 Sample Diagram of Zones and Conduits

The following points are crucial for meeting these requirements:

- Computer-based system and Networks Included in Security Zones

The computer-based system and systems connected to both OT and IT systems included in the security zones, as shown in item i) of Figure 4.3, should be pre-approved in accordance with Chapter 4, Part X (UR E27) as indicated in section 2-2.2.2.

- Logical and Physical Network Segmentation

Regarding "Physical Segmentation" and "Logical Segmentation" for items ii), iii), and vi) in Figure 4.3, this section explains the overview using VLAN (Virtual Local Area Network) as an example of logical segmentation methods.

Figure 4.4 shows an overview of physically segmented segments, and Figure 4.5 shows an overview of logically segmented segments using VLAN. The difference between Figure 4.5 a and Figure 4.5 b lies in whether multiple L2 switches* are connected using cascade connections as described below.

*L2 Switch: A network device that operates on a communication method called Ethernet (Layer 2 of the OSI reference model), which forwards communication data based on MAC addresses that are assigned to each computer and used for communication within a narrower range than IP addresses. In contrast, L3 switches operate on a communication method called IP (Layer 3 of the OSI reference model) and forward communication data based on IP addresses.

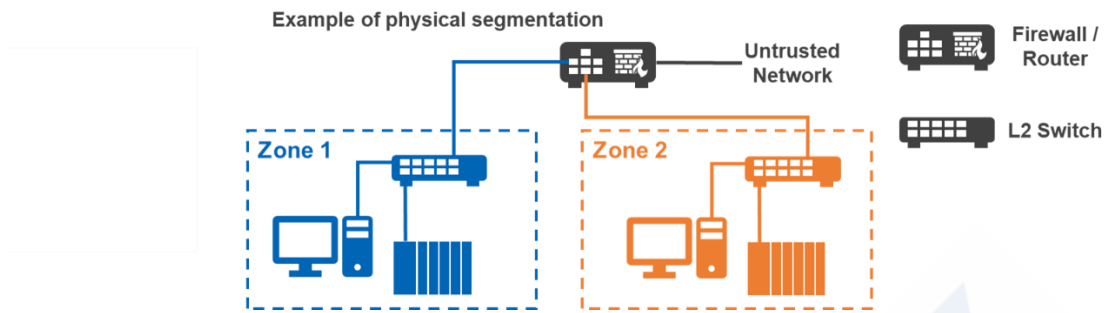


Figure 4.4 Overview Diagram of Physical Segmentation

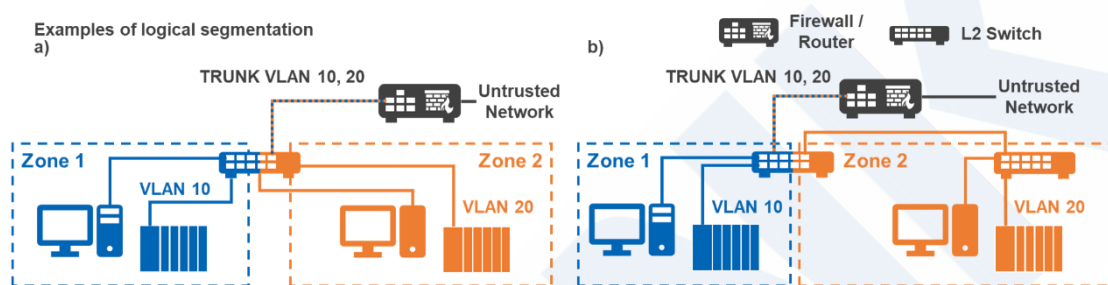


Figure 4.5 Overview Diagram of Logical Segmentation (a: Single L2 Switch Case, b: Cascade Connection of L2 Switches Case)

To understand the logical and physical segmentation of the network as required by Chapter 5, Part X (UR E26), it is helpful to first verify how network segments are defined. A single network segment is defined as the same broadcast domain, consisting of devices connected to one L2 switch (or multiple cascaded L2 switches). All devices within the connected segment can communicate with each other.

*Cascading connection refers to the method of connecting multiple network switches in series to expand the network.

Based on the above, physical segmentation means configuring two or more network segments using at least two L2 switches without sharing the same L2 switch. When two physically segmented network segments communicate, traffic must be controlled using devices such as routers or firewalls. Hereinafter, “Zone boundary devices”).

For both physical segmentation and logical segmentation, the overview of communication paths is shown below of establishing communication from a system in Zone 1 to a system in Zone 2, regarding how communication is conducted via zone boundary devices. In the case of physical separation, as shown in Figure 4.6, the communication path must pass through zone boundary devices at stages ② and ③. On the other hand, in the case of logical segmentation, as shown in Figure 4.7, at each of stages ② and ③ of communication, when the L2 switch detects that the communication crosses zones, instead of forwarding to communication path ④, the communication is forwarded via software to the zone boundary device and traffic control is performed by that device.

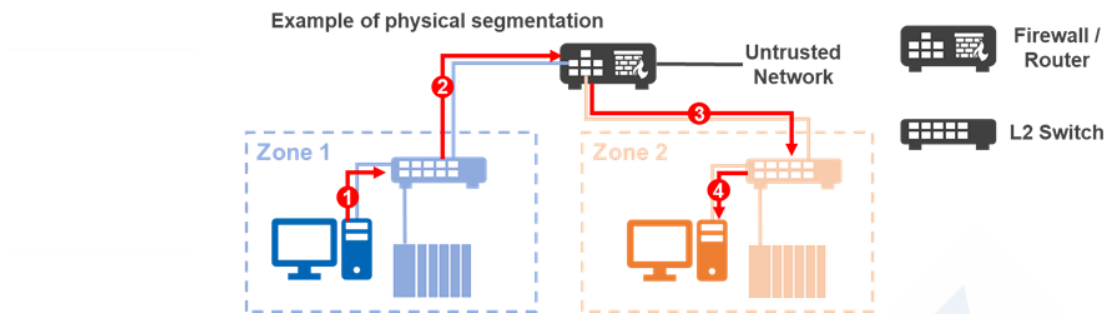


Figure 4.6 Overview of Communication Paths in Physical Segmentation

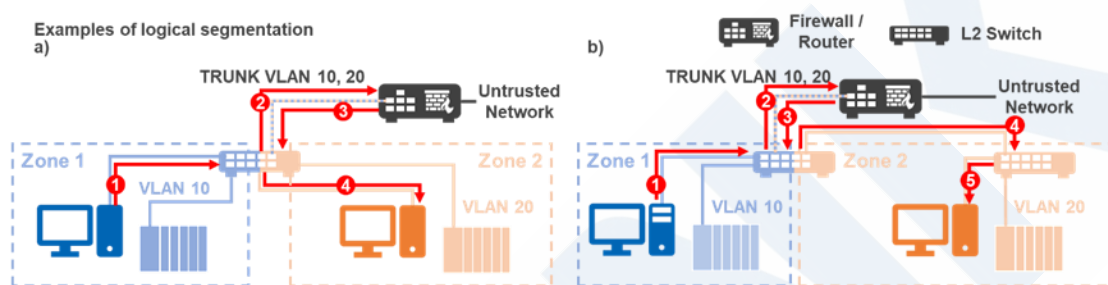


Figure 4.7 Overview of Communication Paths in Logical Segmentation (a: Single L2 Switch Case, b: Cascade Connection of L2 Switches Case)

As described above, logical segmentation means configuring two different network segments using VLANs to virtually separate them within one L2 switch. While the above example explained an implementation using VLAN, various other methods exist, such as subnets and SDN (Software Defined Network).

Furthermore, besides using zone boundary devices, using serial communication, dry contacts, and other methods can achieve zone segmentation.

The following lists the items that require segmentation and whether physical separation or logical separation is acceptable for each:

Table 4.5 Items requiring segmentation and applicable segmentation types (physical vs. logical)

Zones requiring segmentation	Fig. 4.3 Provisions	Physical	Logical
Systems providing required safety functions	iii	Required	NG
Navigational and communication systems, machinery or cargo systems	iv	OK	OK
Wireless devices	v	OK	OK
Untrusted networks	vi	Required	NG
Local control and monitoring system	5.4.5(2)(c) ii)	OK	OK

- Separate Security Zones without Affecting the Primary Functionality of computer-based system within the Security Zone

Regarding item vii) in Figure 4.3, it must be possible to isolate a security zone without affecting the primary functionality of the computer-based system in the zone (see also 5.4.5(3)). This ensures that important functions for the safe navigation of the ship are not interrupted even if there is a disconnection between zones. Therefore, it is necessary to design the zones so that the performance of computer-based system within the zone is not limited when the zones are separated.

Rule 5.4.3(1)(d)i)3), Part X of the Rules

It is to be possible to identify each computer-based system in the Zones and conduit diagram,

In the Zones and conduit diagram, it should be possible to identify each computer-based system within the scope of applicability of this Chapter.

It is not mandatory to include all communication protocols in the Zones and conduit diagram, but if communication protocols are relevant for distinguishing zones, it may be necessary to include them.

4-3. Cyber security design description

Rule Table X2.4 No.3, Part X of the Rules



Systems integrator: Submit, maintain until completion



Shipowner: Maintain

4-3.1 Overview

The Cyber Security Design Description is a document that summarizes the technical measures contributing to the requirements of defense, response, and recovery at both the network level and device level.

This document aims to enable the shipowner to easily understand the security capabilities of each system and network when preparing the Ship Cyber Security and Resilience Program, and to provide easy access to the necessary reference documents. Specifically, at the device level, it organizes the information received from suppliers regarding functionalities and links the necessary documents. At the network level, it involves organizing the policies for zone separation, measures between zones, endpoint measures, and physical measures.

4-3.2 Explanation

Rule 2.2.3-3.(5), Part X of the Rules

The content of “Cyber security design description (CSDD)” is specified in subsections “Design phase” for each requirement in 5.4.

The requirements for this document are specified in 5.4, Part X of the Rules. These requirements are explained in section 4-3.3.

4-3.3 Explanation of Each Requirement in Functional Elements

In this document, it is necessary to meet the requirements specified in each functional element. Detailed explanations of each requirement are provided below.



5.4.3, Part X of the Rules / Protect



5.4.3(1), Part X of the Rules / Security zones and network segmentation

P. 41














5.4.3(3), Part X of the Rules / Antivirus, antimalware, antispam and other protections from malicious code

P. 43



5.4.3(4), Part X of the Rules / Access control

P. 46

	5.4.3(5), Part X of the Rules / Wireless communication	P. 46
	5.4.3(6), Part X of the Rules / Remote access control and communication with untrusted networks	P. 48
	5.4.3(7), Part X of the Rules / Use of mobile and portable devices	P. 51
	5.4.5 Part X of the Rules / Respond	
	5.4.5(1), Part X of the Rules / Incident response plan	P. 53
	5.4.5(2), Part X of the Rules / Local, independent and/or manual operation	P. 54
	5.4.5(3), Part X of the Rules / Network isolation	P. 54
	5.4.5(4), Part X of the Rules / Fallback to a minimal risk condition	P. 54
	5.4.6 Part X of the Rules / Recover	
	5.4.6(1), Part X of the Rules / Recovery plan	P. 56
	5.4.6(3), Part X of the Rules / Controlled shutdown, reset, roll-back and restart	P. 57



Protect

5.4.3(1), Part X of the Rules / Security zones and network segmentation

This item concerns the requirements for configuring security zones and network segments in network design. As explained in the zones and conduit diagram, networks are required to be properly segmented. In the cyber security design description, it is required to describe in detail how segmentation was implemented in the network design.

Rule 5.4.3(1)(d) i) 3), Part X of the Rules

The systems integrator is to include the following information in the cyber security design description:

- a short description of the computer-based systems allocated to the security zone. It is to be possible to identify each computer-based system in the Zones and conduit diagram,
- network communication between computer-based systems in the same security zone. The description is to include purpose and characteristics (i.e. protocols and data flows) of the communication,
- network communication between computer-based systems in different security zones. The description is to include purpose and characteristics (i.e. protocols and data flows) of the communication. The description is to also include zone boundary devices and specify the traffic that is permitted to traverse the zone boundary (e.g. firewall rules), and
- any communication between computer-based systems in security zones and untrusted networks. The description is to include discrete signals, serial communication, and the purpose and characteristics (i.e. protocols and data flows) of IP-based network communication. The description is to also include zone boundary devices and specify the traffic that is permitted to traverse the zone boundary (e.g. firewall rules).

The specific items that need to be documented in the cyber security design description are as follows.

When documenting network configurations based on this item, this information may constitute confidential information depending on the policies of stakeholders such as shipowners and manufacturers. Therefore, they must be implemented with consideration for facilitating management as confidential information. For requirements regarding confidential information, please refer to "Access Control" in the "Ship Cyber Security and Resilience Program."



4-7. Ship cyber security and resilience program

5.4.3(4), Part X of the Rules / Access control

P. 100

- **a short description of the computer-based systems allocated to the security zone. It is to be possible to identify each computer-based system in the Zones and conduit diagram,**

Please clearly specify the names, uses, and purposes of the computer-based system included in each security zone. Each computer-based system needs to be verifiable when compared with the zones and conduit diagram, therefore measures such as standardizing naming conventions are required.

- **network communication between computer-based systems in the same security zone. The description is to include purpose and characteristics (i.e. protocols and data flows) of the communication,**

For IP communication among computer-based systems within each security zone, the following content must be documented:

- Purpose of communication: Briefly specify the purpose of the communication.
- Communication protocol: Specify the protocol used for the communication.
- Data flow: Specify the origin, destination, and the nodes (e.g., firewalls) that the communication passes through, as well as the direction of the communication.

- **network communication between computer-based systems in different security zones. The description is to include purpose and characteristics (i.e. protocols and data flows) of the communication. The description is to also include zone boundary devices and specify the traffic that is permitted to traverse the zone boundary (e.g. firewall rules).**

For communication between applicable security zones, content equivalent to the requirements for communication within the same security zone must be documented.

In addition, for communication between security zones, it is necessary to specify the firewall rules. Firewall rules are a set of policies configured to control traffic passing through the network. By setting rules to allow or deny specific traffic, communication is restricted to necessary traffic only. For example, firewall rules may specify the allowed source and destination IP addresses, port numbers, and protocols.

- **any communication between computer-based systems in security zones and untrusted networks. The description is to include discrete signals, serial communication, and the purpose and characteristics (i.e. protocols and data flows) of IP-based network communication. The description is to also include zone boundary devices and specify the traffic that is permitted to traverse the zone boundary (e.g. firewall rules).**

For communication between each applicable security zone and untrusted networks, content equivalent to communication between applicable security zones must be included.

In addition, for communication between security zones and untrusted networks, it is necessary to include all discrete signals (digital signals) and serial communication.

5.4.3(2), Part X of the Rules / Network protection safeguards

Rule 5.4.3(2)(d) i), Part X of the Rules

No requirements.

5.4.3(3), Part X of the Rules / Antivirus, antimalware, antispam and other protections from malicious code

This item concerns requirements for countermeasures against malware, which refers to maliciously created software including viruses. This requirement demands countermeasures to prevent malware infection at both individual computer-based system level and network level. In the cyber security design description, it is necessary to describe the malware countermeasure methods implemented for each control system, document how these are maintained, and describe the methods to be taken when such measures are supplemented operationally.

Part X 5.4.3(3)(c) The requirement details state the following.

Rule 5.4.3(3)(c), Part X of the Rules

- i) Malware protection is to be implemented on computer-based systems in the scope of applicability of this Chapter. On computer-based systems having an operating system for which industrial-standard anti-virus and anti-malware software is available and maintained up-to-date, anti-virus and/or anti-malware software is to be installed, maintained and regularly updated, unless the installation of such software impairs the ability of computer-based system to provide the functionality and level of service required (e.g. for Category II and Category III computer-based systems performing real-time tasks).
- ii) On computer-based systems where anti-virus and anti-malware software cannot be installed, malware protection is to be implemented in the form of operational procedures, physical safeguards, or according to manufacturer's recommendations.

- Malware protection is to be implemented on computer-based systems in the scope of applicability of this Chapter.

To reduce the cyber risk from viruses, malware, spam, and malicious code, countermeasures need to be implemented on computer-based systems.

- On computer-based systems having an operating system for which industrial-standard anti-virus and anti-malware software is available and maintained up-to-date, anti-virus and/or anti-malware software is to be installed, maintained and regularly updated,

If using a general-purpose OS such as Windows or Linux, it is necessary to install industry-standard antivirus and/or anti-malware software, and to maintain and regularly update it.

There are two types of anti-malware software: blacklist and whitelist. The former stores the characteristic code (signature) of malware or suspicious behavior (behavior) as a definition file, and detects malware by comparing it with the definition file. If this definition file becomes outdated, it will not be able to cope with new threats, so it is necessary to keep updating it continuously. On the other hand, the latter requires specifying the programs to be allowed in advance, but there is no need to update the definition file, and only the response to software changes is required. Anti-malware software needs to be selected by understanding these characteristics and considering the characteristics of the system.

- **unless the installation of such software impairs the ability of computer-based system to provide the functionality and level of service required (e.g. for Category II and Category III computer-based systems performing real-time tasks).**

However, for computer-based systems where real-time task execution is important, and the installation of such software impairs the ability to provide the required functionality and level of service, the installation of such software is not required.

- **On computer-based systems where anti-virus and anti-malware software cannot be installed, malware protection is to be implemented in the form of operational procedures, physical safeguards, or according to manufacturer's recommendations.**

On the other hand, if such software cannot be installed, including cases excluded by the preceding paragraph, malware protection must be implemented in the form of operational procedures, physical safeguards, or according to the manufacturer's recommendations.

The above are the requirements for antivirus and antimalware measures. Based on the above, the cyber security design description must include the following information.

Rule 5.4.3(3)(d) i), Part X of the Rules

The systems integrator is to include the following information in the Cyber security design description:

- 1) For each computer-based system, summary of the approved mechanisms provided by the supplier for protection against malicious code or unauthorized software.
 - 2) For computer-based systems with anti-malware software, information about how to keep the software updated.
 - 3) Any operational conditions or necessary physical safeguards to be implemented in the shipowner's management system.
-

- **1) For each computer-based system, summary of the approved mechanisms provided by the supplier for protection against malicious code or unauthorized software.**

This states that it is necessary to document an overview of the security functions provided by the

supplier to protect against malicious code or unauthorized software so that it can be understood what security functions are implemented.

Specifically, it is necessary to describe how the security functions work to prevent the corresponding threats and vulnerabilities.

For this section, you can refer to the measures taken by each system supplier against the requirements of Part X, Chapter 4, Table X4.1 "18. Protection from malicious code." For details, please refer to Chapter 5, "18. Malicious code protection" of "Guidelines for Cyber resilience of on-board systems and equipment." (P 101).

- **2) For computer-based systems with anti-malware software, information about how to keep the software updated.**

For computer-based systems with anti-malware software, the software needs to be updated when new threats or vulnerabilities that should be addressed by the software update are discovered. Also, if the anti-malware software is blacklist-based, the malware definition file needs to be kept up-to-date in addition to this.

This states that for computer-based systems with anti-malware software, it is necessary to document how to continuously update the software.

Specifically, it is necessary to describe the process of obtaining update files or patch files provided by suppliers, etc., when new threats or vulnerabilities that require updating the anti-malware software are discovered, and the process of applying those files.

- **3) Any operational conditions or necessary physical safeguards to be implemented in the shipowner's management system.**

Viruses, malware, spam, and malicious code need to be addressed by operations and physical safeguards implemented according to the shipowner's management system.

This states that these operational conditions and physical safeguards for security measures also need to be documented.

Specifically, the following are examples of the content:

Operational conditions:

It is necessary to describe operational conditions regarding the introduction of intrusion detection systems (IDS), the use of email and its attachments, websites and web services, scanning removable media (e.g., USB devices, floppy disks, or CDs) for malware before connection, and network connection restrictions.

Physical safeguards:

In accordance with the requirement details of Part X 5.4.3(3)(c) ii), it is necessary to describe physical safeguards such as the adoption of physical access control, such as placing computer-based systems in lockable rooms or storage, or blocking physical ports to protect computer-based systems where antivirus and antimalware software cannot be installed from malware.

5.4.3(4), Part X of the Rules / Access control

Rule 5.4.3(4)(d) i), Part X of the Rules

The systems integrator is to include the information related to location and physical access controls for the computer-based systems in the Cyber security design description. Devices providing Human Machine Interface (HMI) for operators needing immediate access need not enforce user identification and authentication provided they are located in an area with physical access control. Such devices are to be specified.

This section aims to prevent attackers from accessing the ship's systems and data through access control. Access control includes logical methods to control the access rights granted to personnel and physical methods of installing computer-based systems in lockable rooms or controlled spaces. However, for computer-based systems related to the safe operation of the ship (Category II or III) that require immediate access, consideration should be given to allow easy access for authorized personnel.

Please include the following information in the Cyber security design description:

- **Locations where computer-based systems are installed and an overview of physical access control**
- **A list of computer-based systems that require immediate access**

With regard to physical access control, this can be addressed by installation in lockable rooms, controlled spaces, or lockable cabinets or consoles, with reference to the following requirements.

Rule 5.4.3(4)(c) i), Part X of the Rules

Computer-based systems of Category II and Category III are to generally be located in rooms that can normally be locked or in controlled space to prevent unauthorized access or are to be installed in lockable cabinets or consoles. Such locations or lockable cabinets/consoles are to be however easy to access to the crew and various stakeholders who need to access to computer-based systems for installation, integration, operation, maintenance, repair, replacement, disposal etc. so as not to hamper effective and efficient operation of the ship.

5.4.3(5), Part X of the Rules / Wireless communication

Wireless communication includes Wi-Fi for local communication, mobile communication technologies for external communication, and other high-frequency wireless communication technologies. Compared to wired communication, these are difficult to physically protect and carry cyber risks such as interception and tampering by untrusted devices. The aim is to require more strict

requirements for such high-risk wireless communications by restricting access to only authorized devices and clarifying firewall rules, etc.

Rule 5.4.3(5)(d) i), Part X of the Rules

The systems integrator is to include the description of wireless networks in the scope of applicability of this Chapter and how these are implemented as separate security zones in the Cyber security design description. The description is to include zone boundary devices and specify the traffic that is permitted to traverse the zone boundary (e.g. firewall rules)

This requirement necessitates describing how wireless networks are implemented in the Cyber security design description.

The design conditions for wireless networks need to meet the following conditions specified as requirement details:

Rule 5.4.3(5)(c), Part X of the Rules

- i) Cryptographic mechanisms such as encryption algorithms and key lengths in accordance with industry standards and best practices are to be applied to ensure integrity and confidentiality of the information transmitted on the wireless network.
 - ii) Devices on the wireless network are to only communicate on the wireless network (i.e. they are not to be “dual-homed”)
 - iii) Wireless networks are to be designed as separate segments in accordance with 5.4.3(1) and protected as per 5.4.3(2).
 - iv) Wireless access points and other devices in the network are to be installed and configured such that access to the network can be controlled.
 - v) The network device or system utilizing wireless communication is to provide the capability to identify and authenticate all users (humans, software processes or devices) engaged in that communication.
-

- i) Cryptographic mechanisms for wireless network

When using wireless networks, encryption mechanisms need to be adopted to reduce the risk of interception and tampering. For details, please refer to "17. Communication integrity" (P 98) and "22. Use of cryptography" (P 113) in Chapter 5 of the "Guidelines for Cyber resilience of on-board systems and equipment".

- ii) Only communicate on the wireless network (Not to connect wired networks)

Devices connecting to wireless networks need to be in independent segments as the next item. Therefore, connection via wired connection ports that may communicate with other segments needs to be prohibited. If there are such ports, please take physical measures using port blockers or logical

communication prevention measures using software.

- **iii) Separated segmentation for wireless networks**

Devices connecting to wireless networks are more vulnerable compared to wired devices. Therefore, when an incident occurs on a wireless network, it is necessary to prevent the spread of damage to other segments by isolating the segment (by using Firewall, L3 switch, etc.).

- **iv) Control of devices and access points to wireless networks**

Devices connecting to wireless networks and access points providing them need to be capable of control such as authorization, monitoring, and usage restrictions to prevent malicious network connections. For details, please see "9. Wireless use control" (P 78) in Chapter 5 of the "Guidelines for Cyber resilience of on-board systems and equipment".

- **v) Identification of devices and users by each device in wireless networks**

Attackers on wireless networks may access from unexpected ranges using methods such as amplifying wireless communication or using directional antennas. Therefore, authentication functions need to be provided as physical access control is difficult compared to wired connections. For authentication methods, please see "5. Wireless access management" (P 67) in Chapter 5 of the "Guidelines for Cyber resilience of on-board systems and equipment".

5.4.3(6), Part X of the Rules / Remote access control and communication with untrusted networks

These are requirements for implementing more stringent measures in remote access control and communication with untrusted networks, which have high security risks.

Rule 5.4.3(6)(d) i), Part X of the Rules

The systems integrator is to include the following information in the Cyber security design description:

- 1) Identification of each computer-based system in the scope of applicability of this Chapter that can be remotely accessed or that otherwise communicates through the security zone boundary with untrusted networks.
 - 2) For each computer-based system, a description of compliance with requirements in 5.4.3(6)c), as applicable.
-

- **The systems integrator is to include the following information in the Cyber security design description:**

For this item, it is necessary to identify devices that perform remote access and to include descriptions in the Cyber security design description as specified in the following requirements, in

order to confirm that appropriate countermeasures are implemented for each device.

- **Identification of each computer-based system in the scope of applicability of this Chapter that can be remotely accessed or that otherwise communicates through the security zone boundary with untrusted networks.**

This item states that the Cyber security design description needs to specify whether each computer-based system is remotely accessible or if connection via untrusted networks is performed.

Therefore, among the defense requirements, for the "network communication between computer-based systems in the same security zone" required to be described in X5.4.3(1) "Security zones and network segmentation", those that are remotely accessible or have communication with untrusted networks need to be specifically noted.

- **For each computer-based system, a description of compliance with requirements in 5.4.3(6)c, as applicable.**

For computer-based systems that allow remote access or communication with untrusted networks, measures for that purpose are necessary. Furthermore, special consideration needs to be given to systems for which remote maintenance such as remote system changes are performed.

As a necessary consideration in the design phase, devices that are remotely accessible need to implement the measures described in regulation X5.4.3(6)c)iii)(1). Also, devices that are remotely maintained need to implement the measures described in regulation X5.4.3(6)c)iii)(2).

Their contents are shown below.

Firstly, all devices that are remotely accessible are required to satisfy the following:

- **have the capability to terminate a connection from the onboard connection endpoint. Any remote access are not to be possible until explicitly accepted by a responsible role on board.**

From the standpoint that connection needs to be managed by authorized crew members onboard, it is required that connection can be terminated from an onboard endpoint, and that permission by a responsible role onboard is required to make access. These can be implemented as a function of the endpoint to request access permission by an authorized person, and operational methods such as power management of VPN devices necessary for remote access and management of network cable connection can also be adopted.

For the former, please see "35. Access via Untrusted Networks" (P 147) and "37. Remote session termination" (P 151) in Chapter 5 of the "Guidelines for Cyber resilience of on-board systems and equipment". For the latter, please see "36. Explicit access request approval" (P 149).

- **be capable of managing interruptions during remote sessions so as not to compromise the safe functionality of OT systems or the integrity and availability of data used by OT systems.**

Regarding remote access to OT systems, OT systems are supposed to execute session management functions such as "41. Invalidation of session IDs after session termination" (P 162) in Chapter 5 of the "Guidelines for Cyber resilience of on-board systems and equipment" when a session is interrupted. At this time, it is required that safety functions and data of OT devices can be utilized without compromising integrity and availability.

- **provide a logging function to record all remote access events and retain for a period of time sufficient for offline review of remote connections, e.g. after detection of a cyber incident.**

Each computer-based system is required to have a function to record auditable events as an audit log. Regarding these, devices that perform remote access need to record events related to remote access (success and failure of login attempts, changes in access privileges, establishment and termination of sessions, and connection destinations). It is required that their log items are sufficient for performing remote access and that sufficient recording capacity is secured.

For details, please refer to "13. Auditable events" (P 88) and "14. Audit storage capacity" (P 91) in Chapter 5 of the "Guidelines for Cyber resilience of on-board systems and equipment".

Among them, devices for which remote maintenance may be performed need to satisfy the following:

- **Documentation is to be provided to show how they connect and integrate with the shore side.**

In order to clarify the procedure for performing maintenance by remote access, it is necessary to create a document that clearly states the procedure for connecting with the shore side.

- **Security patches and software updates are to be tested and evaluated before they are installed to ensure they are effective and do not result in side effects or cyber events that cannot be tolerated. A confirmation report from the software supplier towards above are to be obtained, prior to undertaking remote update.**

In the case of remote maintenance, if unacceptable vulnerabilities are caused by updating the software of the device, it will have a greater adverse effect compared to on-site updates. Therefore, the impact of updates needs to be particularly confirmed in advance in the case of remote maintenance.

- **Suppliers are to provide plans for- and make security updates available to the shipowner (see 4.5.3, 4.5.4 and 4.5.5).**

When updating, plans by the supplier need to be available to the shipowner in advance so that the shipowner can determine whether they can be accepted or should be accepted. The

Cyber security design description needs to include references to those documents created by the supplier.

For the details, please see "2. Security update documentation" (P 169), "3. Dependent component or operating system security update documentation" (P 171), and "4. Security update delivery" (P 173) in Chapter 6 of the "Guidelines for Cyber resilience of on-board systems and equipment".

- **At any time, during remote maintenance activities, authorized personnel is to have the possibility to interrupt and abort the activity and roll back to a previous safe configuration of the computer-based system and systems involved.**

If a failure occurs or there is a need to suspend due to remote maintenance of the software, it is necessary to be able to safely interrupt the maintenance and roll back to the original state. Therefore, functions for suspending work by authenticated personnel remotely or onboard and for restoring the software to the state before remote maintenance are required.

- **Multi-factor authentication is required for any access by human users to computer-based system's in scope from an untrusted network.**

In remote maintenance, it becomes possible to easily change software, setting values, etc. by remote access, not just mere remote access. Therefore, multi-factor authentication is required as an authentication method.

For details of multi-factor authentication, please see "31. Multifactor authentication for human users" (P 136) in Chapter 5 of the "Guidelines for Cyber resilience of on-board systems and equipment".

- **After a configurable number of failed remote access attempts, the next attempt is to be blocked for a predetermined length of time.**

In remote maintenance, in order to prevent unauthorized access by attacks such as brute-force attacks, it is necessary to provide a function to make access attempts impossible for a predetermined time when access attempts fail several times.

For details, please see "33. Unsuccessful login attempts" (P 142) in Chapter 5 of the "Guidelines for Cyber resilience of on-board systems and equipment".

- **If the connection to the remote maintenance location is disrupted for some reason, access to the system is to be terminated by an automatic logout function.**

If the connection is interrupted for reasons such as communication disruption and the remote session continues without being terminated, it may lead to unauthorized access. Therefore, a function is required to terminate access to the system when the connection is interrupted.

5.4.3(7), Part X of the Rules / Use of mobile and portable devices

Rule 5.4.3(7)(d) i), Part X of the Rules

The systems integrator is to include the information related to any computer-based systems in the scope of applicability that do not meet the requirements in No.10 in Table X4.1, i.e., that are to have protection of interface ports by physical means such as port blockers in the Cyber security design description.

The use of mobile and portable devices needs to be limited to the specific functions or activities in accordance with 10 in Table X4.1, Part X of the Rules. The transfer of code and data to/from portable and mobile devices also needs be restricted. For any computer-based systems that cannot fully meet this requirement, unused ports need to be protected from unauthorized cable or device connections by physical means such as lockable port blockers. (To determine whether a computer-based system meets this requirement, please refer to the description of security capabilities (4.4.1(3), Part X of the Rules) submitted by the manufacturer.)

The cyber security design description needs to include information related to components that require port protection by such physical means (e.g., a list of devices that require physical port protection).

For details, please see "10. Use control for portable and mobile devices" (P 81) in Chapter 5 of the "Guidelines for Cyber resilience of on-board systems and equipment".



Respond

5.4.5(1), Part X of the Rules / Incident response plan

Rule 5.4.5(1)(d) i), Part X of the Rules

The systems integrator is to include the references to information provided by the suppliers (see 4.4.1(8)) that may be applied by the shipowner to establish plans for incident response in the Cyber security design description.

This section aims to efficiently reference information necessary for shipowners to develop Incident response plans. Although the Incident response plan is created by the shipowner, onboard computer-based systems are complexly configured. Therefore, to enable the shipowner to create an accurate Incident response plan, it is necessary to gather information from stakeholders that the shipowner alone cannot know.

Additionally, the Incident response plan needs to include references to information provided by suppliers, and it is required to create a list of documents that can reference each computer-based system and its information in the Cyber security design description.

Rule 4.4.1(8), Part X "Information supporting the owner's incident response and recovery plan"

This document is to be submitted to the Society upon request and is to include procedures or instructions allowing the user to accomplish the following:

- (a) local independent control (see 5.4.5(2)),
- (b) network isolation (see 5.4.5(3)),
- (c) forensics by use of audit records (see No.13 in Table X4.1),
- (d) deterministic output (see 5.4.5(4) and No.20 in Table X4.1),
- (e) backup (see No.26 in Table X4.1),
- (f) restore (see No.27 in Table X4.1), and
- (g) controlled shutdown, reset, roll-back and restart (see 5.4.6(3)).

The documents that should be referenced in the cyber incident response plan are (a), (b), and (d) among the "Information supporting the owner's incident response and recovery plan" specified in Part 4.4.1(8), Part X of the Rules.

Table 4.5 List of Documents Referencing Incident Response Plan

Computer-based system	Product name	Relevant Documents
Main Engine Control System	***	Local independent control (Reference No. : ***)

5.4.5(2), Part X of the Rules / Local, independent and/or manual operation

Rule 5.4.5(2)(d) i), Part X of the Rules

The systems integrator is to include the description of how the local controls specified in Regulation 31, Chapter II-1, SOLAS are protected from cyber incidents in any connected remote or automatic control systems in the Cyber security design description.

This section aims to confirm the details of how local control is protected from cyber incidents in the connected remote or automatic control systems. Regulation 31, Chapter II-1, SOLAS specifies that in case of failure of any part of the remote control locations, the propulsion machinery and the auxiliary machinery, essential for the propulsion and safety of the ship are to be controlled locally.

Specifically, the Cyber security design description needs to include descriptions or diagrams that show how local control is independent from remote or automatic control systems.

5.4.5(3), Part X of the Rules / Network isolation

Rule 5.4.5(3)(d) i), Part X of the Rules

The systems integrator is to include the information related to Specification of how to isolate each security zone from other zones or networks in the Cyber security design description. The effects of such isolation is also to be described, demonstrating that the computer-based systems in a security zone do not rely on data transmitted by IP-networks from other zones or networks.

This section aims to clarify the methods for isolating each security zone and the impact of isolation. This information can be used for instructions and procedures for isolation in the event of a cyber incident, as described in the Incident response plan.

When a cyber incident occurs in a security zone, crew can minimize the impact on other security zones by promptly isolating that security zone. Additionally, for systems that operate depending on data from other systems, isolating a security zone may cause a transition from normal operation to what is called degraded mode, which is the minimum level of operation. Therefore, this should be clearly stated in the Cyber security design description, and countermeasures should be indicated.

5.4.5(4), Part X of the Rules / Fallback to a minimal risk condition

Rule 5.4.5(4)(d) i), Part X of the Rules

The systems integrator is to include the information related to specification of safe state for the control functions in the computer-based systems in the scope of applicability of this Chapter in the Cyber security design description.

This section aims to clarify what the safe state of each computer-based system is and how to achieve

that state. Fallback to a minimal risk condition varies depending on environmental conditions, the stage of the ship's voyage (e.g., whether it is entering/leaving port or in ocean navigation), and the event that has occurred. Therefore, it is required to consider various situations.

The cyber security design description needs to include information on what the safe state specified by the supplier constitutes for these minimal risk conditions.

The following are listed as fallbacks to a minimal risk condition:

- **Bringing the system to a complete stop or other safe state (5.4.5(4)(c)i1))**
By completely shutting down the system or transitioning it to a safe state, it is possible to minimize the impact of a cyber incident.
- **Disengaging the system (5.4.5(4)(c)i2))**
By disengaging the system, it is possible to suppress the impact of a cyber incident on other systems and prevent the spread of damage.
- **Transferring control to another system or human operator (5.4.5(4)(c)i3))**
In case of a security incident against the control system, it is possible to minimize the impact of the security incident by transferring control to a system that has not been attacked or by directly controlling it by crew.



Recover

5.4.6(1), Part X of the Rules / Recovery plan

Rule 5.4.6(1)(d) i), Part X of the Rules

The systems integrator is to include the references to information provided by the suppliers (4.4.1(8)) that may be applied by the shipowner to establish plans to recover from cyber incidents in the Cyber security design description.

This section focuses on enabling shipowners to efficiently reference the information necessary for developing recovery plans to be implemented following the impact of cyber incidents. Developing recovery plans without any relevant documentation is challenging for shipowners because configurations of onboard computer-based systems are complex. Therefore, it is necessary to gather information from stakeholders needed for recovery plans.

The cyber security design description is to include information from documents prepared by suppliers that should be referenced for developing recovery plans.

- the references to information provided by the suppliers (4.4.1(8)) that may be applied by the shipowner to establish plans to recover from cyber incidents

This requirement indicates that reference to the document "Information to support shipowner incident response and recovery plans," which is required as supplier submission documentation in Chapter 4, Part X of the Rules (UR E27), is necessary. The content of this document is as follows:

Rule 4.4.1(8), Part X "Information supporting the owner's incident response and recovery plan"

This document is to be submitted to the Society upon request and is to include procedures or instructions allowing the user to accomplish the following:

- (a) local independent control (see 5.4.5(2)),
- (b) network isolation (see 5.4.5(3)),
- (c) forensics by use of audit records (see No.13 in Table X4.1),
- (d) deterministic output (see 5.4.5(4) and No.20 in Table X4.1),
- (e) backup (see No.26 in Table X4.1),
- (f) restore (see No.27 in Table X4.1), and
- (g) controlled shutdown, reset, roll-back and restart (see 5.4.6(3)).

The reference materials to be consulted in the recovery plan are specified in Regulation X, Part 4.4.1(8) as "Information Supporting the Shipowner's Incident Response and Recovery Plan," specifically items (c), (e), (f), and (g).

This requirement mandates the creation of a list of documents that can be referenced for information related to each computer-based system.

Table 4.6 List of Documents Referencing Recovery Information

Computer-based system	Product Name	Relevant Documents
Main Engine Control System	***	Recovery Plan (Reference No. : ***)

5.4.6(2), Part X of the Rules / Backup and restore capability

Rule 5.4.6(2)(d) i), Part X of the Rules

No requirements.

5.4.6(3), Part X of the Rules / Controlled shutdown, reset, roll-back and restart

Rule 5.4.6(3)(d) i), Part X of the Rules

The systems integrator is to include the references to product manuals or procedures describing how to safely shut down, reset, restore and restart the computer-based systems in the scope of applicability of this Chapter in the Cyber security design description.

This item stipulates content related to a series of procedures that includes safely shutting down systems using secure procedures, resetting them to their initial state or restoring them to their normal state, and restarting the systems, as part of the procedures necessary to restore systems to their normal operational state after the effects of cyber incidents have been eliminated.

The cyber security design description needs to include references to documentation prepared by suppliers regarding these methods.

The references to product manuals or procedures describing how to safely shut down, reset, restore and restart the computer-based systems in the scope of applicability of this Chapter

This refers to the product manuals or procedures that explain how to safely shut down, reset, restore, and restart each computer-based system. This information is specified in Chapter 4, Part X (UR E27) as "Information Supporting the Shipowner's Incident Response and Recovery Plan" to be submitted by the supplier. Therefore, the requirement in Chapter 5.4.6(1) for "a list of documents that can be referenced for information related to each computer-based system" is fulfilled by creating such a list.

4-4. Risk assessment for the exclusion of computer-based systems

Rule Table X2.4 No.5, Part X of the Rules



Systems integrator: Submit, maintain until completion



Shipowner: Maintain

4-4.1 Overview

The risk assessment for excluding a computer-based system from the scope of Chapter 5, Part X (UR E26) is a document that proves the security risks of the system are sufficiently mitigated when [excluding a computer-based system within the scope of Chapter 5, Part X \(UR E26\) from its application](#). If a computer-based system meets the "Acceptance Criteria" defined in this requirement and a risk assessment is conducted, and the Society determines that it is not necessary to apply Chapter 5, Part X (UR E26) to the system, it may be excluded from the scope of application. This document must list the excluded computer-based system and prove that the "Acceptance Criteria" and "Additional Criteria" explained below are met. Note that this document must be prepared by the systems integrator, not the supplier.

4-4.2 Explanation

Rule 2.2.3-3(7), Part X of the Rules

The content of "Risk assessment for the exclusion of computer-based systems" is specified in 5.5.

The requirements for this document are specified in 5.5, Part X of the Rules. Important points in this document in this requirement are explained below.

Rule 5.5.4-1, Part X of the Rules

Exclusion of a computer-based system falling under the scope of applicability of this Chapter from the application of relevant requirements can be accepted by the Society only if assurance is given that the operation of the computer-based system has no impact on the safety of operations regarding cyber risk. The said exclusion may be accepted for a computer-based system which does not fully meet the additional criteria listed below but is provided with a rational explanation together with evidence and is found satisfactory by the Society. The Society may also require submittal of additional documents to consider the said exclusion.

In preparing this document, it is required to meet the "Acceptance Criteria" outlined in 5.5.4-1, Part X of the Rules, and the "Additional Criteria" outlined in 5.5.4-2, Part X of the Rules.

Firstly, the "Acceptance Criteria" for excluding a computer-based system from the scope of Chapter 5, Part X (UR E26) will be explained. There are four requirements defined as acceptance criteria. These requirements are intended to ensure that the cyber risk impact and frequency are sufficiently mitigated for computer-based system that do not apply the cyber resilience requirements mandated by Chapter 4, Part X (UR E27) and Chapter 5, Part X (UR E26). Therefore, no mitigation or alternative measures are allowed in these criteria. If the acceptance criteria are met, the rationale for meeting the requirements must be included in this document.

Next, the "Additional Criteria" for excluding a computer-based system from the scope of Chapter 5, Part X (UR E26) will be explained. The computer-based system considered for exclusion must meet the acceptance criteria mentioned above and, in principle, satisfy the three additional requirements defined as additional criteria. Compliance with these additional requirements involves the systems integrator conducting a risk assessment and determining the compliance based on the results of the risk assessment. The Society does not define the risk assessment methodology itself, so the systems integrator must consider and implement the appropriate method. If the additional criteria are met as a result of the risk assessment, the rationale for meeting the requirements must be included in this document.

Furthermore, even if the additional criteria are not fully met based on the risk assessment results, exclusion may be granted by the Society if deemed acceptable. In such cases, provide a detailed explanation in this document, including relevant materials as necessary, justifying why the exclusion should be considered.

Rule 5.5.4-2, Part X of the Rules

The following criteria are to be met to exclude a system from the scope of applicability of this Chapter:

- (1) The computer-based system is to be isolated (i.e, have no IP-network connections to other systems or networks).
 - (2) The computer-based system is to have no accessible physical interface ports. Unused interfaces are to be logically disabled. It is not to be possible to connect unauthorised devices to the computer-based system.
 - (3) The computer-based system is to be located in areas to which physical access is controlled.
 - (4) The computer-based system is not to be an integrated control system serving multiple ship functions as specified in the scope of applicability of this Chapter.
-

The above "Acceptance Criteria" must be met. The following explains these requirements:

- (1) The computer-based system is to be isolated (i.e.have no IP-network connections to other systems or networks).**

The computer-based system may fall into the following cases:

- Completely separated (air-gapped) from other systems and networks.
- Connected to other systems or networks via non-IP communication methods (e.g., serial communication).

- (2) **The computer-based system is to have no accessible physical interface ports. Unused interfaces are to be logically disabled. It is not to be possible to connect unauthorised devices to the computer-based system.**

There should be no accessible interface ports, such as LAN ports, USB ports, and network ports, completely blocked or enclosed in locked panels. Additionally, other interfaces must be logically disabled.

- (3) **The computer-based system is to be located in areas to which physical access is controlled.**

Areas with controlled physical access may include:

- Permanently closed compartments (e.g., Fire Station).
- Compartments constantly monitored by crew members (e.g., the bridge, engine control room).

- (4) **The computer-based system is not to be an integrated control system serving multiple ship functions as specified in the scope of applicability of this Chapter.**

An integrated control system serving multiple ship functions refers to systems such as Integrated Automation Systems (IAS) that can monitor and control both cargo and engine systems.

Rule 5.5.4-3, Part X of the Rules

The following additional criteria are to be considered for the evaluation of risk level acceptability:

- (1) The computer-based system should not serve ship functions of category III.
- (2) Known vulnerabilities, threats, potential impacts deriving from a cyber incident affecting the computer-based system have been duly considered in the risk assessment.
- (3) The attack surface for the computer-based system is minimized, having considered its complexity, connectivity, physical and logical access points, including wireless access points.

Items (1) to (3) above must be assessed by the systems integrator, who will determine whether the requirements are met based on the results of a risk assessment. The systems integrator must include the rationale for their determination in this document. The Society will review the rationale to confirm that it is reasonable.

4-5. Description of compensating countermeasures

Rule Table X2.4 No. 6, Part X of the Rules



Systems integrator: Submit, maintain until completion



Shipowner: Maintain

4-5.1 Overview

This document compiles information on [computer-based systems that do not independently meet the system requirements of Chapter 4, Part X \(UR E27\)](#) within the scope of Chapter 5, Part X (UR E26). It organizes the [compensating countermeasures](#) described in the "Description of Security Capabilities" provided by the supplier and details how these measures are implemented on the ship.

The purpose of this document is to enable the shipowner to understand concisely how the security capabilities required for each computer-based system are achieved (e.g., through network-level and physical management) when preparing the "Ship Cyber Security and Resilience Program," and to provide easy access to necessary reference materials. Therefore, it is recommended that this document be referenced in conjunction with the "Cyber Security Design Description."

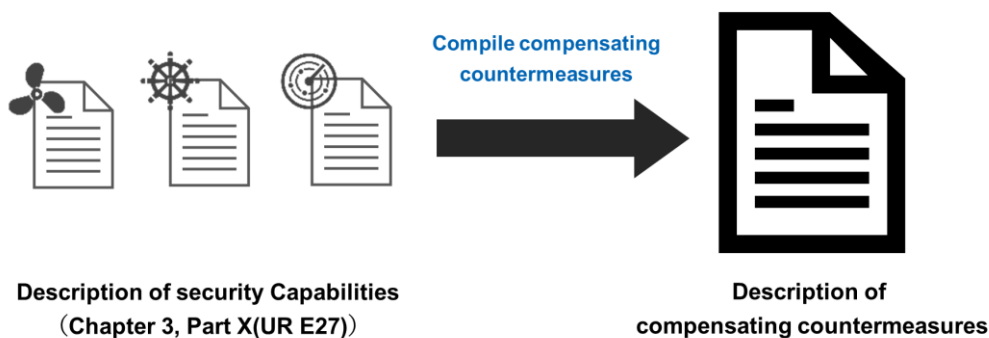


Figure 4.5 Description of compensating countermeasures

4-5.2 Explanation

Rule 2.2.3-3(8), Part X of the Rules

If any computer-based system in the scope of applicability of this Chapter has been approved with compensating countermeasures in lieu of a requirement in Chapter 4, "Description of compensating countermeasures" is to specify the respective computer-based system, the lacking security capability, as well as provide a detailed description of the compensating countermeasures. See also 4.4.1(3) requiring that the supplier describes such compensating countermeasures in the system documentation.

The compensating countermeasures for each computer-based system are mentioned in the "Description of Security Capabilities," which is one of the submission documents of Chapter 4, Part X (UR E27). If these countermeasures are adopted for a computer-based system, the "Description of Compensating Countermeasures" must include relevant information. The information to be included should cover the name of the computer-based system, the applicable system requirements, and the adopted compensating countermeasures.

Below is an example of the "Description of Compensating Countermeasures."

Example: Use Control for Portable and Mobile Devices

The system requirements of Chapter 4, Part X (UR E27) stipulate the implementation of capabilities to restrict the use and transfer of portable and mobile devices within the computer-based system. Portable and mobile devices refer to carry-on devices such as USB memory sticks.

The purpose of this capability is to reduce the risk of malware infection via portable or mobile devices. However, if this function cannot be implemented for some reason, an alternative measure can be adopted to fulfill the requirement. This could include physical means such as port blockers. This alternative measure achieves the same objective as the original function, thereby meeting the requirement.

4-6. Ship cyber resilience test procedure

Rule Table X2.4 No. 7, Part X of the Rules



Systems integrator: Submit and verify during the commissioning phase



Shipowner: Maintain and verify during special surveys

4-6.1 Overview

The Ship Cyber Resilience Test Procedures outlines [the test plans for verifying the security functions of the network and each computer-based system](#). The tests described in this document are to be conducted by the systems integrator during the commissioning phase of ship construction and by the shipowner during periodic surveys after the ship has been delivered.

4-6.2 Explanation

Rule 2.2.3-4(2)(a), Part X of the Rules

The content of this document is specified for the Commissioning phase in each subsection “Demonstration of compliance” in 5.4.

The details of this document are specified in 5.4, Part X of the Rules. These requirements are explained in **4-6.3**.

Rule 2.2.3-4(2)(b), Part X of the Rules

For each computer-based system, the required inherent security capabilities and configuration thereof are verified and tested in the certification process of each computer-based system (see Chapter 4). Testing of such security functions may be omitted if specified in the respective subsection “Commissioning phase” in 5.4, on the condition that these security functions have been successfully tested during the certification of the computer-based system as per Chapter 4. Nevertheless, all tests are to be included in the Ship cyber resilience test procedure and the decision to omit tests will be taken by the Society. Tests may generally not be omitted if findings/comments are carried over from the certification process to the commissioning phase, if the respective requirements have been met by compensating countermeasures, or due to other reasons such as modifications of the computer-based system after the certification process.

Regarding the verification tests of the security capabilities of each computer-based system conducted in this document, if these tests have been successfully conducted through the approval process of Chapter 4, Part X (UR E27), the relevant tests may be omitted. However, regardless of whether the tests can be omitted, the test methods must be included in this document. This is because the test methods are also used for the periodic inspections conducted by the shipowner, as mentioned earlier

in Chapter 5, Part X (UR E26). Moreover, if compensating countermeasures have been adopted for the security capabilities of any computer-based system, the tests for these compensating countermeasures cannot be omitted, regardless of their verification in the approval process of Chapter 4, Part X (UR E27). The test methods for the compensating countermeasures must be included in this document, and the tests must be conducted.

Rule 2.2.3-4(2)(c), Part X of the Rules

The Ship cyber resilience test procedure is also to specify how to test any compensating countermeasures described in 2.2.3-3(8).

As mentioned above, if compensating countermeasures have been adopted for the security capabilities of each computer-based system, the test methods for these countermeasures must be included. The test methods for each computer-based system are described in the "Test procedure of security capabilities," which is one of the submission documents required by Chapter 4, Part X (UR E27).

Rule 2.2.3-4(2)(d), Part X of the Rules

The Ship cyber resilience test procedure is to include means to update status and record findings during the testing, and specify the following information:

- i) Necessary test setup (i.e. to ensure the test can be repeated with the same expected result)
 - ii) Test equipment
 - iii) Initial condition(s)
 - iv) Test methodology, detailed test steps
 - v) Expected results and acceptance criteria
-

This document must include the test conditions, test equipment, initial conditions, test methods, and expected test results for each requirement validation test. Additionally, it should contain sections for recording test results and observations during the tests.

4-6.3 Explanation of Each Requirement in Functional Elements

In this document, the requirements set for each functional element must be met. The details of each requirement are explained below.



5.4.2, Part X of the Rules / Identify



5.4.2(1), Part X of the Rules / Vessel asset inventory



5.4.3, Part X of the Rules / Protect



5.4.3(1) Part X of the Rules / Security zones and network segmentation

P. 68



5.4.3(2), Part X of the Rules / Network protection safeguards

P. 69



5.4.3(3), Part X of the Rules / Antivirus, antimalware, antispam and other protections from malicious code

P. 71



5.4.3(4), Part X of the Rules / Access control

P. 72



5.4.3(5), Part X of the Rules / Wireless communication

P. 72



5.4.3(6), Part X of the Rules / Remote access control and communication with untrusted networks

P. 73



5.4.3(7), Part X of the Rules / Use of mobile and portable devices

P. 76



5.4.4 Part X of the Rules / Detect



5.4.4(1), Part X of the Rules / Network operation monitoring

P. 78



5.4.4(2), Part X of the Rules / Verification and diagnostic functions of computer-based system and networks

P. 82



5.4.5 Part X of the Rules / Respond



5.4.5(2), Part X of the Rules / Local, independent and/or manual operation

P. 84



5.4.5(3), Part X of the Rules / Network isolation

P. 84



5.4.5(4), Part X of the Rules / Fallback to a minimal risk condition

P. 85



5.4.6 Part X of the Rules / Recover



5.4.6(1), Part X of the Rules / Recovery plan

P. 87



5.4.6(2), Part X of the Rules / Backup and restore capability

P. 87



5.4.6(3), Part X of the Rules / Controlled shutdown, reset, roll-back and restart

P. 88



Identify

5.4.2(1), Part X of the Rules / Vessel asset inventory

Rule Part X 5.4.2(1)(d) iii)

The systems integrator is to submit Ship cyber resilience test procedure (see 2.2.3-4(2)) and demonstrate the following to the Society:

- 1) vessel asset inventory is updated and completed at delivery,
- 2) computer-based systems in the scope of applicability of this Chapter are correctly represented by the vessel asset inventory, and
- 3) software of the computer-based systems in the scope of applicability of this Chapter has been kept updated, e.g. by vulnerability scanning or by checking the software versions of computer-based systems while switched on.

The ship cyber resilience test procedure is to specify the means to demonstrate to the Society that the vessel asset inventory and the software listed in the inventory are appropriately managed.

The ship cyber resilience test procedure is to specify the means to demonstrate the following to the Society by the commissioning phase:

- 1) The vessel asset inventory is completed with the information to be included in the inventory. (Items such as shipowner-supplied equipment that were previously unlisted or marked as TBD (To be determined) have been finalized.)
- 2) All computer-based systems in the scope of this chapter are included in the vessel asset inventory.
- 3) Procedures to update each software listed in the vessel asset inventory, based on the management of software updates planned in the ship cyber security and resilience program. (This can be verified by checking software versions, among other methods.)

The systems integrator is also to carry out the test in accordance with the procedures specified in the commissioning phase and demonstrate this to the Society.

The demonstration to the Society can be done by combining the following methods. Please describe the procedures necessary to implement these methods.

- Verification by direct comparison by the Society surveyor:
The surveyor directly compares the contents of the vessel asset inventory with the actual status on board the vessel.
- Use of automated tools:
The Society surveyor confirms the operation of a tool that automatically collect the data in

the vessel asset inventory to obtain the latest information.

The procedures may refer to the manuals of each computer-based system. In this case, please specify the references in the Ship cyber resilience test procedure (or vessel asset inventory).

ClassNK



Protect

5.4.3(1), Part X of the Rules / Security zones and network segmentation

Rule 5.4.3(1)(d) iii), Part X of the Rules

The systems integrator is to submit Ship cyber resilience test procedure (see 2.2.3-4(2)) and demonstrate the following to the Society:

- 1) The security zones on board are implemented in accordance with the approved documents (i.e. zones and conduit diagram, cyber security design description, asset inventory, and relevant documents provided by the supplier). This may be done by e.g., inspection of the physical installation, network scanning and/or other methods providing the Surveyor assurance that the installed equipment is grouped in security zones according to the approved design.
- 2) Security zone boundaries allow only the traffic that has been documented in the approved Cyber security description. This may be done by e.g., evaluation of firewall rules or port scanning.

- **1) The security zones on board are implemented in accordance with the approved documents (i.e. zones and conduit diagram, cyber security design description, asset inventory, and relevant documents provided by the supplier). This may be done by e.g., inspection of the physical installation, network scanning and/or other methods providing the Surveyor assurance that the installed equipment is grouped in security zones according to the approved design.**

This test confirms that the network zones are installed and wired as specified in the approved documents. Examples of verification methods include:

- Inspection of Physical Installation:
Referencing the zone and conduit diagrams, the installation and wiring of the equipment on-board are inspected to ensure compliance.
- Network Scanning:
Network scanning involves sending ping requests (or commands of protocols that the equipment can respond to) to all IP addresses in the relevant network zone and confirming their responses. To perform network scanning efficiently, ping requests can be automated with scripts. Alternatively, automated network scanning can be performed using dedicated tools such as nmap or hping.

However, response confirmation alone cannot guarantee that the equipment shown in the drawings is actually using those IP addresses. To make sure individual device verification, methods such as the following can be considered: confirming that there is a ping response from the equipment under normal conditions and that the ping response disappears when the ethernet cable of the relevant equipment is disconnected or disabled, or remotely logging in using the relevant IP address to confirm equipment information such as the hostname.

- **2) Security zone boundaries allow only the traffic that has been documented in the approved Cyber security description. This may be done by e.g., evaluation of firewall rules or port scanning.**

This test ensures that the traffic passing through the security zone boundaries is only what is documented in the "Cybersecurity Design Description." Specific examples include:

- Evaluation of Firewall Rules:

Verify that the zone boundary devices (equipment that controls network traffic, such as a firewall) are configured according to the designed firewall rules. Specifically, confirm that the firewalls installed on the vessel are configured as described in the "Cybersecurity Design Description."

- Port Scanning:

Port scanning involves attempting to connect to ports on network-connected devices and checking their responses. By identifying which ports are open or closed, you can verify the traffic passing through the ports. Nmap is an example of a tool used for port scanning.

5.4.3(2), Part X of the Rules / Network protection safeguards

Rule 5.4.3(2)(d) iii), Part X of the Rules

The systems integrator is to submit Ship cyber resilience test procedure (see 2.2.3-4(2)) and demonstrate the following to the Society. The tests specified in 2) and 3) may be omitted if performed during the certification of computer-based systems as per 2.2.3-4(2).

- 1) Test denial of service (DoS) attacks targeting zone boundary protection devices, as applicable.
- 2) Test denial of service (DoS) to ensure protection against excessive data flow rate, originating from inside each network segment. Such denial of service (DoS) tests are to cover flooding of network (i.e., attempt to consume the available capacity on the network segment), and application layer attack (i.e., attempt to consume the processing capacity of selected endpoints in the network)
- 3) Test e.g. by analytic evaluation and port scanning that unnecessary functions, ports, protocols and services in the computer-based systems have been removed or prohibited in accordance with hardening guidelines provided by the suppliers (see 4.5.8 and 2.2.2-5(7)).

- **1) Test denial of service (DoS) attacks targeting zone boundary protection devices, as applicable.**

This test is required when zone boundary devices are subject to application according to the network design. Specifically, it verifies that zone boundary protection functions are maintained through mechanisms such as filtering and rate limiting, even when DoS events hit against the zone boundary devices. Tools used for this test include both commercial and open-source ones.

- **2) Test denial of service (DoS) to ensure protection against excessive data flow rate, originating from inside each network segment. Such denial of service (DoS) tests are to cover flooding of network (i.e., attempt to consume the available capacity on the network segment), and application layer attack (i.e., attempt to consume the processing capacity of selected endpoints in the network)**

This test confirms that the network and computer-based systems can withstand high-load data flows deliberately generated by DoS events. Specifically, using external tools such as commercial and open-source tools, a high volume of data packets are transmitted to verify that the network and computer-based systems can maintain their essential functions. This test must target both network flooding and application layer attacks.

Network Flooding:

For example, creating a loop in the LAN causes storms (bandwidth capacity saturation) due to a loop of flooding frames, such as broadcasts. Even without loops, that can be simulated by generating large amounts of flooding traffic using multiple test devices. In this condition, the objective is to verify that "essential minimum functions are maintained."

Application Layer Attacks:

These are attacks that consume the processing capacity of endpoints in the network by sending communications that require application-level processing. It includes excessive requests for communication protocols (such as TLS), concentrated access to control protocols (such as Modbus TCP), and transmission of excessive data (such as NMEA sentences). Using tools and other means, data flows exceeding the application processing capacity recognized by the supplier are transmitted, and in this condition, it is to verify that "essential minimum functions are maintained."

For security capabilities that have already been approved by the Society in accordance with the requirements of UR E27 (Chapter 4 of Part X), such tests are to be documented in the ship cyber resilience test procedure required under this paragraph, and conducting the test may be omitted.

20	Deterministic output	The computer-based system is to provide the capability to set outputs to a predetermined state if normal operation cannot be maintained as a result of an attack. The predetermined state could be the following: - unpowered state, - last-known value, or - fixed value. (IEC 62443-3-3/SR 3.6)
24	Denial of service protection	The computer-based system is to provide the minimum capability to maintain essential functions during DoS events. (IEC 62443-3-3/SR 7.1)

- 3) Test e.g. by analytic evaluation and port scanning that unnecessary functions, ports, protocols and services in the computer-based systems have been removed or prohibited in accordance with**

hardening guidelines provided by the suppliers (see 4.5.8 and 2.2.2-5(7)).

This test confirms that "unnecessary functions, ports, protocols, and services" on each computer-based system have been removed or disabled. "Unnecessary functions, ports, protocols, and services" are minimized as specified in Table X4.1 Item 30 of Chapter 4, Part X (UR E27), and hardening guidelines with recommended security configurations provided by the supplier are detailed in 4.5.8. Therefore, this test confirms that the security configuration based on the above has not been altered. Specific methods include:

Analysis Evaluation:

Verify that the settings screen of the computer-based system does not include prohibited protocols.

Port Scanning:

Conduct tests such as the previously mentioned nmap test.

For security capabilities that have already been approved by the Society in accordance with the requirements of UR E27 (Chapter 4 of Part X), such tests are to be documented in the ship cyber resilience test procedure required under this paragraph, and conducting the test may be omitted.

30	Least Functionality	<p>The installation, the availability and the access rights of the following are to be limited to the strict needs of the functions provided by the computer-based system:</p> <ul style="list-style-type: none"> - operating systems software components, processes and services - network services, ports, protocols, routes and hosts accesses and any software <p>(IEC 62443-3-3/SR 7.7)</p>
----	---------------------	--

5.4.3(3), Part X of the Rules / Antivirus, antimalware, antispam and other protections from malicious code

Rule 5.4.3(3)(d) iii), Part X of the Rules

The systems integrator is to submit Ship cyber resilience test procedure (see 2.2.3-4(2)) and demonstrate the following to the Society. The above tests may be omitted if performed during the certification of computer-based systems as per 2.2.3-4(2).

- 1) Approved anti-malware software or other compensating countermeasures is effective (e.g. test with a trustworthy anti-malware test file).

This test confirms that the approved anti-malware software or other compensating countermeasures are effective.

An example of a verification method is a test using a trustworthy anti-malware test file. This file is used to evaluate the detection capability of anti-malware software, and a well-known example is the EICAR (European Institute for Computer Antivirus Research) test file. Using such a test file, it is demonstrated that the anti-malware software can accurately detect malware.

If whitelist-type anti-malware protection is employed, the test includes attempting to execute programs not registered in the whitelist and they cannot be executed.

For security capabilities that have already been approved by the Society in accordance with the

requirements of UR E27 (Chapter 4 of Part X), such tests are to be documented in the ship cyber resilience test procedure required under this paragraph, and conducting the test may be omitted.

18	Malicious code protection	The computer-based system is to provide capability to implement suitable protection measures to prevent, detect and mitigate the effects due to malicious code or unauthorized software. It is to have the feature for updating the protection mechanisms. (IEC 62443-3-3/SR 3.2)
----	---------------------------	--

5.4.3(4), Part X of the Rules / Access control

Rule 5.4.3(4)(d) iii), Part X of the Rules

The systems integrator is to submit Ship cyber resilience test procedure (see 2.2.3-4(2), Part X) and demonstrate the following to the Society:

- 1) Components of the computer-based systems are located in areas or enclosures where physical access can be controlled to authorised personnel.
- 2) User accounts are configured according to the principles of segregation of duties and least privilege and that temporary accounts have been removed (may be omitted based on certification of computer-based systems as per 2.2.3-4(2), Part X)

This test verifies that computer-based systems are placed in locations accessible only to authorized personnel, user accounts are configured according to the principle of least privilege, and temporary accounts are deleted when no longer needed.

The Ship cyber resilience test procedure needs to include the following:

- **The location of each computer-based system and the personnel who can access that location**
- **An overview of the configuration following the principle of least privilege for each computer-based system**
- **A list of temporary accounts set for each computer-based system and their expiration dates**

5.4.3(5), Part X of the Rules / Wireless communication

Wireless communication includes Wi-Fi for local communication, mobile communication technologies for external communication, and other high-frequency wireless communication technologies. Compared to wired communication, these are difficult to physically protect and carry cyber risks such as interception and tampering by untrusted devices. The aim is to require more stringent requirements for such high-risk wireless communications by restricting access to only authorized devices and clarifying firewall rules, etc.

Rule 5.4.3(5)(d) iii), Part X of the Rules

The systems integrator is to submit Ship cyber resilience test procedure (see 2.2.3-4(2)) and demonstrate the following to the Society. The above tests may be omitted if performed during the certification of computer-based systems as per 2.2.3-4(2).

- 1) Only authorised devices can access the wireless network.
- 2) Secure wireless communication protocol is used as per approved documentation by the respective supplier (demonstrate e.g. by use of a network protocol analyser tool).

The Ship cyber resilience test procedure needs to include the following:

- 1) Only authorised devices can access the wireless network.

This test is conducted to verify item iv) (wireless access control) of the wireless communication requirement details in X5.4.3(5)(c). Details are provided in Chapter 4, Section 3 "Defense - Wireless Communication" of this Guidelines.



4-3 Cyber security design description

5.4.3(5) Wireless communication

P. 46

Specifically, it includes, for example, verifying that PSK authentication or 802.1x authentication, which are widely used in Wi-Fi, are functioning properly if they are used to control wireless access by devices. Additionally, if identification and connection control are performed based on device MAC addresses, that functionality is verified.

- 2) Secure wireless communication protocol is used as per approved documentation by the respective supplier (demonstrate e.g. by use of a network protocol analyser tool).

This test is performed to verify whether encryption and authentication wireless communication protocols are functioning correctly according to the supplier's design. This verifies items i) (encryption of wireless access) and v) (authentication in wireless networks) of the wireless communication requirement details in X5.4.3(5)(c).

Specifically, this is done by displaying the wireless communication protocol connected to the access point. The network analyzer tool mentioned in the rules needs to have the capability to display wireless communication protocols, such as Wireshark.

For security capabilities that have already been approved by the Society in accordance with the requirements of UR E27 (Chapter 4 of Part X), such tests are to be documented in the ship cyber resilience test procedure required under this paragraph, and conducting the test may be omitted.

5	Wireless access management	The computer-based system is to provide the capability to identify and authenticate all users (humans, software processes or devices) engaged in wireless communication. (IEC 62443-3-3/SR 1.6)
9	Wireless use Control	The computer-based system is to provide the capability to authorize, monitor and enforce usage restrictions for wireless connectivity to the system according to commonly accepted security industry practices. (IEC 62443-3-3/SR 2.2)

5.4.3(6), Part X of the Rules / Remote access control and communication with

untrusted networks

The remote access and remote maintenance described in this section refer to access or maintenance from untrusted networks. Since such remote access control and communication with untrusted networks involve high security risks, this requirement aims to implement more stringent countermeasures for each of these scenarios.

Note that the terminology used in this section is generally distinguished as follows:

- Remote connection/communication with untrusted networks: refers to all communication with untrusted networks, regardless of direction or protocol.
- Remote access: refers to information retrieval (including requests for viewing) and operations performed from untrusted networks.
- Remote maintenance: refers, in principle, to changing or modifying any values in the system from untrusted networks.

Rule 5.4.3(6)(d) iii), Part X of the Rules

The systems integrator is to submit Ship cyber resilience test procedure (see 2.2.3-4(2)) and demonstrate the following to the Society:

- 1) Communication with untrusted networks is secured in accordance with 4.4.3 and that the communication protocols cannot be negotiated to a less secure version (demonstrate e.g., by use of a network protocol analyzer tool).
 - 2) Remote access requires multifactor authentication of the remote user.
 - 3) A limit of unsuccessful login attempts is implemented, and that a notification message is provided for the remote user before session is established.
 - 4) Remote connections must be explicitly accepted by responsible personnel on board.
 - 5) Remote sessions can be manually terminated by personnel on board or that the session will automatically terminate after a period of inactivity.
 - 6) Remote sessions are logged (see No.13 in Table X4.1).
 - 7) Instructions or procedures are provided by the respective product suppliers (see 4.4.1(3)).
-

The systems integrator is to submit Ship cyber resilience test procedure (see 2.2.3-4(2)) and demonstrate the following to the Society:

For this item, a test procedure including the following contents needs to be created and tests conducted during the commissioning phase to verify its functionality:

- **Communication with untrusted networks is secured in accordance with 4.4.3 and that the communication protocols cannot be negotiated to a less secure version (demonstrate e.g., by use of a network protocol analyzer tool).**

This item requires describing methods to verify that equipment communicating with untrusted networks satisfies the requirements of Chapter 4, Part X.

Specifically, for example, when initiating TLS-based communication (such as HTTPS) between

a server system and a client, the negotiation process for selecting the TLS version can be analyzed using protocol analyzers such as Wireshark. Even if the client proposes using the vulnerable TLS 1.1 during this negotiation process, there is a method to verify that the server rejects it and selects a cipher suite of TLS 1.2 or higher, which is currently considered secure.

- **Remote access requires multifactor authentication of the remote user.**

In remote maintenance, not only remote access but also changes to software and settings become easily possible. Therefore, multi-factor authentication is required as an authentication method. For details on multi-factor authentication and verification methods, please see "31. Multifactor authentication for human users" (P 136) in Chapter 5 of the "Guidelines for cyber resilience of on-board systems and equipment".

- **A limit of unsuccessful login attempts is implemented, and that a notification message is provided for the remote user before session is established.**

In remote maintenance, to prevent unauthorized access through attacks such as brute force methods, it is necessary to provide a function that prevents access attempts for a set time after several failed access attempts. Also, before an access attempt, a message requesting consent must be displayed to the remote user of the system.

For details on blocking access attempts, please see "33. Unsuccessful login attempts" (P 142), and for messages, see "34. System use notification" (P 144) in Chapter 5 of the "Guidelines for Cyber resilience of on-board systems and equipment".

To verify this function, this test verifies that access attempts are restricted after repeating access attempts with invalid authentication information for the specified number of times, and that a notification requesting consent is displayed before the access attempt.

- **Remote connections must be explicitly accepted by responsible personnel on board.**

To prevent unintended system infiltration due to careless or malicious remote connections, explicit permission by responsible personnel on board is required when making remote connections.

For details, please see "36. Explicit access request approval" (P 149) in Chapter 5 of the "Guidelines for Cyber resilience of on-board systems and equipment".

- **Remote sessions can be manually terminated by personnel on board or that the session will automatically terminate after a period of inactivity.**

In remote access, to manage the communication state, the processing status of a series of operations from connection establishment to disconnection is stored as a session to manage each processing status. If this session is kept even after it is no longer needed, it can cause impersonation, so it is necessary to terminate and invalidate it to deny access from terminated sessions.

In the test, it is confirmed whether each device automatically terminates the session after a set period of inactivity (times out) or whether manual termination of the session is possible.

For details, please see "37. Remote session termination" (P 151), "40. Session integrity" (P 159), and "Invalidation of session IDs after session termination" (P 162) in Chapter 5 of the "Guidelines for Cyber resilience of on-board systems and equipment".

- **Remote sessions are logged (see No.13 in Table X4.1).**

In systems that allow remote access, audit logs of connection destinations and connection/disconnection times need to be kept to check the intrusion route from remote in the event of a cyber incident. Therefore, during testing, it is necessary to check whether devices that communicate with untrusted networks have the function to record these.

For details, please see "13. Auditable events" (P 88) and "35. Access via Untrusted Networks" (P 147) in Chapter 5 of the "Guidelines for Cyber resilience of on-board systems and equipment".

- **Instructions or procedures are provided by the respective product suppliers (see 4.4.1(3)).**

Remote access needs to be implemented based on methods guaranteed by the supplier. Therefore, it is necessary to confirm that the method for remote access is described in the description of security capabilities or the manual created by the supplier according to X4.4.1(3).

5.4.3(7), Part X of the Rules / Use of mobile and portable devices

Rule 5.4.3(7)(d) iii), Part X of the Rules

The systems integrator is to submit Ship cyber resilience test procedure (see 2.2.3-4(2)) and demonstrate to the Society that capabilities to control use of mobile and portable devices are implemented correctly, the following countermeasures are to be demonstrated as relevant:

- 1) use of mobile and portable devices is restricted to authorised users,
- 2) interface ports can only be used by specific device types,
- 3) files cannot be transferred to the system from such devices,
- 4) files on such devices will not be automatically executed (by disabling autorun),
- 5) network access is limited to specific MAC or IP addresses,
- 6) unused interface ports are disabled, and
- 7) unused interface ports are physically blocked.

It is generally known that malware infection via mobile and portable devices can cause failure of computer-based systems.

This test confirms that the functionality to restrict the use of mobile and portable devices is properly implemented to avoid such above situations. Specifically, the following tests need to be performed:

- **1) Use of mobile and portable devices is restricted to authorized users**

Confirm that the use of mobile and portable devices is restricted to authorized personnel. It includes confirmation that authorized personnel are granted authorization for device usage while

unauthorized personnel are not.

- **2) Interface ports can only be used by specific device types**

Confirm that the use of interface ports is restricted to specific device types, verify those devices, and if possible, confirm the restriction by testing.

- **3) Files cannot be transferred to the system from such devices**

Confirm that files cannot be transferred from unauthorized devices, and if possible, verify that these devices meet requirements by testing.

- **4) Files on such devices will not be automatically executed (by disabling autorun)**

For Windows OS, confirm that autorun is disabled in the control panel settings. For proprietary OS, confirm from the specifications that auto-run is not performed, and if possible, verify that automatically execution is not conducted following the manufacturer's test methods.

- **5) Network access is limited to specific MAC or IP addresses**

If mobile and portable devices use the network, confirm that network access is limited to specific MAC or IP addresses. If possible, verify following the manufacturer's test methods or check settings screens.

- **6) Unused interface ports are disabled**

Unused interface ports in the computer-based systems are to be blocked and disabled through logical means, such as computer-based system settings, or physical means, such as port blockers. In this test, if the former method is adopted, this is verified by confirming the settings that restrict their use or by attempting to connect.

- **7) Unused interface ports are physically blocked**

Unused interface ports of computer-based systems need to be blocked and made unusable through logical means including computer-based system settings, or physical means such as port blockers. In this test, if the latter method is adopted, we visually confirm that the ports are blocked by physical means such as port blockers and are in an unusable state.



Detect

5.4.4(1), Part X of the Rules / Network operation monitoring

Rule 5.4.4(1)(d) iii) 1), Part X of the Rules

The systems integrator is to specify in the Ship cyber resilience test procedure and demonstrate to the Society the network monitoring and protection mechanisms in the computer-based systems. The following tests may be omitted if performed during the certification of computer-based systems as per 2.2.3-4(2).

- Test that disconnected network connections will activate alarm and that the event is recorded.
- Test that abnormally high network traffic is detected, and that alarm and audit record is generated. This test may be carried on together with the test in 5.4.5(4)(d)iii).
- Demonstrate that the computer-based system will respond in a safe manner to network storm scenarios, considering both unicast and broadcast messages (see also 5.4.3(2)(d)iii))
- Demonstrate generation of audit records (logging of security-related events)
- If Intrusion detection systems are implemented, demonstrate that this is passive and will not activate protection functions that may affect intended operation of the computer-based systems.

The purpose of this section is to improve cyber resilience by detecting the sign of cyber attacks, enabling early response and recovery. Cyber attacks also include those that do not result in actual damage (for example, attempts at intrusion or communication). Verifying such signs is also one of the objectives to further enhance the defense functions of computer-based systems.

Among the tests in this section, those that have been confirmed to correspond to the requirements of this section based on Chapter 4 of Part X may be omitted.

- **Test that disconnected network connections will activate alarm and that the event is recorded.**

This section is performed to demonstrate that the network connection monitoring function specified in the requirement details is functioning correctly and to comply with the security policy.

By monitoring network connections and logging/analyzing connection information, violations of the security policy, such as suspicious activities and unauthorized access, can be detected. This enables quick response to threats and minimizes damage. The information to be logged includes:

- Success/failure status of authentication to each computer-based system
- Access status/destination (IP, port)/error status for each computer-based system
- Access from each computer-based system to networks deviating from the design

This test is conducted by disconnecting network connections within or between systems. It is then verified that an alarm indicating the disconnection of the network connection is triggered and that a record indicating this is retained as an audit log.

- **Test that abnormally high network traffic is detected, and that alarm and audit record is generated. This test may be carried on together with the test in 5.4.5(4)(d)iii).**

This test is performed to demonstrate that excessive traffic can be monitored and detected as specified in the requirement details. This requirement enables response to DoS/DDoS attacks.

During a DDoS attack and when a large amount of data is received, traffic temporarily increases. By monitoring this traffic and detecting its abnormal increase, it can be detected that a DDoS attack is being received. Also, if the software itself is infected with malware that makes the system participate in attacks, it is assumed that it may launch a DoS attack against other internal systems. By monitoring traffic, it is also possible to monitor whether such attacks are being launched.

In this test, a large number of packets are sent as a simulation of excessive traffic, and it is verified that the resulting increase in traffic is detected and alarmed, and that an audit log of the alarm is recorded.

- **Demonstrate that the computer-based system will respond in a safe manner to network storm scenarios, considering both unicast and broadcast messages (see also 5.4.3(2)(d)iii))**

This section is performed to demonstrate that even when subjected to excessive traffic, the impact on the target computer-based system is minimized.

In this test, by verifying the behavior of the computer-based system when exposed to a network storm, it is demonstrated that even in such scenarios, the computer-based system maintains normal operation or its essential minimum functions due to the protection of security functions or the design of the computer-based system itself. This test can be conducted simultaneously with the test in the protection requirement "5.4.3(2) Network protection safeguards". For details, please refer to Section 7 of Chapter 4 of this Guidelines, the second item of Protect, "5.4.3(2) Network protection safeguards".



4-6 Ship cyber resilience test procedure

5.4.3(2) Network protection safeguards

P. 69

- **Demonstrate generation of audit records (logging of security-related events)**

This section is performed to demonstrate that network connections and device management activities are correctly logged by security functions. The purpose is to accurately determine the intrusion path and the extent of damage when an intrusion occurs, and to promptly recover. In terms of protection, it is also possible to discover and block unintended changes to management information by utilizing this detection information.

The contents to be logged include:

- Shutdown attempts and operational status of each computer-based system (e.g., dead or alive monitoring)
- Resource status of each computer-based system (e.g., processor/memory usage)
- Changes to administrator privileges, environment settings, and account settings of each computer-based system

- Log of clearing clearable logs
- Physical intrusion records of each computer (e.g., access to storage, power operations)

In this test, for the items of audit logs in network connections and device management activities that are specified to be logged in the system designer's specifications, it is confirmed that the records are actually generated by operations that should be audited.

For security capabilities that have already been approved by the Society in accordance with the requirements of UR E27 (Chapter 4 of Part X), such tests are to be documented in the ship cyber resilience test procedure required under this paragraph, and conducting the test may be omitted.

13	Auditable events	The computer-based system is to generate audit records relevant to security for at least the following events: access control, operating system events, backup and restore events, configuration changes, loss of communication. (IEC 62443-3-3/SR 2.8)
20	Deterministic output	The computer-based system is to provide the capability to set outputs to a predetermined state if normal operation cannot be maintained as a result of an attack. The predetermined state could be the following: - unpowered state, - last-known value, or - fixed value. (IEC 62443-3-3/SR 3.6)
24	Denial of service protection	The computer-based system is to provide the minimum capability to maintain essential functions during DoS events. (IEC 62443-3-3/SR 7.1)

- **If Intrusion detection systems are implemented, demonstrate that this is passive and will not activate protection functions that may affect intended operation of the computer-based systems.**

An Intrusion Detection System (IDS) refers to a system that monitors the behavior of networks and systems, and detects and alerts suspicious communications estimated to be malicious or unauthorized communications caused by external attacks or programs that have infiltrated internally.

When installing such an IDS, the following requirements must be met.

Rule 5.4.4(1)(c) ii), Part X of the Rules

Intrusion detection systems (IDS) may be implemented, subject to the following:

- 1) The IDS is to be qualified by the supplier of the respective computer-based system
 - 2) The IDS is to be passive and not activate protection functions that may affect the performance of the computer-based system
 - 3) Relevant personnel should be trained and qualified for using the IDS
-

- **The IDS is to be qualified by the supplier of the respective computer-based system**

This section aims to ensure compatibility between IDS functionality and computer-based system functionality.

IDS is a system that monitors networks to provide security functions. However, if the IDS does not adapt the ship's system architecture, there is a risk that the IDS may fail to function as intended, such as missing malicious communications, conversely detecting legitimate communications as malicious. In the worst case, this could pose a danger of causing unauthorized operations to the computer-based systems.

For these reasons, when implementing IDS, it is necessary that the IDS be qualified by the supplier of the respective computer-based system.

- **The IDS is to be passive and not activate protection functions that may affect the performance of the computer-based system**

This section aims to ensure system availability.

Among IDS products in a broad sense, some can enable IPS (Intrusion Prevention System) functions that actively block communications when malicious communications are detected. If IPS functions block communications, this could cause malfunctions in communications of critical equipment and potentially have a significant impact on ship operations. The risk is particularly severe in the case of false positives. Therefore, when implementing IDS as OT equipment onboard ships, it must be operated in a passive mode (operation with detection and alerting functions only, without active blocking).

- **Relevant personnel should be trained and qualified for using the IDS**

The purpose of this section is to operate the IDS effectively.

To maximize the effectiveness of detecting signs of attacks by the IDS, it is necessary to be able to properly utilize various functions of the IDS. For example, to find signs of cyber attacks, it is necessary to analyze the connection information detected by the IDS, which requires specialized knowledge of networks. It is also believed that specialized knowledge of networks is useful in preventing false detections by the IDS by setting appropriate detection criteria.

Based on the above, this test confirms the response of the IDS when intrusions are detected by executing operations that trigger detection according to the IDS specifications. During this process, it is necessary to confirm that there is no impact on the operation of computer-based systems through communication blocking or other means.

Rule 5.4.4(1)(d) iii)(2), Part X of the Rules

Any Intrusion detection systems in the computer-based systems in scope of applicability to be implemented are to be subject to verification by the Society. Relevant documentation are to be

submitted for approval, and survey/tests are to be carried out on board.

This section applies when an IDS is implemented in addition to the network monitoring means set forth in the first half of the requirement details. In the Society's approval process, network monitoring means are subject to both plan approval and inspection attendance, but if an IDS is implemented, plan approval and inspection attendance for the IDS are also required in addition to those.

Regarding the IDS, it is stipulated that it should be approved by the supplier of each computer-based system to maintain compatibility between the security functions and the computer-based system or network, and that the personnel involved should be trained and qualified because specialized knowledge is required to detect signs of attacks using the IDS.

5.4.4(2), Part X of the Rules / Verification and diagnostic functions of computer-based system and networks

Rule 5.4.4(2)(d) iii), Part X of the Rules

The systems integrator is to submit Ship cyber resilience test procedure (see 2.2.3-4(2)) and demonstrate to the Society the effectiveness of the procedures for verification of security functions provided by the suppliers. The above tests may be omitted if performed during the certification of computer-based systems as per 2.2.3-4(2).

Rule 5.4.4(2)(c), Part X of the Rules

Computer-based systems and networks' diagnostics functionality are to be available to verify the intended operation of all required security functions during test and maintenance phases of the ship.

This requirement aims to confirm the soundness of security functions, discover malfunctions, and improve security functions.

By regularly verifying that the security functions are operating normally, owners can ensure the maintenance of the security functions. In addition, if an abnormality is found in the security functions, there is a possibility that the system is vulnerable to cyber attacks, so it is necessary to detect and deal with it early. Furthermore, by regularly conducting operational verification of security functions, it is possible to lead to the improvement of functions.

The test procedure should include procedures for verifying the security functions of the computer-based system. To document these procedures, it is effective to refer to the verification methods for the security functions described in the "Description of security capabilities" of each computer-based system based on No. 19 in Table X4.1 of Chapter 4 of Part X or the "Plans for Maintenance and Verification".

For security capabilities that have already been approved by the Society in accordance with the requirements of UR E27 (Chapter 4 of Part X), such tests are to be documented in the ship cyber resilience test procedure required under this paragraph, and conducting the test may be omitted.

19	Security functionality verification	The computer-based system is to provide the capability to support verification of the intended operation of security functions and report when anomalies occur during maintenance. (IEC 62443-3-3/SR 3.3)
----	-------------------------------------	--



Respond

5.4.5(1), Part X of the Rules / Incident response plan

Rule 5.4.5(1)(d) iii), Part X of the Rules

No requirements.

5.4.5(2), Part X of the Rules / Local, independent and/or manual operation

Rule 5.4.5(2)(d) iii), Part X of the Rules

The systems integrator is to submit Ship cyber resilience test procedure (see 2.2.3-4(2)) and demonstrate to the Society that the required local controls in the scope of applicability of this Chapter needed for safety of the ship can be operated independently of any remote or automatic control systems. The tests are to be carried out by disconnecting all networks from the local control system to other systems/devices. The above tests may be omitted if performed during the certification of computer-based systems as per 2.2.3-4(2).

This section aims to confirm through documentation that the local control necessary for the safe operation of the ship can be operated independently from remote or automatic control systems.

The Ship cyber resilience test procedure should indicate the procedure for switching the target computer-based system to local control, and the passing criteria should be that the computer-based system can be operated independently from any remote or automatic control systems.

For security capabilities that have already been approved by the Society in accordance with the requirements of UR E27 (Chapter 4 of Part X), such tests are to be documented in the ship cyber resilience test procedure required under this paragraph, and conducting the test may be omitted.

However, since there are no security capabilities under UR E27 (Chapter 4 of Part X) that correspond to this item, the feasibility of omitting testing should be considered based on what specific test content has been conducted in testing for each OT system.

5.4.5(3), Part X of the Rules / Network isolation

Rule 5.4.5(3)(d) iii), Part X of the Rules

The systems integrator is to submit Ship cyber resilience test procedure (see 2.2.3-4(2)) and demonstrate to the Society by disconnecting all networks traversing security zone boundaries, that the computer-based systems in the security zone will maintain adequate operational functionality without network communication with other security zones or networks. The above tests may be omitted if performed during the certification of computer-based systems as per 2.2.3-4(2).

This section aims to confirm through documentation that each computer-based system maintains appropriate operational functionality even when the network is isolated.

The Ship cyber resilience test procedure should indicate the procedure for logical and/or physical isolation of the network, and the passing criteria should be that each computer-based system operates appropriately without communication.

For security capabilities that have already been approved by the Society in accordance with the requirements of UR E27 (Chapter 4 of Part X), such tests are to be documented in the ship cyber resilience test procedure required under this paragraph, and conducting the test may be omitted.

However, since there are no security capabilities under UR E27 (Chapter 4 of Part X) that correspond to this item, the feasibility of omitting testing should be considered based on what specific test content has been conducted in testing for each OT system.

5.4.5(4), Part X of the Rules / Fallback to a minimal risk condition

Rule 5.4.5(4)(d) iii), Part X of the Rules

The systems integrator is to submit Ship cyber resilience test procedure (see 2.2.3-4(2)) and demonstrate to the Society that computer-based systems in the scope of applicability of this Chapter respond to cyber incidents in a safe manner (as per 5.4.5(4)(d)i)), e.g. by maintaining its outputs to essential services and allowing operators to carry out control and monitoring functions by alternative means. The tests are to at least include denial of service (DoS) attacks and may be done together with related test in 5.4.4(1)(d)iii). The above tests may be omitted if performed during the certification of computer-based systems as per 2.2.3-4(2).

This section aims to confirm through documentation that cyber incidents can be responded to by the function to fall back to minimal condition.

This test can be executed simultaneously with the test related to network operation monitoring specified in 5.4.4(1)(d)iii), Part X of the Rules. Also, this test needs to include a Denial of Service (DoS) attack. The Ship cyber resilience test procedure should indicate the procedure for conducting a DoS attack and show what kind of fallback will be performed when attacked. The passing criteria should be that each computer-based system operates appropriately while maintaining output to essential services after receiving a DoS attack.

For security capabilities that have already been approved by the Society in accordance with the requirements of UR E27 (Chapter 4 of Part X), such tests are to be documented in the ship cyber resilience test procedure required under this paragraph, and conducting the test may be omitted.

20	Deterministic output	The computer-based system is to provide the capability to set outputs to a predetermined state if normal operation cannot be maintained as a result of an attack. The predetermined state could
----	----------------------	---

		<p>be the following:</p> <ul style="list-style-type: none">- unpowered state,- last-known value, or- fixed value. <p>(IEC 62443-3-3/SR 3.6)</p>
--	--	---



Recover

5.4.6(1), Part X of the Rules / Recovery plan

Rule 5.4.6(1)(d) iii), Part X of the Rules

The systems integrator is to submit Ship cyber resilience test procedure (see 2.2.3-4(2)) and demonstrate to the Society the effectiveness of the procedures and instructions provided by the suppliers to respond to cyber incidents as specified in 5.4.6(2) and (3). The above tests may be omitted if performed during the certification of computer-based systems as per 2.2.3-4(2).

Demonstrate to the Society the effectiveness of the procedures and instructions provided by the suppliers to respond to cyber incidents as specified in 5.4.6(2) and (3)

This requirement involves verifying whether the items described in the "Information supporting incident response and recovery plans" prepared by the supplier (manufacturer) function correctly. Since most of the functional criteria are specified in Part X 5.4.6(2) and (3), please refer to the following for details of those items. Testing under this section is expected to be conducted for items that do not overlap with those requirements.

For security capabilities that have already been approved by the Society in accordance with the requirements of UR E27 (Chapter 4 of Part X), such tests are to be documented in the ship cyber resilience test procedure required under this paragraph, and conducting the test may be omitted.

However, since there are no security capabilities under UR E27 (Chapter 4 of Part X) that correspond to this item, the feasibility of omitting testing should be considered based on what specific test content has been conducted in testing for each OT system.

5.4.6(2), Part X of the Rules / Backup and restore capability

Rule 5.4.6(2)(d) iii), Part X of the Rules

The systems integrator is to submit Ship cyber resilience test procedure (see 2.2.3-4(2)) and demonstrate to the Society the procedures and instructions for backup and restore provided by the suppliers for computer-based systems in the scope of applicability of this Chapter. The above tests may be omitted if performed during the certification of computer-based systems as per 2.2.3-4(2).

• The Society the procedures and instructions for backup and restore provided by the suppliers for computer-based systems

This test requires the demonstration of backup and restoration procedures and instructions for each computer-based system. Specifically, the backup and recovery tests should be conducted according to the "Information Supporting the Shipowner's Incident Response and Recovery Plan" as submitted in

Chapter 4, Part X (UR E27).

For security capabilities that have already been approved by the Society in accordance with the requirements of UR E27 (Chapter 4 of Part X), such tests are to be documented in the ship cyber resilience test procedure required under this paragraph, and conducting the test may be omitted.

26	System backup	The identity and location of critical files and the ability to conduct backups of user-level and system-level information (including system state information) are to be supported by the computer-based system without affecting normal operations. (IEC 62443-3-3/SR 7.3)
27	System recovery and reconstitution	The computer-based system is to provide the capability to be recovered and reconstituted to a known secure state after a disruption or failure. (IEC 62443-3-3/SR 7.4)

5.4.6(3), Part X of the Rules / Controlled shutdown, reset, roll-back and restart

Rule 5.4.6(3)(d) iii), Part X of the Rules

The systems integrator is to submit Ship cyber resilience test procedure (see 2.2.3-4(2)) and demonstrate to the Society that manuals or procedures are established for shutdown, reset and restore of the computer-based systems in the scope of applicability of this Chapter. These manuals/procedures are to be provided to the shipowner. The above tests may be omitted if performed during the certification of computer-based systems as per 2.2.3-4(2).

• Demonstrate to the Society that manuals or procedures are established for shutdown, reset and restore of the computer-based systems in the scope of applicability of this Chapter. These manuals/procedures are to be provided to the shipowner. The above tests may be omitted if performed during the certification of computer-based systems as per 2.2.3-4(2)

This test requires the demonstration of controlled shutdown, reset, rollback, and restart procedures or instructions for each computer-based system. As a principle, controlled shutdown, reset, rollback, and restart tests should be conducted for each computer-based system.

For security capabilities that have already been approved by the Society in accordance with the requirements of UR E27 (Chapter 4 of Part X), such tests are to be documented in the ship cyber resilience test procedure required under this paragraph, and conducting the test may be omitted.

27	System recovery and reconstitution	The computer-based system is to provide the capability to be recovered and reconstituted to a known secure state after a disruption or failure. (IEC 62443-3-3/SR 7.4)
----	------------------------------------	---

4-7. Ship cyber security and resilience program

Rule Table X2.4 No.8, Part X of the Rules



Systems Integrator: —



Shipowner: Maintain and verify during periodical surveys

4-7.1 Overview

The Ship Cyber Security and Resilience Program is [a document that outlines the management of cybersecurity and cyber resilience for computer-based systems and networks within the scope of Chapter 5, Part X \(UR E26\)](#). The shipowner is required to compile the processes within this document to manage cybersecurity and cyber resilience both technically and organizationally during the operational life of the ship.

The shipowner must develop the program based on the documents handed over from the shipyard. Specifically, as indicated in 4-7.3, this includes procedures for securely using computer-based systems within security zones, network devices installed for zone separation and protection, procedures for updating anti-malware software, responding to security device alerts, and establishing response procedures for incidents.

4-7.2 Explanation

Reg. 2.2.3-5(7)(b) Part X of the Rules

The Ship cyber security and resilience program are to include policies, procedures, plans and/or other information documenting the processes/activities specified in subsections “Demonstration of compliance” in 5.4.

The details of this document are specified in 5.4, Part X of the Rules. These requirements are explained in 4-7.3.

Reg. 2.2.3-5(4), Part X of the Rules

The shipowner is to prepare and implement operational procedures, provide periodic training and carry out drills for the onboard personnel and other concerned personnel ashore to familiarize them with the computer-based systems onboard the ship and the networks connecting such systems to each other and to other computer-based systems not onboard (e.g. ashore), and to properly manage the measures adopted for the fulfilment of requirements.

To become proficient with the onboard computer-based systems, the shore-based computer-based systems, and networks connected to these systems, and to manage the measures adopted to meet the requirements appropriately, the following requirements must be met:

- **Preparation and implementation of operating procedures:**
Specific operating procedures must be created and followed to ensure consistent operation of the systems.
- **Provision of periodic training:**
Regular training on system and network knowledge and operation methods must be provided to ensure that onboard personnel and related shore-based personnel maintain up-to-date knowledge and skills.
- **Drills for onboard personnel and other concerned personnel ashore:**
Training must be provided not only to onboard personnel but also to other shore-based personnel involved with the systems to ensure that all relevant parties possess the necessary knowledge and skills for managing and operating the systems.

Rule 2.2.3-5(5), Part X of the Rules

The shipowner, with the support of supplier, is to keep the measures adopted for the fulfilment of requirements up to date, e.g. by periodic maintenance of hardware and software of computer-based systems onboard the ship and the networks connecting such systems.

Computer-based systems and network devices within the scope of Chapter 5, Part X (UR E26) must be maintained regularly to ensure proper operation. This includes activities such as software updates and hardware maintenance.

Rule Table X2.4, Part X of the Rules

Maintain: The stakeholder is to keep the document updated in accordance with procedure for management of change (MoC). Updated document and change management records are to be submitted to the Society as per Table X2.2.

Ship owners are provided with shipyard documentation and supplier documentation through the shipyard. Regarding change management of these documents, maintaining these documents in an up-to-date state is stipulated here. The documents specified for maintenance by ship owners, primarily during the post-delivery operational phase, are as follows:

- Approved supplier documents (2.2.3)
- Zones and conduit diagram (2.2.3-3.(4))
- Cyber security design description (2.2.3-3.(5))
- Vessel asset inventory (2.2.3-3.(6))
- Risk assessment for exclusion of computer-based systems (2.2.3-3.(7))

- Description of compensating countermeasures (2.2.3-3.(8))
- Ship cyber resilience test procedure (2.2.3-4.(2))
- Ship cyber security and resilience program (2.2.3-5.(7)).

4-7.3 Explanation of Each Requirement in Functional Elements

This document must meet the requirements set for each functional element. The following sections provide a detailed explanation of each requirement. This explanation covers both the "Contents to be included in the plan" and the "Records to be continuously kept or documented evidence."

- Contents to be included in the plan :

Management processes that must be included in the plan, as required during the "Operational Phase" in 5.4, Part X of the Rules.

- Records to be continuously kept or documented evidence :

Records that must be submitted during periodical surveys. This includes records mandated by the management processes outlined in the plan and lists of tools necessary for the procedures.



5.4.2, Part X of the Rules / Identify



5.4.2(1), Part X of the Rules / Vessel asset inventory

P. 93



5.4.3, Part X of the Rules / Protect



5.4.3(1) , Part X of the Rules / Security zones and network segmentation

P. 96



5.4.3(3), Part X of the Rules / Antivirus, antimalware, antispam and other protections from malicious code

P. 98



5.4.3(4), Part X of the Rules / Access control

P. 100



5.4.3(6), Part X of the Rules / Remote access control and communication with untrusted networks

P. 104



5.4.3(7), Part X of the Rules / Use of mobile and portable devices

P. 106



5.4.4 Part X of the Rules / Detect



5.4.4(1), Part X of the Rules / Network operation monitoring

P. 109



5.4.4(2), Part X of the Rules / Verification and diagnostic functions of computer-based system and networks

P. 110



5.4.5 Part X of the Rules / Respond



5.4.5(1), Part X of the Rules / Incident response plan

P. 113



5.4.6 Part X of the Rules / Recover



5.4.6(1), Part X of the Rules / Recovery plan

P. 119



Identify

5.4.2(1), Part X of the Rules / Vessel asset inventory

■ Contents to be included in the plan

Rule 5.4.2(1)(d) iv) 2), Part X of the Rules

The shipowner is to in the Ship cyber security and resilience program describe the process of management of change (MoC) for the computer-based systems in the scope of applicability of this Chapter, addressing at least the following requirements in this Chapter:

- management of change (2.2.3-5), and
- hardware and software modifications (5.4.2(1)(c)).

Based on this section, it is required to document the procedures for change management of computer-based systems within the scope of the rules.

Specifically, the above procedures are to be documented under the change management requirements of Steel Ship Rules Part X 3.5. The Ship Cyber Security and Resilience Program must document or reference the processes for this purpose. For details on change management procedures, please refer to the Technical Information (TEC-1348) regarding the rules for computer-based systems (related to IACS Unified Requirements UR E22 (Rev.3)) issued by our Society.

Additionally, when modifications to computer-based systems result in changes to computer-based system documentation, the documentation is to be updated, and the procedures are to be included in change management. For change management of computer-based system documentation, please refer to the commentary in section 4-7.2.



4-7 Cyber security and resilience program

4-7.2 Explanation

P. 89

Rule 5.4.2(1)(d) iv) 3), Part X of the Rules

The shipowner is to in the Ship cyber security and resilience program also describe the management of software updates, addressing at least the following requirements in this Chapter:

- vulnerabilities and cyber risks (5.4.2(1)(b) and (c)), and
- security patching (5.4.3(6)(c)iii)2)).

The shipowner is to in the Ship cyber security and resilience program also describe the management of software updates, addressing at least the following requirements in this Chapter:

This section requires the description of the software update management methods for computer-based

systems. The management must include the following:

- **vulnerabilities and cyber risks (5.4.2(1)(b) and (c))**

Vulnerabilities and cyber risks are security weaknesses existing in computer-based systems and the risks arising from them.

In the ship cyber security and resilience program, it is necessary to state that newly emerged vulnerabilities through software updates will be recorded and the vessel asset inventory will be updated.

- **security patching (5.4.3(6)(c)iii2))**

Security patches or software updates are changes to security measures to address vulnerabilities in the software. Generally, relatively small changes are called security patches, and relatively large changes are called software updates.

Software vulnerabilities change due to changes in attackers' methods, new discoveries of vulnerabilities through analysis by attackers, etc. If these vulnerabilities are not addressed, attacks by attackers will become easier, so security functions need to be changed accordingly.

When implementing such security patches or software updates, it is necessary to conduct tests and evaluations to demonstrate that they are effective and that their implementation does not cause adverse effects or cyber incidents. For such tests and evaluations, a confirmation report is created by the supplier, so it is required to obtain and confirm it before updating.

■ Records or documented evidence to be continuously created

Rule 5.4.2(1)(d) iv) 4), Part X of the Rules

The shipowner is to present to the Society records or other documented evidence demonstrating implementation of the Ship cyber security and resilience program, i.e., that:

- the approved management of change process has been adhered to,
- known vulnerabilities and functional dependencies have been considered for the software in the computer-based systems, and
- the Vessel asset inventory has been kept updated.

- **the approved management of change process has been adhered to,**

This section requires management in accordance with the change process defined in the requirements of Part X 3.6 of the Rules for Steel Ships. The change management record is an example of a record to be created.

known vulnerabilities and functional dependencies have been considered for the software in the computer-based systems, and

This section requires consideration of known vulnerabilities and functional dependencies.

Known vulnerabilities: Refers to security holes or bugs that have already been discovered. This

information is generally provided along with security update information.

Functional dependencies: Refers to the nature of a software function depending on other software or other computer-based system functions. The functional dependencies of each computer-based system may be included in the user manual provided by the supplier.

Examples of records or documented evidence to be created include update information, user manuals describing functional dependencies, and the vessel asset inventory.

- the Vessel asset inventory has been kept updated.

The vessel asset inventory functions as a list of onboard computer-based systems. It also serves as a reference for vulnerabilities and functional dependencies when making changes such as software updates. Therefore, the vessel asset inventory needs to be kept up to date so that it reflects the current onboard systems.

In the ship cyber security resilience plan, please state that the vessel asset inventory needs to be updated correctly when there are hardware or software changes that require changes to the vessel asset inventory.



Protect

5.4.3(1) , Part X of the Rules / Security zones and network segmentation

■ Contents to be included in the plan

Rule 5.4.3(1)(d) iv) 1), Part X of the Rules

The shipowner is to in the Ship cyber security and resilience program describe the management of security zone boundary devices (e.g., firewalls), addressing at least the following requirements in this Chapter:

- principle of Least Functionality (5.4.3(2)(a)),
- explicitly allowed traffic (5.4.3(1)(a)),
- protection against denial of service (DoS) events (5.4.3(2)(a)), and
- inspection of security audit records (5.4.4(1)(c)).

This section requirement defines the configuration of security zones and network segments in network design. Although we made explanations in the Zones and Conduit Diagram section, this requirement mandates proper network segmentation. In the Ship Cyber Security and Resilience Program, it is necessary to specify matters regarding the maintenance and modification of security zones and network segments.

The shipowner is to in the Ship cyber security and resilience program describe the management of security zone boundary devices (e.g., firewalls), addressing at least the following requirements in this Chapter:

It is necessary to describe the management methods for zone boundary devices, such as firewalls. The management is to include the following:

- principle of Least Functionality (5.4.3(3)(a))

Devices are to be configured to provide only essential functions by disabling or prohibiting unnecessary functions, ports, protocols, and services.

- explicitly allowed traffic (5.4.3(1)(a))

Traffic permitted to cross the zone boundary is to be explicitly allowed. Traffic is to be permitted according to the firewall rules described in the "Cyber Security Design Description."

- protection against denial of service (DoS) events (5.4.3(3)(a))

The network is to be protected against excessive data flow rates and other events that could degrade the quality of network resources. The management is to include documenting the

monitoring and regular testing for such events.

- **inspection of security audit records (5.4.4(1)(c))**

This involves reviewing the security audit records stored on the zone boundary devices. It is required to regularly check the security audit records to identify any abnormal events. Specifically, the following items are to be regularly reviewed and documented:

- 1) Monitoring and protection against excessive traffic
- 2) Monitoring of network connections
- 3) Monitoring and recording of device management activities
- 4) Protection against connection of unauthorized devices
- 5) Generate alarm if utilization of the network's bandwidth exceeds a threshold specified as abnormal by the supplier. See 3.7.2-1, Part X of the Rules.

■ Records to be continuously kept or documented evidence

Rule 5.4.3(1)(d) iv) 2), Part X of the Rules

The shipowner is to demonstrate to the Society that the Zones and conduit diagram has been kept updated and present records or other documented evidence demonstrating implementation of the Ship cyber security and resilience program, i.e., that security zone boundaries are managed in accordance with the above requirements.

Regarding this requirement, it is necessary to create documented records that can verify the following matters.

- **Zones and Conduit Diagram Updates:**

If the zones and conduit diagram has been updated, the revised diagram is to be submitted to our machinery department as a modified drawing, obtain approval, and be properly installed onboard.

- **Management of Security Zone Boundaries:**

Records demonstrating the proper management of zone boundary devices, such as firewalls, must be created. Specifically, the following records need to be created:

- **principle of Least Functionality (5.4.3(3)(a))**

- List of Functions, Ports, Protocols, and Services:

A list of disabled or prohibited functions, ports, protocols, and services.

- Change Management Records:

Records of regular checks to confirm that disabled or prohibited functions are not intentionally or accidentally enabled.

- **explicitly allowed traffic (5.4.3(1)(a))**

- Firewall Rules List:

A list of firewall settings that specify the rules for explicitly allowed traffic.

- Traffic Permission List:

A list of traffic permitted to cross zone boundaries.

- Traffic Monitoring Logs:
Logs to verify that actual traffic is limited to what is permitted.
- **protection against denial of service (DoS) events (5.4.3(3)(a))**
 - DoS Protection Settings List:
A list of DoS protection settings for the network.
 - DoS Event Monitoring Logs:
Logs monitoring excessive data flow rates and other events.
 - Test Records:
Documents recording the results of regular tests of DoS protection functions.
- **inspection of security audit records (5.4.4(1)(c))**
 - Security Audit Logs:
Audit logs stored on zone boundary devices.
 - Traffic Monitoring Records:
Records of monitoring and detecting excessive traffic.
 - Network Connection Monitoring Logs:
Logs monitoring network connections.
 - Device Management Activity Monitoring Logs:
Logs monitoring device management activities.
 - Unauthorized Device Connection Monitoring Records:
Records monitoring the connection of unauthorized devices.
 - Network Bandwidth Usage Monitoring Records:
Records monitoring network bandwidth usage and the activation of alarms when usage exceeds thresholds designated as abnormal.

5.4.3(2), Part X of the Rules / Network protection safeguards

Rule 5.4.3(2)(d) iv), Part X of the Rules

No specific requirements.

5.4.3(3), Part X of the Rules / Antivirus, antimalware, antispyware and other protections from malicious code

Contents to be included in the plan

Rule 5.4.3(3)(d) iv) 1), Part X of the Rules

The shipowner is to in the Ship cyber security and resilience program describe the management of malware protection, addressing at least the following requirements in this Chapter:

- Maintenance/update (5.4.3(3)(c))

-
- Operational procedures, physical safeguards (5.4.3(3)(c))
 - Use of mobile, portable, removable media (5.4.3(4)(c)iv) and 5.4.3(7)(c))
 - Access control (5.4.3(4))
-

It is necessary to manage antivirus, antimalware, antispam and other protections from malicious code. If anti-malware software is installed, it is necessary to explain the appropriate management and update methods, and if it is not installed, it is necessary to describe alternative physical protection.

The Ship Cyber Security and Resilience Program is to include the following information on the management of countermeasures against viruses, malware, spam, and malicious code such as antimalware software, zone boundary devices, and network equipment (e.g., firewalls with antimalware capabilities, operational measures, and physical measures) as required in detail in Part X, 5.4.3(3)(c) of the Rules:

- Maintenance/update
- Operational procedures, physical safeguards
- Use of mobile, portable, removable media
- Access control

For details on Part X, 5.4.3(3)(c) of the Rules, see 4. Description of Cybersecurity Design, 5.4.3(3).

4-3 Cyber security design description



Part X of the Rules 5.4.3(3) / Antivirus, antimalware, antispam and other protections from malicious code

P. 43

A zone boundary device is a hardware or software device that connects different security zones and controls traffic to prevent unauthorized access, data leakage, etc., such as the following:

- Firewall
- Intrusion Detection/Prevention System (IDS/IPS)
- VPN device
- Web filtering device
- Application control device

If there are any changes to antivirus, antimalware, antispam and other protections from malicious code that affect the contents of the Ship Cyber Security Resilience Plan, the Ship Cyber Security Resilience Plan must be updated.

■ Records to be continuously kept or documented evidence

Rule 5.4.3(3)(d) iv) 2), Part X of the Rules

The shipowner is to present to the Society records or other documented evidence demonstrating

implementation of the Ship cyber security and resilience program, i.e., that:

- any anti-malware software has been maintained and updated,
- procedures for use of portable, mobile or removable devices have been followed,
- policies and procedures for access control have been followed, and
- physical safeguards are maintained.

The shipowner is to submit to the Society the following records or other documented evidence on the management of zone boundary devices used for antivirus, antimalware, antispam and other protections from malicious code in order to prove the implementation of the Ship Cyber Security Resilience Plan:

- Anti-malware software has been maintained and updated.
- Procedures for use of portable, mobile or removable devices have been followed.
- Policies and procedures for access control have been followed.
- Physical safeguards are maintained.

5.4.3(4), Part X of the Rules / Access control

■ Contents to be included in the plan

Rule 5.4.3(4)(d) iv) 1), Part X of the Rules

The shipowner is to in the Ship cyber security and resilience program describe the management of logical and physical access, addressing at least the following requirements in this Chapter:

- physical access control (5.4.3(4)(c)i),
- physical access control for visitors (5.4.3(4)(c)ii),
- physical access control of network access points (5.4.3(4)(c)iii),
- management of credentials (5.4.3(4)(c)v), and
- least privilege policy (5.4.3(4)(c)vi).

This section aims to prevent untrusted access to ship systems and data through access control.

Access control includes logical methods for controlling the access privileges granted to personnel, and physical methods by installing computer-based systems in lockable rooms or controlled spaces. However, for computer-based systems related to the safe operation of ships that require immediate access (Category II or Category III), consideration must be given to ensure that only authorized personnel can easily access them.

The Ship cyber security and resilience program needs to describe access control methods for the following.

- Physical access control (5.4.3(4)(c)i), Part X of the Rules)

Computer-based systems of Categories II and III should normally be placed in lockable rooms, controlled spaces, or lockable cabinets. However, such locations or cabinets should allow easy

access for crew members and various stakeholders who need to access the computer-based systems, so as not to hinder the safe operation of the ship

For systems requiring physical access control, it is necessary to list them with reference to the shipyard's cyber security design description and describe how these physical access controls are protected, focusing on operational aspects such as key management.

- Physical access control for visitors (5.4.3(4)ii), Part X of the Rules)

Access by visitors such as authorities, technicians, port personnel, and shipowners to the ship's computer-based systems while on board should be restricted, for example, by only allowing access under the supervision of an authorized administrator.

Documentation of the operational procedures for such physical access control for visitors is required.

- Physical access control of network access points (5.4.3(4)(c)iii), Part X of the Rules)

Wired or wireless access points to the onboard networks connected to computer-based systems of Categories II and III should be physically and/or logically prevented from connection, except such connections for maintenance or similar purposes under the supervision of an authorized administrator or according to documented procedures. When visitors request temporary connections (e.g., for printing documents), an isolated standalone computer or a guest network that is segmented from all other onboard networks should be used.

The term "physically prevent" here means blocking the physical entry of personnel to access points or physically securing the access points themselves.

Procedures for managing visitor network connection requirements should be established.

- Management of credentials (5.4.3(4)(c)v), Part X of the Rules)

- 1) Computer-based systems and related information should be protected using access control lists (ACLs) specific to file systems, networks, applications, or databases. An access control list is a compilation of access settings that enumerates who can perform which operations on a particular computer-based system. Accounts for onboard and onshore personnel should be valid for a limited period according to the role and responsibilities of the account holder and should be deleted when no longer needed, with their privileges managed through implementation in ACLs.
- 2) While computer-based systems should be protected by access control, care should be taken to avoid adversely affecting the intended functions of the computer-based systems. Also, computer-based systems that require strong access control should be protected using strong passwords or multi-factor authentication.
- 3) Administrative privileges should be managed so that only authorized and properly trained personnel have full access to computer-based systems.

- Least privilege principle (5.4.3(4)(c)vi), Part X)

- All users permitted access to computer-based systems and networks should only be granted the minimum privileges required to perform their duties. This principle is called the "least privilege principle." Based on this principle, system access privileges should be allocated according to roles and job functions, taking into account physical access controls and system-based access controls, and should be documented in the program.
- The default privilege settings for all new accounts should be the lowest possible privilege. For example, it is effective to use time-limited privileges obtained with one-time credentials (ID, password, etc.). The accumulation of privileges over time should be avoided (e.g., regularly auditing user accounts.) Therefore, the following points are to be considered in the program development process:
 - Minimize privileges when creating accounts.
 - Where possible, use temporary accounts instead of granting permanent account privileges.
 - Regularly verify that no accounts have unintended privileges.

Rule 5.4.3(4)(d) iv) 2), Part X

The shipowner is to in the Ship cyber security and resilience program describe the management of confidential information, addressing at least the following requirements in this Chapter:

- confidential information (5.4.2(1)(c)),
 - information allowed to authorized personnel (5.4.3(4)(c)), and
 - information transmitted on the wireless network (5.4.3(5)(c)).
-

Ship cyber security and resilience program needs to describe methods for managing confidential information as follows:

- Confidential information (5.4.2(1)(c), Part X)

Access to confidential information should be restricted to authorized personnel only. (such as IP addresses, protocols, port numbers, etc., that are evaluated based on the policies of stakeholders, including shipowners, shipyards, manufacturers, etc.) Careful attention is required on confidential information when it appears in the vessel asset inventory and the cyber security design descriptions.



4-1. Vessel asset inventory

P. 27

4-3 Cyber security design description



5.4.3(1), Part X of the Rules / Security zones and network segmentation

P. 41

When storing this confidential information electronically, an access control is required using Access Control Lists (ACLs), similar to credential management, to ensure that only users with the necessary privileges can access the information.

- Information allowed to authorized personnel (5.4.3(4)(c), Part X)

Access to computer-based systems, networks within the scope of Chapter 4, Part X of the Rules, and all information stored in those systems should be permitted only for authorized personnel

- Information transmitted on the wireless network (5.4.3(5)(c), Part X)

- 1) Information transmitted over wireless networks should be encrypted to ensure integrity and confidentiality.
- 2) Devices on wireless networks should communicate only on wireless networks (i.e., they should not be dual-purpose).
- 3) Wireless networks must be designed as segregated network segments in accordance with 5.4.3(1), Part X of the Rules "Security zones and network segmentation" and defended in accordance with 5.4.3(2), Part X of the Rules "Network protection safeguards".
- 4) Wireless access points and other devices on the network should be installed and configured to control access to the network.
- 5) Network devices or systems utilizing wireless communications should be able to identify and authenticate all users (human, software process, or device) involved in the communication.

■ Records to be continuously kept or documented evidence

Rule 5.4.3(4)(d) iv) 3), Part X

The shipowner is to present to the Society records or other documented evidence demonstrating implementation of the Ship cyber security and resilience program, i.e., that:

Personnel are authorized to access the computer-based systems in accordance with their responsibilities.

- Only authorised devices are connected to the computer-based systems.
- Visitors are given access to the computer-based systems according to relevant policies and procedures.
- Physical access controls are maintained and applied.
- Credentials, keys, secrets, certificates, relevant computer-based system documentation, and other sensitive information is managed and kept confidential according to relevant policies and procedures.

The shipowner should submit to the Society the following records or other documented evidence of any access controls in order to prove the implementation of the Ship Cyber Security Resilience Plan:

- Only authorised devices are connected to the computer-based systems.
- Visitors are given access to the computer-based systems according to relevant policies and procedures.
- Physical access controls are maintained and applied.
- Credentials, keys, secrets, certificates, relevant computer-based system documentation, and other

sensitive information is managed and kept confidential according to relevant policies and procedures.

5.4.3(5), Part X of the Rules / Wireless communication

Rule 5.4.3(5)(d) iv), Part X of the Rules

No specific requirements.

5.4.3(6), Part X of the Rules / Remote access control and communication with untrusted networks

■ Contents to be included in the plan

Rule 5.4.3(6)(d) iv) 1), Part X of the Rules

The shipowner is to in the Ship cyber security and resilience program describe the management of remote access and communication with/via untrusted networks, addressing at least the following requirements in this Chapter:

- user's manual (5.4.3(6)(c)),
- roles and permissions (5.4.3(6)(c)),
- patches and updates (5.4.3(6)(c)iii)2)),
- confirmation prior to undertaking remote software update (5.4.3(6)(c)iii)2)), and
- interrupt, abort, roll back (5.4.3(6)(c)iii)2)).

These are requirements for implementing more stringent measures in remote access control and communication with untrusted networks, which have high security risks.

The shipowner is to in the Ship cyber security and resilience program describe the management of remote access and communication with/via untrusted networks, addressing at least the following requirements in this Chapter:

To confirm devices performing remote access and confirm that appropriate measures are taken for each, the following requirements exist for this item:

- **user's manual (5.4.3(6)(c))**

For remote access, as stated in 5.4.3(6)(c)i), a user manual for remote access needs to be created.

This user manual must include the following information:

- **Procedures of remote access**

- **Procedures to read audit logs generated due to remote access**

For the shipyard's description in the Cyber security design description, please refer to Chapter 4, Section 4, Defense, Item 6 "5.4.3(6) Control of remote access and communication with untrusted networks" in this Guidelines.

4-3. Cyber security design description

**5.4.3(6) Control of remote access and communication with untrusted networks****P. 48**

This manual can reference documents created by suppliers who provide each device capable of remote connection.

- roles and permissions (5.4.3(6)(c)),

For remote access, as stated in 5.4.3(6)(c)i), Guidelines clarifying roles and permissions for remote connections need to be created. As explained in Chapter 4, Sections 4 and 7, Item 6 "5.4.3(6) Control of remote access and communication with untrusted networks" of this Guidelines, remote access must be authorized by authorized onboard crew members and must be interruptible by authorized personnel. The Guidelines can be created as part of the user manual.

4-3. Cyber security design description

**5.4.3(6) Control of remote access and communication with untrusted networks****P. 48**

4-6. Ship cyber resilience test procedure

**5.4.3(6) Control of remote access and communication with untrusted networks****P. 73**

Therefore, roles and permissions related to remote access need to be clarified, including personnel who will actually perform remote connections in practical operations.

- patches and updates (5.4.3(6)(c)iii)2))

When supplying security patches or updating software via remote access, as stated in 5.4.3(6)(c)iii) 2), tests and evaluations are required to demonstrate that patches and software updates are effective and that implementing them does not cause secondary effects or cyber incidents.

To clarify which devices fall under such additional requirements, documents (such as lists) need to be created to clarify this for the relevant software.

- confirmation prior to undertaking remote software update (5.4.3(6)(c)iii)2))

When problems occur during the implementation of security patches or software updates via remote access, they can have a greater adverse effect compared to on-site updates. Therefore, prior to remote updates, confirmation reports regarding the effectiveness, secondary effects, and absence of incidents described above must be obtained from software suppliers and verified. These descriptions are to be documented in the Ship Cyber Security and Resilience Program.

- interrupt, abort, roll back (5.4.3(6)(c)iii)2)).

In case of malfunctions or need for interruption during remote maintenance, it must be possible to safely interrupt maintenance and restore to the original state. Therefore, functions are needed for

interrupting work by authenticated personnel remotely or onboard, and for restoring software to its state prior to remote maintenance. The Ship cyber security and resilience program needs to describe the method of interruption and means of restoration in this case.

■ Records to be continuously kept or documented evidence

Rule 5.4.3(6)(d) iv) 2), Part X of the Rules

The shipowner is to present to the Society records or other documented evidence demonstrating implementation of the Ship cyber security and resilience program, i.e., that:

- remote access sessions have been recorded or logged and carried out as per relevant policies and user manuals, and
- installation of security patches and other software updates have been carried out in accordance with Management of change procedures and in cooperation with the supplier.

- remote access sessions have been recorded or logged and carried out as per relevant policies and user manuals

This requirement states that necessary information such as connection destinations and connection times need to be audited when remote access sessions occur, as described in "User manual (5.4.3(6)(c))" in the previous section "Content to be included in the program". This information must always be recorded during remote access and will be submitted as documentation for annual surveys. Note that this information is recorded as logs by device functions, so for annual surveys, these will be documented and submitted.

- installation of security patches and other software updates have been carried out in accordance with Management of change procedures and in cooperation with the supplier

This requirement demands the presentation of documents recorded during remote maintenance, as described in "Confirmation prior to remote software updates (5.4.3(6)(c)iii)2)" in the previous section "Content to be included in the program". This information must always be recorded when remote maintenance is performed and will be submitted as documentation for annual surveys.

5.4.3(7), Part X of the Rules / Use of mobile and portable devices

■ Contents to be included in the plan

Rule 5.4.3(7)(d) iv) 1), Part X of the Rules

The shipowner is to in the Ship cyber security and resilience program describe the management of mobile and portable devices, addressing at least the following requirements in this Chapter:

- policy and procedures (5.4.3(4)(c)iv)),
- physical block of interface ports (5.4.3(7)(a)),

-
- use by authorized personnel (5.4.3(7)(c)),
 - connect only authorized devices (5.4.3(7)(c)), and
 - consider risk of introducing malware (5.4.3(7)(c)).
-

It is generally known that computer-based systems can be impaired by malware infection via mobile or portable devices. Therefore, the connection of mobile or portable devices should be carefully considered.

The Ship cyber security and resilience program needs to include the following regarding mobile and portable devices:

- Policy and procedures (5.4.3(4)(c)iv))

The policies established by the shipowner regarding the use of mobile and portable devices needs to be documented and included in the Ship cyber security and resilience program.

In accordance with X Part 5.4.3(4)(c)iv), the policy needs to include the following:

- Procedures for verifying malware on portable devices and/or procedures for verifying legitimacy of software by digital signatures and watermarks
- Procedures for scanning devices prior to updating files to ship systems or downloading data from ship systems

If possible, please also include the manufacturer's recommended items regarding "Management of the use of portable and mobile devices" specified in No.10 of Table X4.1, Part X of the Rules.

- Physical block of interface ports (5.4.3(7)(a))

For computer-based systems that cannot fully meet the requirements of No.10 in Table X4.1, Part X of the Rules, unused interface ports need to be protected by physical means such as lockable port blockers. Describe the means and methods. Information on components that require physical port protection is included in the description of the Cyber security design description.

- Use by authorized personnel (5.4.3(7)(c))

The use of mobile and portable devices need to be managed to allow only authorized personnel. Therefore, include the following in the Ship cyber security and resilience program:

- Authorized personnel assigned for each system or device
- If physical access control is adopted, key management methods
- Management via user authentication

- Connect only authorized devices (5.4.3(7)(c))

Connection to computer-based systems need to be managed to allow only authorized devices through device control. Describe how to restrict the devices that can connect to the computer-based systems. If possible, also describe a list of devices that are permitted to connect.

- **Consider risk of introducing malware (5.4.3(7)(c))**

The use of mobile and portable devices needs to follow the policies that consider the risk of malware infiltrating computer-based systems. The Ship cyber security and resilience program needs to include content that considers the risk of malware infiltration.

■ **Records to be continuously kept or documented evidence**

Rule 5.4.3(7)(d) iv) 2), Part X of the Rules

The shipowner is to present to the Society records or other documented evidence demonstrating implementation of the Ship cyber security and resilience program, i.e., that:

- The use of mobile, portable or removable media is restricted to authorised personnel and follows relevant policies and procedures.
- Only authorised devices are connected to the computer-based systems. - Means to restrict use of physical interface ports are implemented as per approved design documentation.

- **The use of mobile, portable or removable media is restricted to authorized personnel and followed relevant policies and procedures.**

The use of mobile and portable devices needs to be restricted to a limited personnel. At the annual survey, submit records or other documented evidence showing the users and dates/times of use of the devices to the Society.

Additionally, evidence that these devices are being used in accordance with the policies and procedures for their use (X Part 5.4.3(4)(c)iv)), such as log files from malware scan or records of software legitimacy verification by digital signatures, needs to be documented and submitted to the Society as submission materials at the annual survey.

- **Only authorized devices are connected to the computer-based systems.**

Records, such as access logs, that certify that only authorized devices are connected to the computer-based systems need to be documented and submitted to the Society at the annual survey.

- **Means to restrict use of physical interface ports are implemented as per approved design documentation.**

The use of physical interface ports of mobile and portable devices needs to be restricted to prevent unauthorized physical access. Evidence proving that the means to restrict use of ports are implemented in accordance with approved design documents such as the "Cyber security design description", e.g. a photographs of a port protected by a port blocker, need to be documented and submitted to the Society as submission materials at the annual survey.



Detect

5.4.4(1), Part X of the Rules / Network operation monitoring

■ Contents to be included in the plan

Rule 5.4.4(1)(d) iv) 1), Part X of the Rules

The shipowner is to in the Ship cyber security and resilience program describe the management activities to detect anomalies in the computer-based systems and networks, addressing at least the following requirements in this Chapter. The following activities may be addressed together with incident response in 5.4.5(1).

- reveal and recognize anomalous activity (5.4.4),
- inspection of security audit records (5.4.4(1)(c)), and
- instructions or procedures to detect incidents (5.4.5(1)(a)).

This requirement aims to enhance cyber resilience by detecting the impact of cyber attacks for early response and recovery. Additionally, cyber attacks include those that do not result in actual damage (such as failed intrusions and communication attempts). Verification of such indicators improves the protection capabilities of computer-based systems.

The program must include the following content to address this requirement:

- reveal and recognize anomalous activity (5.4.4)

This section aims to detect signs of cyber attacks at an early stage during the operation phase.

By establishing means to recognize abnormal security events, security incidents can be detected early, the time to respond can be minimized, and damage can be minimized. Specifically, it is required to clarify the criteria for discovering abnormal events when confirming the audit records by the security functions of each computer-based system. As a means to achieve this objective, it is recommended to document the standard traffic volume and communication destinations of audit records that are assumed during normal navigation in the system subject to audit, in order to compare abnormal and normal states.

- inspection of security audit records (5.4.4(1)(c))

This section aims to detect signs of cyber attacks at an early stage and analyze vulnerabilities.

By regularly analyzing audit logs according to the above criteria, abnormal activities can be discovered from the history of activities, and abnormal activities that may be signs of cyber attacks can be detected early. In addition, through the analysis of audit logs, it is possible to discover vulnerable items among the system security functions. If vulnerabilities are discovered, it will lead to considering appropriate measures based on the log information.

- instructions or procedures to detect incidents (5.4.5(1)(a))

This section aims to determine whether the detected event constitutes an incident at an early stage.

Even if an abnormal security event is detected, there is a possibility of false detection, and the recommended response method varies depending on the type of attack. Therefore, it is required to determine in advance how to respond when an abnormal security event is detected. Specific means include determining the timing and personnel to be aware of the alarm, as well as the criteria for events that are assumed to be incidents and the criteria for events that should be judged as normal, in addition to the aforementioned alarms triggered by security functions.

■ Records to be continuously kept or documented evidence

Rule 5.4.4(1)(d) iv) 2), Part X of the Rules

The shipowner is to present to the Society records or other documented evidence demonstrating implementation of the Ship cyber security and resilience program, i.e., that:

- The computer-based systems are routinely monitored for anomalies by inspection of security audit records and investigation of alerts in the computer-based systems.

- The computer-based systems are routinely monitored for anomalies by inspection of security audit records and investigation of alerts in the computer-based systems.

This section aims to find signs of cyber attacks at an early stage and analyze vulnerabilities.

This requirement is one of the notable ones that require regular implementation regarding detection. Specifically, the ship operator needs to present to the Society samples of abnormal events recorded up to the first annual survey, plans for regular security audit record inspections and their records, and records of events judged to be incidents, if any.

■ 5.4.4(2), Part X of the Rules / Verification and diagnostic functions of computer-based system and networks

■ Contents to be included in the plan

Rule 5.4.4(2)(d) iv) 1), Part X of the Rules

The shipowner is to in the Ship cyber security and resilience program describe the management activities to verify correct operation of the security functions in the computer-based systems and networks, addressing at least the following requirements in this Chapter:

- test and maintenance periods (5.4.4(2)(c)) and
- periodic maintenance (2.2.3-5(9)).

This requirement aims to verify the proper functioning of security capabilities, discover malfunctions, and improve security capabilities. By regular confirmations of security capabilities,

their integrity can be improved. Additionally, when anomalies are found in security capabilities, there is a possibility of vulnerability to cyber incidents, so early detection and response are necessary.

This requirement requires two aspects to be documented in the Ship Cyber Security and Resilience Program: daily operational verification and specification of test items for special surveys conducted under the supervision of the Society.

- test and maintenance periods (5.4.4(2)(c))

This section states that for each product to which Chapter 4 of Part X applies, verification based on "19. Security functionality verification" in Table X2.4 of Chapter 4 of Part X needs to be conducted regularly. The plan for this verification should be described in the Ship cyber security and resilience program, and the results verified based on it need to be retained as documented records.

Here, it is required to determine the timing for conducting tests and maintenance using the verification and diagnostic functions required by this requirement in normal operating conditions. This enables regular confirmation of the soundness of security functions and maintenance of the effectiveness of security functions at all times.

The timing of these tests and maintenance needs to take into account the criticality of the component on the network. Therefore, for example, pay attention to the verification frequency of high-risk devices such as firewalls. Also, assign personnel with a deep understanding of the OT environment to be involved in testing and maintenance.

For related requirements in Chapter 4 of Part X, please refer to "19. Security functionality verification" on page 101 of the "Guidelines for Cyber resilience of on-board systems and equipment (Version 1.0)".

- periodic maintenance (2.2.3-5(9))

This section requires determining the contents to be confirmed in the Society's periodical surveys.

In periodical surveys, it is necessary to carry out a class attendance test based on the Ship cyber resilience test procedure (refer to 2.2.3-5(9)). When verifying security functions in this test, it is necessary to clarify the scope covered by the verification of security functions based on this requirement.

■ Records to be continuously kept or documented evidence

Rule 5.4.4(2)(d) iv) 2), Part X of the Rules

The shipowner is to present to the Society records or other documented evidence demonstrating implementation of the Ship cyber security and resilience program, i.e., that:

- The security functions in the computer-based systems are periodically tested or verified.

- The security functions in the computer-based systems are periodically tested or verified.

This item is for confirming whether the soundness of security functions is routinely tested.

To confirm that the testing and maintenance based on the requirement "Test and maintenance periods (5.4.4(2)(c))" for the operation phase in the previous item (5.4.4(2)(d)(iv)(1)) have been carried out, their records need to be disclosed to the Society.



Respond

5.4.5(1), Part X of the Rules / Incident response plan

■ Contents to be included in the plan

Rule 5.4.5(1)(d) iv) 1), Part X of the Rules

The shipowner is to in the Ship cyber security and resilience program describe incident response plans. The plans are to cover the computer-based systems in scope of applicability of this Chapter and are to address at least the following requirements in this Chapter:

- Description of who, when and how to respond to cyber incidents in accordance with requirements of 5.4.5(1)
- Procedures or instructions for local/manual control in accordance with requirements in 5.4.5(2)
- Procedures or instructions for isolation of security zones in accordance with requirements in 5.4.5(3)
- Description of expected behaviour of the computer-based systems in the event of cyber incidents in accordance with requirements in 5.4.5(4)

This section aims to clarify the information that should be included in the Incident response plan contained in the Ship cyber security and resilience program.

The items to be documented in the incident response plan are as follows:

- **Description of who, when and how to respond to cyber incidents in accordance with requirements of 5.4.5(1), Part X of the Rules (this requirement)**

This section summarizes the basic requirements for incident response plans.

The requirements specified in 5.4.5(1) referenced in this section are as follows:

Rule 5.4.5(1)(c) ii), Part X of the Rules

The Incident Response Plan is to be kept up-to-date (e.g. upon maintenance) during the operational life of the ship. The Incident response plan is to provide procedures to respond to detected cyber incidents on networks by notifying the proper authority, reporting needed evidence of the incidents and taking timely corrective actions, to limit the cyber incident impact to the network segment of origin.

Based on this section, the incident response plan must include the following items:

- **Notification to appropriate authorities regarding cyber incidents**

It is necessary to notify appropriate authorities (such as flag state governments if required) during or after the occurrence of cyber incidents.

- **Reporting of necessary evidence related to incidents**

When reporting cyber incidents, procedures for collecting necessary evidence must be documented.

- **Procedures for responding by implementing timely corrective measures to limit the impact of cyber incidents to the originating network segment**

Procedures must be established to limit damage to affected network segments and prevent incidents from spreading to other equipment, by disconnection and local controls as described below.

Rule 5.4.5(1)(c) iii), Part X of the Rules

The incident response plan is to, as a minimum, include the following information. The Incident response plan is to be kept in hard copy in the event of complete loss of electronic devices enabling access to it.

- 1) Breakpoints for the isolation of compromised systems
- 2) A description of alarms and indicators signalling detected ongoing cyber events or abnormal symptoms caused by cyber events
- 3) A description of expected major consequences related to cyber incidents
- 4) Response options, prioritizing those which do not rely on either shut down or transfer to independent or local control, if any
- 5) Independent and local control information for operating independently from the system that failed due to the cyber incident, as applicable

The incident response plan is to include each item of this requirement.

For each item, references to manufacturer documentation are in the Cyber Security Design Description prepared by the shipyard, which can be utilized during the preparation process.



4-3. Cyber security design description

5.4.5(1), Part X of the Rules / Incident response plan

P. 53

- **The Incident response plan is to be kept in hard copy in the event of complete loss of electronic devices enabling access to it.**

Since incident response plans are required to be stored in paper format, this requirement must also be specified in the plan, and paper storage is necessary.

- **Breakpoints for the isolation of compromised systems**

Referring to the following documents, breakpoints for system isolation are to be documented. To document breakpoints, isolation of affected zones and system isolation according to predetermined procedures for each computer-based system should be specified. In addition, the shipowner's policies should be reflected.

- Zones and Conduit Diagrams

Used to identify zone boundaries during isolation.

- Cyber Security Design Description

Used if zone isolation procedures are documented.

- Information Supporting Incident Response and Recovery Plans

Used if communications to be disconnected are documented in the incident response procedures for each equipment.

- **A description of alarms and indicators signalling detected ongoing cyber events or abnormal symptoms caused by cyber events**

Referring to the following documents, documentation of alarms and indications related to cyber events are to be included.

- Information Supporting Incident Response and Recovery Plans

These describe audit records, alerts, and displays required for forensic identification of abnormal conditions for each OT system.

These can be utilized to summarize the required items.

- **A description of expected major consequences related to cyber incidents**

Referring to the following documents, documentation of expected OT system behavior during cyber incidents is to be included.

- Cyber Security Design Description

Can be used if descriptions of stable shutdown states of systems are available.

- Information Supporting Incident Response and Recovery Plans

For each OT system, expected behavior during cyber incidents and stable shutdown states is documented. (behavior of controlled objects during OT system failures)

- **Response options, prioritizing those which do not rely on either shut down or transfer to independent or local control, if any**

Referring to the following documents, the prioritized response methods that maintain OT system functionality without shutdown or local control in the next section are to be documented, if exist.

- Information Supporting Incident Response and Recovery Plans

If available, document or reference any OT systems that have measures available to respond to cyber incidents while maintaining normal control functions.

- **Independent and local control information for operating independently from the system that failed due to the cyber incident, as applicable**

Referring to the following documents, it is to be documented local control methods for propulsion equipment to operate independently when OT systems fail.

- Cyber Security Design Description
Can be used for descriptions of local control methods.
- Information Supporting Incident Response and Recovery Plans
Can be used or referenced for descriptions of local control methods.

- **Procedures or instructions for local/manual control in accordance with requirements in 5.4.5(2) , Part X of the Rules**

This section aims to include procedures or instructions for switching to local/manual control in the event of a cyber incident in the Incident response plan. Procedures or instructions related to local/manual control mean, for example, when a cyber incident against the remote control system for main engines is detected, the chief engineer switches the engines to local control and instructs a engineer to control the engines locally.

For this requirement, functional description documents are prepared in the cyber security design description created by the shipyard, which can be utilized during the preparation process.

4-3. Cyber security design description



5.4.5(2), Part X of the Rules / Local, independent and/or manual operation

P. 54

- **Procedures or instructions for isolation of security zones in accordance with requirements in 5.4.5(3), Part X of the Rules**

This section aims to include information in the Incident response plan so that responsible person onboard can give instructions to each crew member and isolate security zones quickly and accurately when a cyber incident occurs. Procedures or instructions related to the isolation of security zones mean, for example, when a cyber incident against the Automatic Radar Plotting Aid (ARPA) is detected, the captain instructs a crew member to operate the physical ON/OFF switch or disconnect the cable to the router/firewall.

For this requirement, functional description documents are prepared in the cyber security design description created by the shipyard, which can be utilized during the preparation process.

4-3. Cyber security design description



545.4.5(3), Part X of the Rules / Network isolation

P. 54

- **Description of expected behaviour of the computer-based systems in the event of cyber incidents in accordance with requirements in 5.4.5(4) , Part X of the Rules**

This section aims to include information on how computer-based systems reach a safe state in the event of a cyber incident in the Incident response plan. Information on how computer-based systems reach a safe state means, for example, when a cyber incident against the engine control

device is detected, the engine control device automatically controls the engine to output 0 (when entering/leaving port) or to a ship speed of 10 knots (when in ocean navigation).

For this requirement, functional description documents are prepared in the cyber security design description created by the shipyard, which can be utilized during the preparation process.



4-3. Cyber security design description

545.4.5(4), Part X of the Rules / Fallback to a minimal risk condition

P. 54

■ Records to be continuously kept or documented evidence

Rule 5.4.5(1)(d) iv) 2), Part X of the Rules

The shipowner is to present to the Society records or other documented evidence demonstrating implementation of the Ship cyber security and resilience program, i.e., that:

- The incident response plans are available for the responsible personnel onboard.
- Procedures or instructions for local/manual controls are available for responsible personnel onboard.
- Procedures or instructions for disconnection/isolation of security zones are available for responsible personnel onboard.
- Any cyber incidents have been responded to in accordance with the incident response plans.

This section is to confirm whether the contents described in the Incident response plan included in the Ship cyber security and resilience program are being continuously implemented

- **The incident response plans are available for the responsible personnel onboard.**

Please create documented evidence showing that the responsible person is continuously managing the Incident response plan. Since incident response plans are required to be stored in paper format, this must also be proven.

- **Procedures or instructions for local/manual controls are available for responsible personnel onboard.**

Please create documented evidence showing that the responsible person is continuously managing the procedures or instructions related to local/manual control.

- **Procedures or instructions for disconnection/isolation of security zones are available for responsible personnel onboard.**

Please create documented evidence showing that the responsible person is continuously managing the procedures or instructions for disconnection/isolation of security zones.

- **Any cyber incidents have been responded to in accordance with the incident response plans.**

Please create a list of cyber incidents that have occurred and their response records.

5.4.5(2), Part X of the Rules / Local, independent and/or manual operation

Rule 5.4.5(2)(d) iv), Part X of the Rules

No specific requirements.

5.4.5(3), Part X of the Rules / Network isolation

Rule 5.4.5(3)(d) iv), Part X of the Rules

No specific requirements.

5.4.5(4), Part X of the Rules / Fallback to a minimal risk condition

Rule 5.4.5(4)(d) iv), Part X of the Rules

No specific requirements.



Recover

5.4.6(1), Part X of the Rules / Recovery plan

■ Contents to be included in the plan

Rule 5.4.6(1)(d) iv) 1), Part X of the Rules

The shipowner is to in the Ship cyber security and resilience program describe incident recovery plans. The plans are to cover the computer-based systems in scope of applicability of this Chapter and are to address at least the following requirements in this Chapter:

- Description of who, when and how to restore and recover from cyber incidents in accordance with requirements in 5.4.6(1)
- Policy for backup addressing frequency, maintenance and testing of the backups, considering acceptable downtime, availability of alternative means for control, vendor support arrangements and criticality of the computer-based systems in accordance with requirements in 5.4.6(2).
- Reference to user manuals or procedures for backup, shutdown, reset, restore and restart of the computer-based systems in accordance with requirements in 5.4.6(2) and 5.4.6(3).

A recovery plan is a document that outlines the procedures for restoring computer-based system within the scope of this chapter to a functional state following disruption or failure caused by a cyber incident.

The recovery plan is to satisfy the following requirements.

Description of who, when and how to restore and recover from cyber incidents in accordance with requirements in 5.4.6(1)

It is required to clarify the roles and procedures of onboard personnel regarding the system recovery procedures specified in 5.4.6(1). The content must comply with the requirements for recovery plans stipulated in the same requirement.

The requirements for recovery plans in this requirement are as follows:

Rule 5.4.6(1)(c) i), Part X of the Rules

The various stakeholders involved in the design and construction phases of the ship are to provide information to the shipowner for the preparation of the recovery plan to be placed onboard at the first Annual Survey. The recovery plan is to be kept up-to-date (e.g. upon maintenance) during the operational life of the ship.

As described in this section, manufacturers and shipyards provide information for recovery plans. Therefore, when shipowners prepare recovery plans, they can reference this information. Since the the Cyber Security Design Description refers to the necessary documents, recovery plans can

be prepared while reviewing that content.



4-3. Cyber security design description

P. 56

545.4.6(1), Part X of the Rules / Recovery plan

Additionally, recovery plans are to be updated throughout the operational life of the ship.

Rule 5.4.6(1)(c) ii), Part X of the Rules

Recovery plans are to be easily understandable by the crew and external personnel and include essential instructions and procedures to ensure the recovery of a failed system and how to get external assistance if the support from ashore is necessary. In addition, software recovery medium or tools essential for recovery on board are to be available.

As described in this section, owners can adopt external support for system recovery such as service engineers of the manufacturer. Recovery plans must specifically describe how to obtain the necessary support for ship system recovery.

Additionally, media or tools necessary for recovery are to be prepared. (such as recovery CDs, USB memory devices, etc.)

Rule 5.4.6(1)(c) iii) 1), Part X of the Rules

When developing recovery plans, the various systems and subsystems involved are to be specified. The following recovery objectives are also to be specified:

- 1) System recovery: methods and procedures to recover communication capabilities are to be specified in terms of Recovery Time Objective (RTO). This is defined as the time required to recover the required communication links and processing capabilities.
- 2) Data recovery: methods and procedures to recover data necessary to restore safe state of OT systems and safe ship operation are to be specified in terms of Recovery Point Objective (RPO). This is defined as the longest period of time for which an absence of data can be tolerated.

As described in this section, the following objectives are to be specified in recovery plans for planning backup and restoration activities:

- Recovery Time Objective (RTO)

This objective represents the target time for recovery activities from an incident to restore data to its backed-up state and resume operational communications and processing. In other words, this is the acceptable period until getting back to normal operations. In recovery plans, considering this objective, the sequence of recovery operations will be determined.

- **Recovery Point Objective (RPO)**

This objective represents the maximum acceptable duration of data loss that occurs when data is corrupted or lost due to an incident and restored from backup data during recovery activities from the incident. In other words, this is the maximum value of the period from the last backup to the incident. In recovery plans, considering this objective, the backup frequency will be determined.

For the concepts of these two objectives, see Figure 4.8.

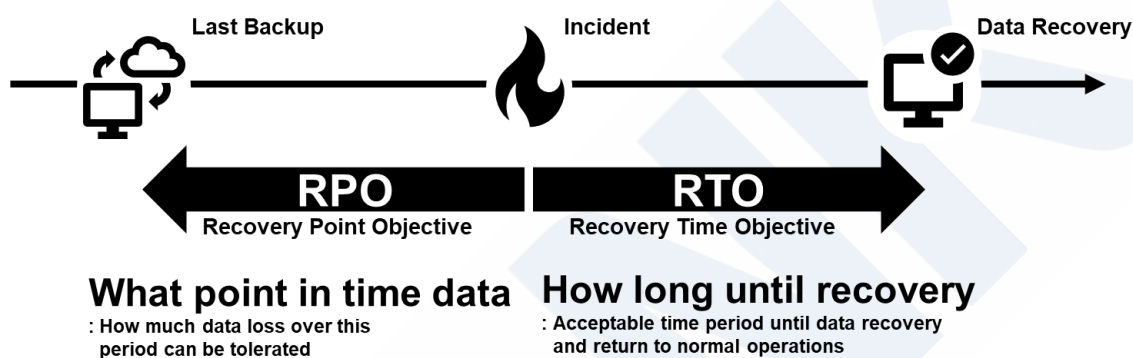


Figure 4.8 Recovery Point Objective and Recovery Time Objective

These Recovery Time Objectives and Recovery Point Objectives should be established for equipment as necessary and reflected in recovery procedures and backup frequency.

Rule 5.4.6(1)(c) iv) 1), Part X of the Rules

Once the recovery objectives are defined, a list of potential cyber incidents is to be created, and the recovery procedure developed and described. Recovery plans are to include, or refer to the following information;

- 1) Instructions and procedures for restoring the failed system without disrupting the operation from the redundant, independent or local operation.
- 2) Processes and procedures for the backup and secure storage of information.
- 3) Complete and up-to-date logical network diagram.
- 4) The list of personnel responsible for restoring the failed system.
- 5) Communication procedure and list of personnel to contact for external technical support including system support vendors, network administrators, etc.
- 6) Current configuration information for all components.

After determining RPO and RTO, the following requirements need to be addressed:

- **Instructions and procedures for restoring the failed system without disrupting the operation from the redundant, independent or local operation.**

In "Respond," when operations have been transferred to independent backup control systems or local control systems, it is necessary to restore remote control operations without interrupting these operations. Instructions and procedures for this purpose must be documented or referenced.

For the related "Respond" requirement, please refer to the explanation of "Local, independent and/or manual operation" in the incident response plan.



4-7. Ship cyber security and resilience program

P. 113

5.4.5(1), Part X of the Rules / Incident response plan

- **Processes and procedures for the backup and secure storage of information.**
Regular backup procedures for each OT system are to be documented or referenced.
- **Complete and up-to-date logical network diagram.**
Network diagrams are to be maintained as a reference for restoring the shipboard network. Logical network diagrams include Zone and Conduit Diagrams prepared by the system integrator (shipyard), and Topology Diagrams prepared by suppliers (manufacturers), and they are to be updated and referenced as necessary.
- **The list of personnel responsible for restoring the failed system.**
For the restoration of shipboard systems, rapid response is required, so it is necessary to assign the responsible person for each restoration task. Please create a list of personnel responsible for this purpose.
- **Communication procedure and list of personnel to contact for external technical support including system support vendors, network administrators, etc.**
For the recovery of shipboard systems, as described in section 5.4.6(1)(c)ii), it is expected that external assistance may be utilized. Please create a list of contact information and communication methods for external technical support available for this purpose.
- **Current configuration information for all components.**
The current configuration values for each shipboard system may be effective for system recovery. Please include or reference this information in the recovery plan.

Rule 5.4.6(1)(c) vi), Part X of the Rules

Recovery plans in hard copy onboard and ashore are to be available to personnel responsible for cyber security and who are tasked with assisting in cyber incidents.

- **Recovery plans in hard copy onboard and ashore are to be available to personnel**

responsible for cyber security and who are tasked with assisting in cyber incidents.

Furthermore, since recovery plans are required to be stored in hard copy, the plan shall specify this requirement and needs to be stored in hard copy.

Policy for backup addressing frequency, maintenance and testing of the backups, considering acceptable downtime, availability of alternative means for control, vendor support arrangements and criticality of the computer-based systems in accordance with requirements in 5.4.6(2).

In this section, the backup and restoration capabilities for each computer-based system and network are to address the following points:

- Backup Frequency:

A backup plan is to be developed based on the recommended backup frequency for each computer-based system as specified by the supplier.

- Backup Maintenance and Testing Considering Acceptable Downtime:

Maintenance and testing of backups are to be conducted while ensuring acceptable downtime when the system is operational.

- Availability of Alternative Means for Control:

The use of alternative means when maintaining and testing backups for each computer-based system and network is to be indicated.

- Vendor Support System:

Support from the supplier or maintenance provider for the maintenance and testing of backups for each computer-based system and network is to be indicated.

- Importance of computer-based system:

The importance of each computer-based system to the operation must be determined. Specifically, the recovery activities' priority in the event of a cyber incident affecting multiple computer-based system must be established.

Reference to user manuals or procedures for backup, shutdown, reset, restore and restart of the computer-based systems in accordance with requirements in 5.4.6(2) and 5.4.6(3).

It is required to refer to the procedures for "backup, shutdown, reset, restore, and restart" described in the "Information Supporting Incidents" provided by the supplier. The systems integrator is required to create a list of references for each computer-based system and the information that can be referred to in the "Cyber Security Design Description." Therefore, when preparing the plan, this list is to be transcribed.

4-3. Cyber security design description



5.4.6(3), Part X of the Rules / Controlled shutdown, reset, roll-back and restart

Table 4.7 List of Documents Referencing Recovery Information

Computer-based system	Product Name	Relevant Documents
Main Engine Control System	***	Recovery Plan (Reference No. : ***)

■ Records to be continuously kept or documented evidence

Rule 5.4.6(1)(d) iv) 2), Part X of the Rules

The shipowner is to present to the Society records or other documented evidence demonstrating implementation of the Ship cyber security and resilience program, i.e., that:

- Instructions and/or procedures for incident recovery are available for the responsible personnel onboard.
- Equipment, tools, documentation, and/or necessary software and data needed for recovery is available for the responsible personnel onboard.
- Backup of the computer-based systems have been taken in accordance with the policies and procedures.
- Manuals and procedures for shutdown, reset, restore and restart are available for the responsible personnel onboard.

This section is intended to verify whether the contents described in the recovery plan included in the Ship cyber security and resilience program are being continuously implemented.

- **Instructions and/or procedures for incident recovery are available for the responsible personnel onboard.**

The instructions and procedures for incident recovery included in the recovery plan are to be kept accessible to the responsible personnel on board.

- **Equipment, tools, documentation, and/or necessary software and data needed for recovery is available for the responsible personnel onboard.**

The resources required for recovery from an incident are to be clearly identified, and the responsible personnel on board is to be able to respond promptly. Records or other documented evidence to prove this may include the following examples:

- Equipment and Tools List: A list detailing the necessary equipment and tools for recovery and their storage locations.
- Software and Data List: A list detailing the necessary software and data for recovery.

- **Backup of the computer-based systems have been taken in accordance with the policies and procedures.**

To prevent data loss, regular and accurate backups are to be performed. Records or other documented evidence to prove this may include the following examples:

- Backup Records: Records of backups performed based on a regular backup schedule.

- **Manuals and procedures for shutdown, reset, restore and restart are available for the responsible personnel onboard.**

The manuals and procedures for shutdown, reset, restore, and restart included in the recovery plan are to be kept accessible to the responsible personnel on board.

5.4.6(2), Part X of the Rules / Backup and restore capability

Rule 5.4.6(2)(d)iv), Part X of the Rules

No specific requirements.

5.4.6(3), Part X of the Rules / Controlled shutdown, reset, roll-back and restart

Rule 5.4.6(3)(d)iv), Part X of the Rules

No specific requirements.

Chapter 5 Explanation of Surveys

This chapter explains the details regarding the surveys specified in Chapter 5, Part X (UR E26).

Chapter 5, Part X (UR E26) requires the execution of surveys by Systems integrators and shipowners. Systems integrators are required to conduct "commissioning surveys" during the commissioning phase after design and construction. These surveys verify the operation of the security capabilities of the network and each computer-based system, ensuring compliance with the requirements of Chapter 5, Part X (UR E26).

Shipowners are required to conduct attendance surveys corresponding to the timing of periodical surveys. These surveys demonstrate and/or verify the operation of the security capabilities of the network and each computer-based system, ensuring that the vessel maintains compliance with the requirements of Chapter 5, Part X (UR E26).

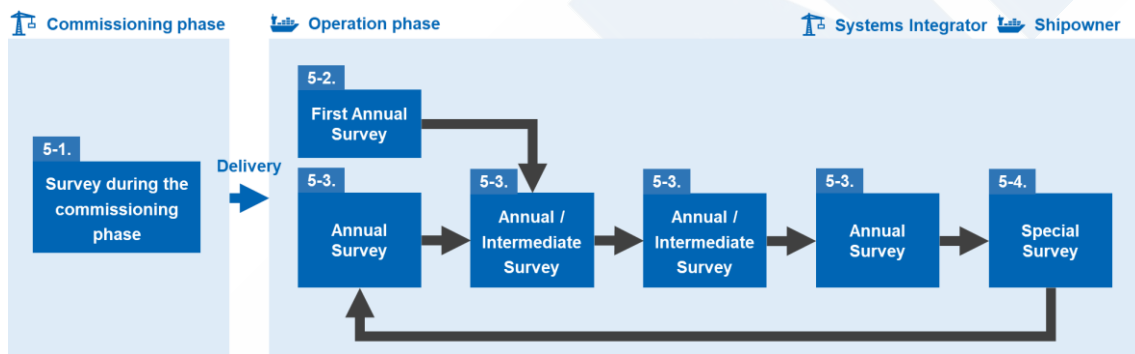


Figure 5.1 Surveys in Chapter 5, Part X (UR E26)

Details of each survey are explained on the following pages.



Survey Requirements



5-1. Survey during the commissioning phase

P. 127



5-2. First Annual Survey

P. 130



5-3. Subsequent Annual Surveys / Intermediate Survey

P. 132



5-4. Special Survey

P. 133

5-1. Survey during the Commissioning Phase

During the commissioning phase, it is required to [verify the operation of the security capabilities of the network and each computer-based system in accordance with the approved "Ship Cyber Resilience Test Procedure."](#)

The requirements for this test are specified in the "Commissioning Phase" section of Chapter 5.4 of Part X.

Rule 2.2.3-4(2)(a), Part X of the Rules

The content of this document* is specified for the Commissioning phase in each subsection "Demonstration of compliance" in 5.4.

* Ship Cyber Resilience Test Procedures

These requirements are included as test items in the "Ship Cyber Resilience Test Procedure." Therefore, in this Guidelines, the explanations of each requirement are described in Chapter 4, "Explanation of Submission of Plans and Documents," specifically in section "4-6. Ship Cyber Resilience Test Procedure." Please refer to that section for detailed explanations of each requirement.



4-6. Ship cyber resilience test procedure

P. 63



5.4.2, Part X of the Rules / Identify



5.4.2(1), Part X of the Rules / Vessel asset inventory

P. 66



5.4.3, Part X of the Rules / Protect



5.4.3(1), Part X of the Rules / Security zones and network segmentation

P. 68



5.4.3(2), Part X of the Rules / Network protection safeguards

P. 69



5.4.3(3), Part X of the Rules / Antivirus, antimalware, antispam and other protections from malicious code

P. 71



5.4.3(4), Part X of the Rules / Access control

P. 72



5.4.3(5), Part X of the Rules / Wireless communication

P. 72



5.4.3(6), Part X of the Rules / Remote access control and communication with untrusted networks

P. 73

	5.4.3(7), Part X of the Rules / Use of mobile and portable devices	P. 76
	5.4.4 Part X of the Rules / Detect	
	5.4.4(1), Part X of the Rules / Network operation monitoring	P. 78
	5.4.4(2), Part X of the Rules / Verification and diagnostic functions of computer-based system and networks	P. 82
	5.4.5 Part X of the Rules / Respond	
	5.4.5(2), Part X of the Rules / Local, independent and/or manual operation	P. 84
	5.4.5(3), Part X of the Rules / Network isolation	P. 84
	5.4.5(4), Part X of the Rules / Fallback to a minimal risk condition	P. 85
	5.4.6 Part X of the Rules / Recover	
	5.4.6(1), Part X of the Rules / Recovery plan	P. 87
	5.4.6(2), Part X of the Rules / Backup and restore capability	P. 87
	5.4.6(3), Part X of the Rules / Controlled shutdown, reset, roll-back and restart	P. 88

Additionally, the "Survey during the Commissioning Phase" specifies the conditions under which tests related to computer-based system may be omitted, as outlined below

Rule 2.2.3-4(2)(b), Part X of the Rules

For each computer-based system, the required inherent security capabilities and configuration thereof are verified and tested in the certification process of each computer-based system (see Chapter 4). Testing of such security functions may be omitted if specified in the respective subsection "Commissioning phase" in 5.4, on the condition that these security functions have been successfully tested during the certification of the computer-based system as per Chapter 4. Nevertheless, all tests are to be included in the Ship cyber resilience test procedure and the decision to omit tests will be taken by the Society. Tests may generally not be omitted if findings/comments are carried over from the certification process to the commissioning phase, if the respective requirements have been met by compensating countermeasures, or due to other reasons such as modifications of the computer-based system after the certification process.

Computer-based systems within the scope of Chapter 5, Part X (UR E26) are to be approved by the Society in accordance with Chapter 4, Part X (UR E27), during which the security capabilities of the computer-based system are verified. While the commissioning phase requires verification of the security capabilities of computer-based system, if these tests have been successfully conducted through the approval process of Chapter 4, Part X (UR E27), it is possible to omit these tests.

When omitting the relevant tests, the systems integrator is to contact our machinery department with the test results for the relevant security capabilities as specified by Chapter 4, Part X (UR E27).

5-2. First Annual Survey

Rule 2.2.3-5(7)(c), Part X of the Rules

After the Society has approved the Ship cyber security and resilience program, the shipowner is to in the first Annual Survey demonstrate compliance by presenting records or other documented evidence of implementation of the processes described in the approved Ship cyber security and resilience program.

During the first annual survey, it is required to [demonstrate the operational status based on the approved "Ship cyber security and resilience program."](#) Therefore, the shipowner is to implement the program in practice and prepare documents that serve as evidence of the program's operation, such as records, [by the first annual survey.](#)

In this survey, the Society authorised Surveyor will verify that [records/evidence are created and maintained as described in the "Ship cyber security and resilience program."](#) This Guidelines provides detailed explanations of the required records or evidence in Chapter 4, "Explanation of Submission of Plans and Documents," specifically in section "4-7. Ship cyber security and resilience program." Please refer to that section for detailed explanations of each requirement for this survey.



4-7. Ship cyber security and resilience program

P. 89



5.4.2, Part X of the Rules / Identify



5.4.2(1), Part X of the Rules / Vessel asset inventory

P. 93



5.4.3, Part X of the Rules / Protect



5.4.3(1), Part X of the Rules / Security zones and network segmentation

P. 96



5.4.3(3), Part X of the Rules / Antivirus, antimalware, antispam and other protections from malicious code

P. 98



5.4.3(4), Part X of the Rules / Access control

P. 100



5.4.3(6), Part X of the Rules / Remote access control and communication with untrusted networks

P. 104



5.4.3(7), Part X of the Rules / Use of mobile and portable devices

P. 106



5.4.4 Part X of the Rules / Detect



5.4.4(1), Part X of the Rules / Network operation monitoring

P. 109



5.4.4(2), Part X of the Rules / Verification and diagnostic functions of computer-based system and networks

P. 110



5.4.5 Part X of the Rules / Respond



5.4.5(1), Part X of the Rules / Incident response plan

P. 113



5.4.6 Part X of the Rules / Recover



5.4.6(1), Part X of the Rules / Recovery plan

P. 119

5-3. Subsequent Annual Surveys / Intermediate Survey

Rule 2.2.3-5(8), Part X of the Rules

In the subsequent Annual Surveys of the ship, the shipowner is to upon request by the Society demonstrate implementation of the Ship cyber security and resilience program.

Firstly, there is no difference in the inspection content between the subsequent annual surveys and the intermediate surveys. Therefore, they are explained together in this section.

During the subsequent annual surveys / intermediate survey, it is required to [demonstrate the operational status based on the approved "Ship cyber security and resilience program,"](#) similar to the first annual survey. Therefore, the operation must be based on this program, and all records must be created. However, unlike the first annual survey, the verification of records during subsequent surveys will be conducted "at the request of the Society," meaning that [not all records will be reviewed, but rather a sampling may be done](#). This decision is at the discretion of the surveyor and generally applies to cases where there have been changes to the ship's network or the program since the last survey.

- Changes to the computer-based system:

If there have been changes to the computer-based system, such as software updates or hardware modifications, it will be verified that change management has been conducted based on the ship cyber security and resilience program.

- Updates to the Ship Cyber Security and Resilience Program:

If the program has been updated due to operational reviews, the relevant sections will be verified after re-approval by the Society.

This Guidelines provide detailed explanations of the records or evidence that need to be created in Chapter 4, "Explanation of Submission of Plans and Documents," specifically in "4-7. Ship cyber security and resilience program." Please refer to that section for a detailed explanation of each requirement for this test.



4-7. Ship cyber security and resilience program

P. 89

5-4. Special Survey

Rule 2.2.3-5(9), Part X of the Rules

Upon renewal of the ship's Certificate of Classification, the shipowner is to carry out testing witnessed by the Society in accordance with the Ship cyber resilience test procedure. Certain security safeguards are to be demonstrated at Special Survey whereas other need only be carried out upon request by the Society based on modifications to the computer-based systems as specified in subsections "Operation phase" in 5.4.

During the Special Surveys, in addition to the inspections required for the Subsequent Annual Surveys / Intermediate Survey, it is required to [verify the operation of the network and the security capabilities of each computer-based system in accordance with the "Ship cyber security and resilience test procedure."](#) The "Ship cyber security and resilience test procedure" is prepared by the systems integrator (shipyard), tested during the commissioning phase, and handed over to the shipowner. Each requirement for this test is included in the test items of this document. Therefore, for a detailed explanation of each requirement for this test, please refer to "4-6. Ship cyber security and resilience test procedure" in Chapter 4, "Explanation of Submission of Plans and Documents," of this Guidelines.



4-6. Ship cyber resilience test procedure

P. 63

• Requirements for Attendance Surveys



5.4.2, Part X of the Rules / Identify



5.4.2(1), Part X of the Rules / Vessel asset inventory

P. 66



5.4.3, Part X of the Rules / Protect



5.4.3(1), Part X of the Rules / Security zones and network segmentation

P. 68



5.4.3(3), Part X of the Rules / Antivirus, antimalware, antispyware and other protections from malicious code

P. 71



5.4.3(6), Part X of the Rules / Remote access control and communication with untrusted networks

P. 73



5.4.3(7), Part X of the Rules / Use of mobile and portable devices

P. 76

Some tests required in this inspection are to be conducted "when requested by the Society based on changes to the computer-based systems." Therefore, if there have been no changes to the computer-

based systems, it is generally possible to omit the relevant tests. The list of requirements for which attendance surveys can be omitted is as follows:

• **Requirements for Which Attendance Surveys Can Be Omitted:**



5.4.3, Part X of the Rules / Protect



5.4.3(2), Part X of the Rules / Network protection safeguards

P. 69



5.4.3(5), Part X of the Rules / Wireless communication

P. 72



5.4.4 Part X of the Rules / Detect



5.4.4(1), Part X of the Rules / Network operation monitoring

P. 78



5.4.5 Part X of the Rules / Respond



5.4.5(2), Part X of the Rules / Local, independent and/or manual operation

P. 84



5.4.5(3), Part X of the Rules / Network isolation

P. 84



5.4.5(4), Part X of the Rules / Fallback to a minimal risk condition

P. 85



5.4.6 Part X of the Rules / Recover



5.4.6(2), Part X of the Rules / Backup and restore capability

P. 87



5.4.6(3), Part X of the Rules / Controlled shutdown, reset, roll-back and restart

P. 88



NIPPON KAIJI KYOKAI

**Plan Approval and Technical Solution Division
Machinery Department**

3-3 Kioi-cho, Chiyoda-ku, Tokyo 102-0094, JAPAN
Tel : +81-3-5226-2022
E-mail : mcd@classnk.or.jp

www.classnk.com