

# 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.

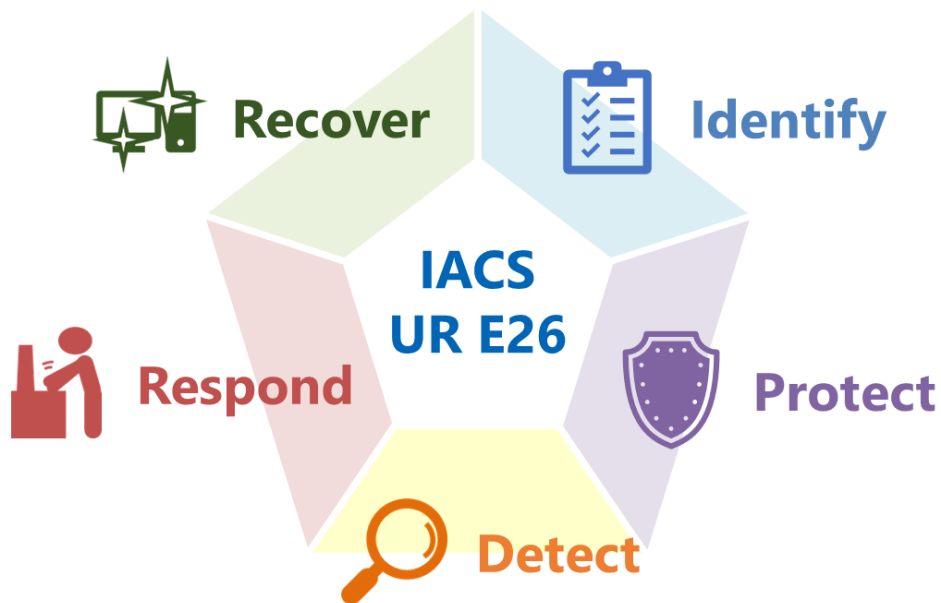


Figure 1.1 Conceptual figure of Chapter 5, Part X (UR E26)

## 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.

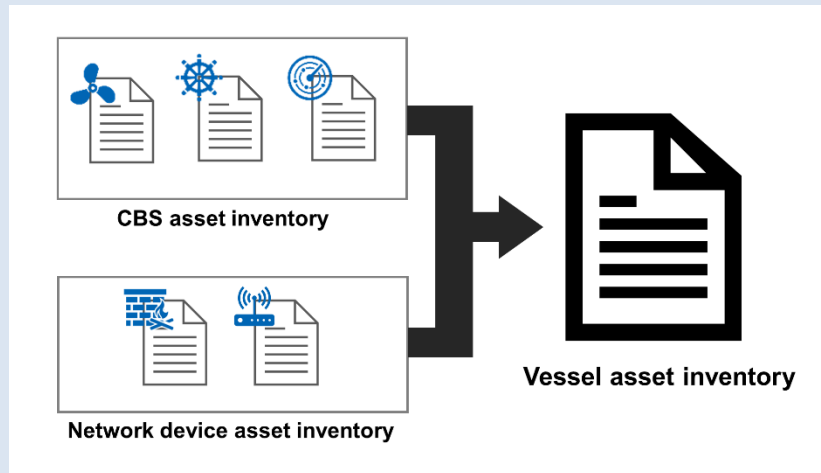


Figure 1.2 Vessel asset inventory

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.

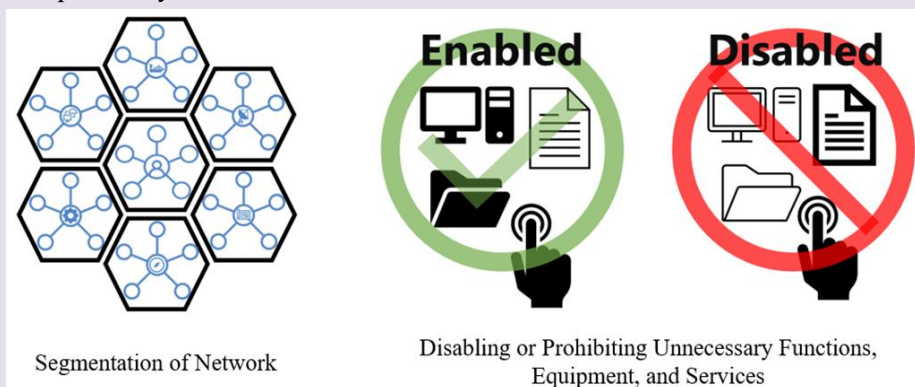




Fig.1.3 Significant safeguards required by these requirements

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.

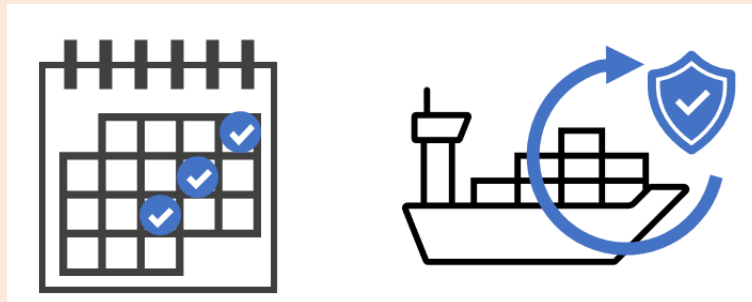




Figure 1.5 Protection through periodic verification of security functions

### 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.

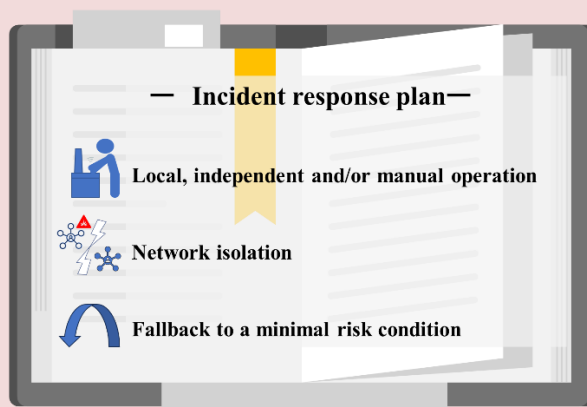




Figure 1.6 Incident response plan

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.

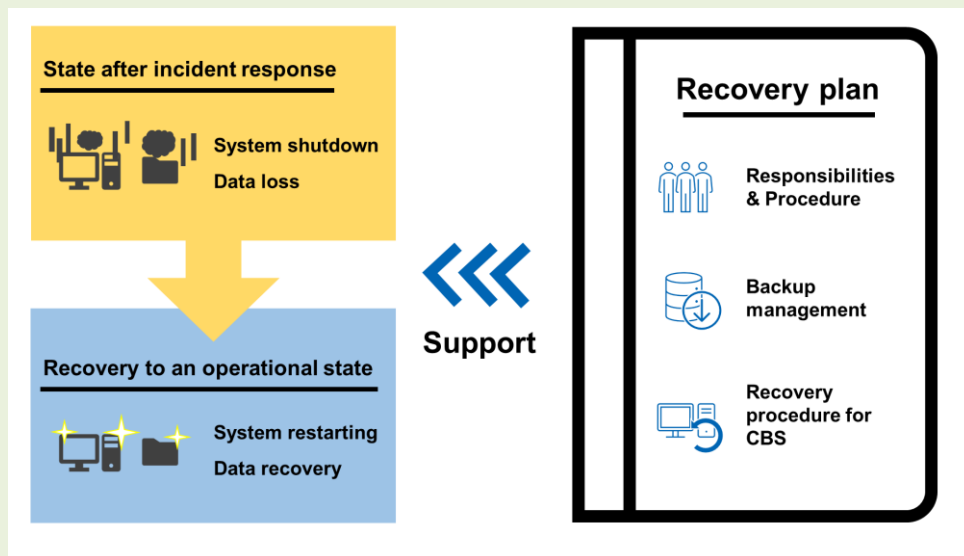




Figure 1.7 Recovery plan

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.