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 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 make the assets owned by the ship, such as systems and network devices, "visible." Specifically, this involves creating an inventory of the ship's assets. This inventory is called the vessel asset inventory and clarifies what CBSs and equipment are currently onboard.

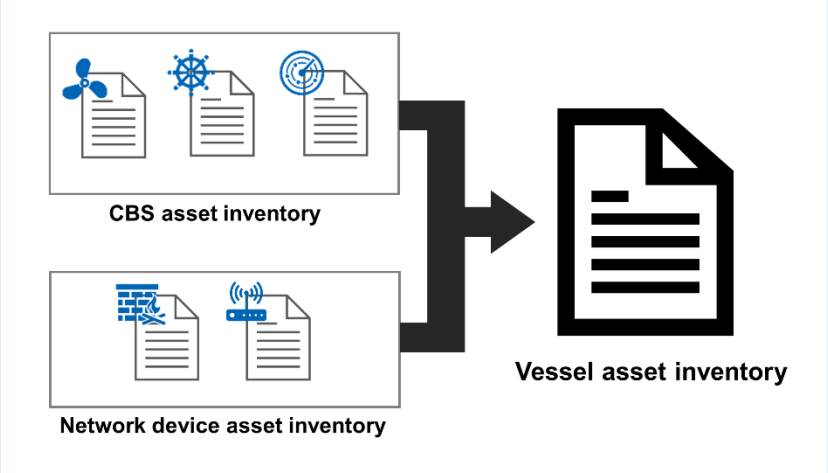

Figure 1.2 Vessel asset inventory

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, including the location of the equipment onboard after being integrated into the ship's network, connected devices, and whether there is external access.

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

- It is possible to understand the security risks of the ship's assets by comparing information on security weaknesses and their fixes obtained from manufacturers with the information in the vessel asset inventory.
- By making detailed information about the ship's assets visible in advance, it is possible to respond quickly in the event of a cyber incident.

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. A particularly important aspect is "segmenting" the networks connected to the ship's assets. Segmentation means to partitioning computer 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.

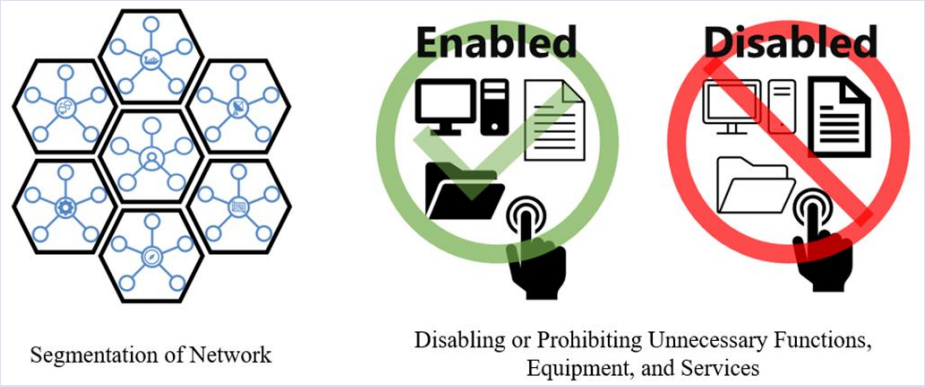

Fig.1.3 Especially important safeguards required by these requirements

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 limits the 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 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 find attacks. 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 recognition of cyber attacks or other threats that the ship has experienced.

- **Network operation monitoring:** Many cyber attacks or other threats 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 and triggering alarms for out-of-design network activities that are suspected to be attacks, attacks can be found.

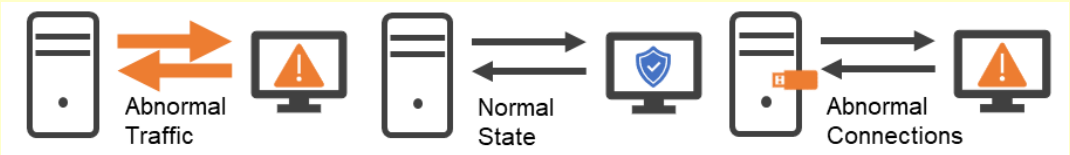

Figure 1.4 Alarms triggered by out-of-design network activities

Furthermore, during normal operations, it is necessary to establish verification procedures, methods, and timings for verifying that the security functions related to identify, protect, detect, respond, and recover, including the above-mentioned network operation monitoring, are functioning correctly. This enhances the ship's cyber resilience against cyber attacks and other threats.

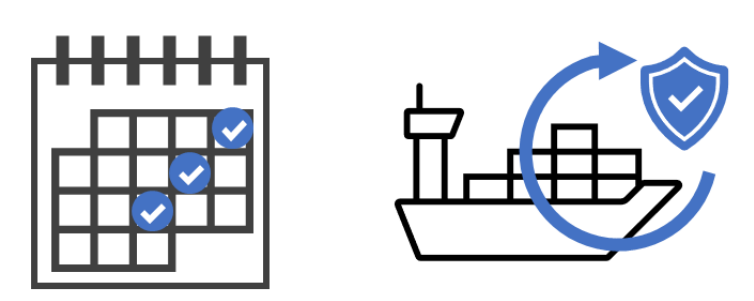

Figure 1.5 Protection through periodic verification of security functions

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 acting 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, and other propulsion equipment 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 minimal risk condition" means a stable, stopped condition that reduces safety risks in the event of a cyber incident. The plan should create specific procedures for how to achieve a s stable, stopped condition for each computer system provided by the systems integrator, referring to information on each system.

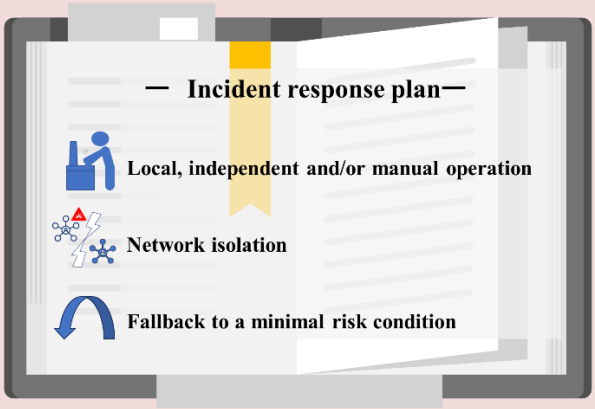

Figure 1.6 Incident response plan

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, damages can be minimized.

What to do?

- Systems integrators are required to compile and document information to assist shipowners in creating Incident response plans.
- Shipowners are 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 an operational state after a disruption or failure caused by a cyber incident. By planning and implementing a recovery plan according to these requirements, CBSs and networks can be quickly restored.

In the recovery plan, "roles and procedures for personnel in recovering from a cyber incident" and "management of backups, including maintenance and testing" are to be developed based on the shipowner's policy. Additionally, when creating the recovery plan for each CBS, it is necessary to refer to the "Information supporting the owner's incident response and recovery plan. "

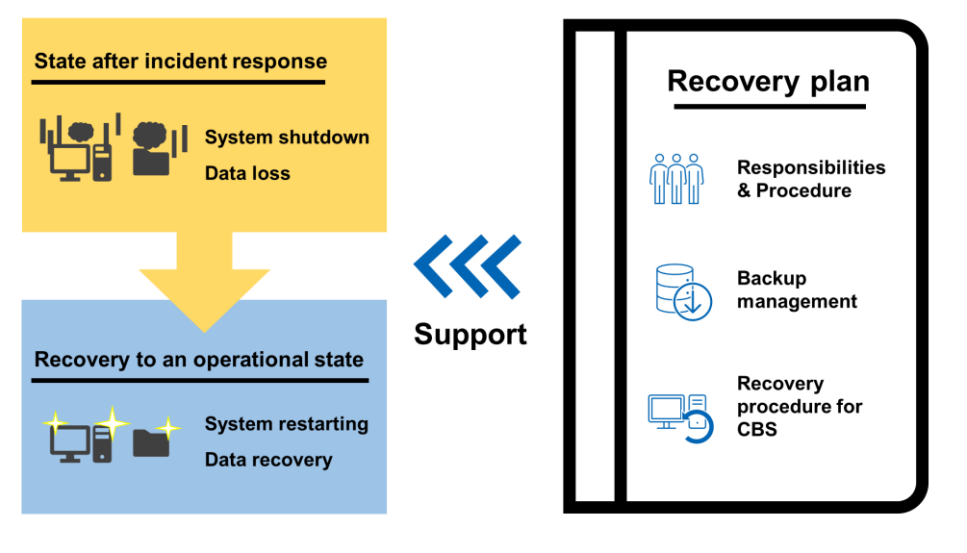

Figure 1.7 Recovery plan

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

- Clarification of the responsibilities and tasks of each personnel in recovering from an incident.
- Ensuring that recovery is performed with procedures appropriate to each computer system.

What to do?

- The systems integrator is required to compile and document information that will enable the shipowner to create recovery plan for each CBS.
- The shipowner is required to manage backups, including maintenance and testing, and ensure that recovery work is performed swiftly and accurately according to the plan's procedures.