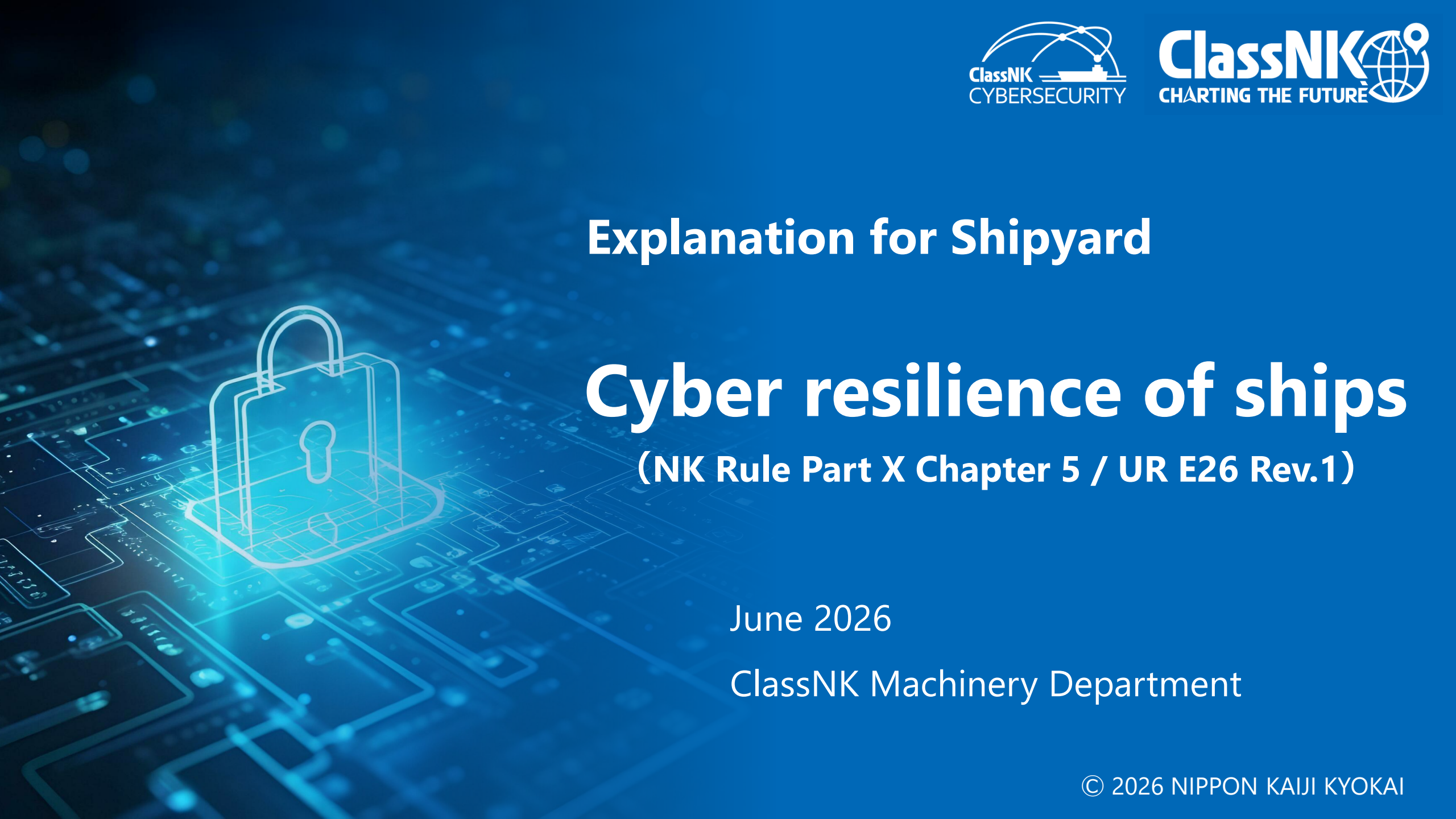


Explanation for Shipyard

Cyber resilience of ships

（NK Rule Part X Chapter 5 / UR E26 Rev.1）

June 2026

ClassNK Machinery Department

Agenda

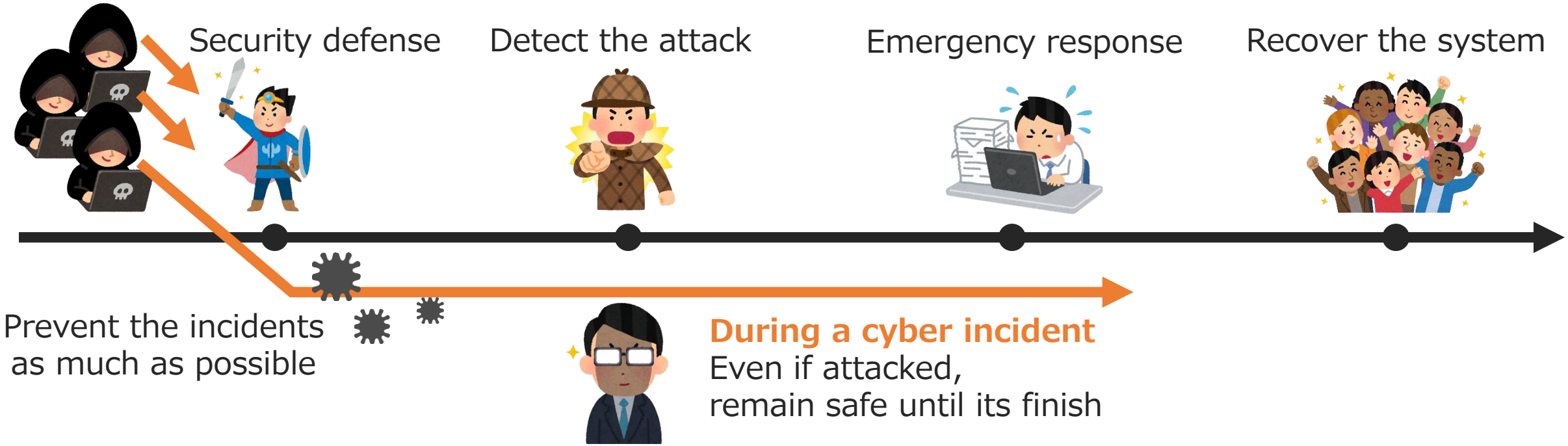
0. Introduction
1. Overview of IACS UR E26
2. Scope of Application
3. Process for Compliance
4. Documents to be Submitted
5. Inspection at Shipyard
6. Summary and attentions

What is Cyber Resilience?

The capability to reduce the occurrence of **cyber incidents** and to mitigate the effects of incidents disrupting or impairing the operational technology (OT) used for the safe operation of the ship.

Cyber Security: Focuses on preventing cyber-attacks.

Cyber Resilience: Ensures the **ability to recover ("resilience")** when attacks cannot be prevented.



0. Introduction

For details on each requirement, please also refer to the guidelines and FAQ.

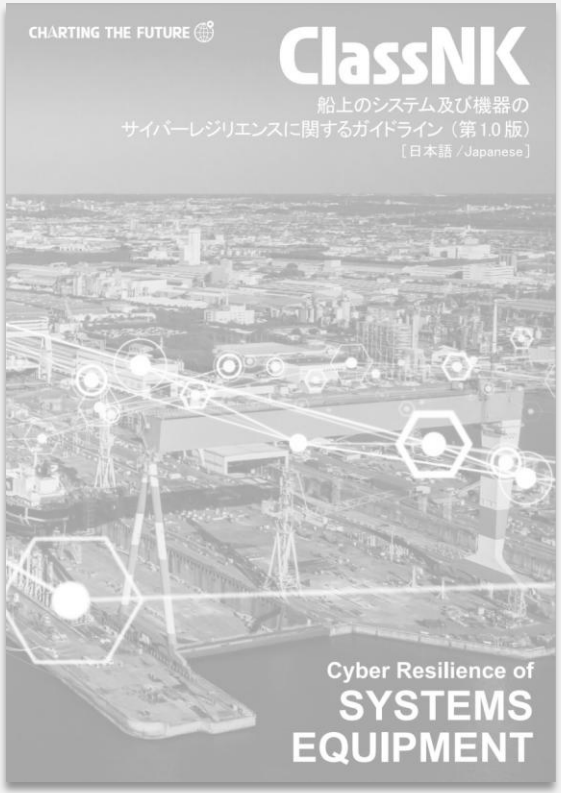
Guidelines for Cyber resilience of on-board systems and equipment

Part X, Chapter 4

Target: Manufacturers

Contents: Application
Approval process
Requirements
Documents
Witnessed test
Type Approval

etc.



Guidelines for Cyber Resilience of Ships

Part X, Chapter 5

Target: **Shipyard**
Shipowner

Contents: Application
Network configuration
Requirements
Documents
Witnessed test
Omission

etc.

🌐 **Portal page (Guidelines / Movies / FAQ etc.)**
https://www.classnk.or.jp/hp/en/activities/cybersecurity/ur-e26e27.html

ClassNK

Suppliers, Systems Integrators, and Shipowners have roles at each stage

IACS UR E27 (Rev.1)

Cyber resilience of onboard systems and equipment

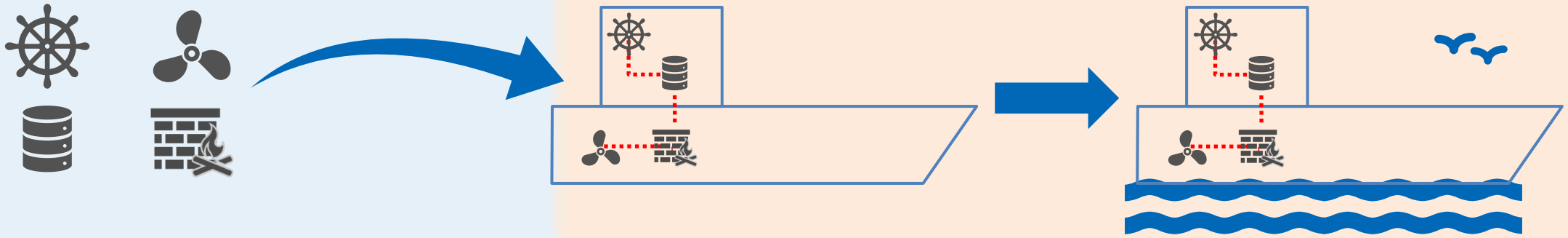
Manufacturers (Suppliers)
supply products considered cyber resilience

IACS UR E26 (Rev.1)

Cyber resilience of ships

Shipyards (integrators)
build cyber resilient ships

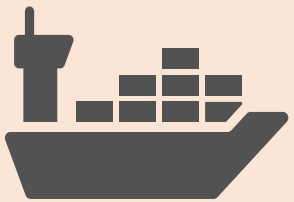
Shipowners
maintain cyber resilience in operation



Requirements for achieving ships with cyber resilience

Part X, Chapter 5 (IACS UR E26)

Cyber Resilience of Ship



Identify

To **"visualize"** and manage assets such as on-board systems and network equipment

Protect

To **minimize the scale and frequency** of potential cyber incidents

Detect

To **identify cyber incidents**

Respond

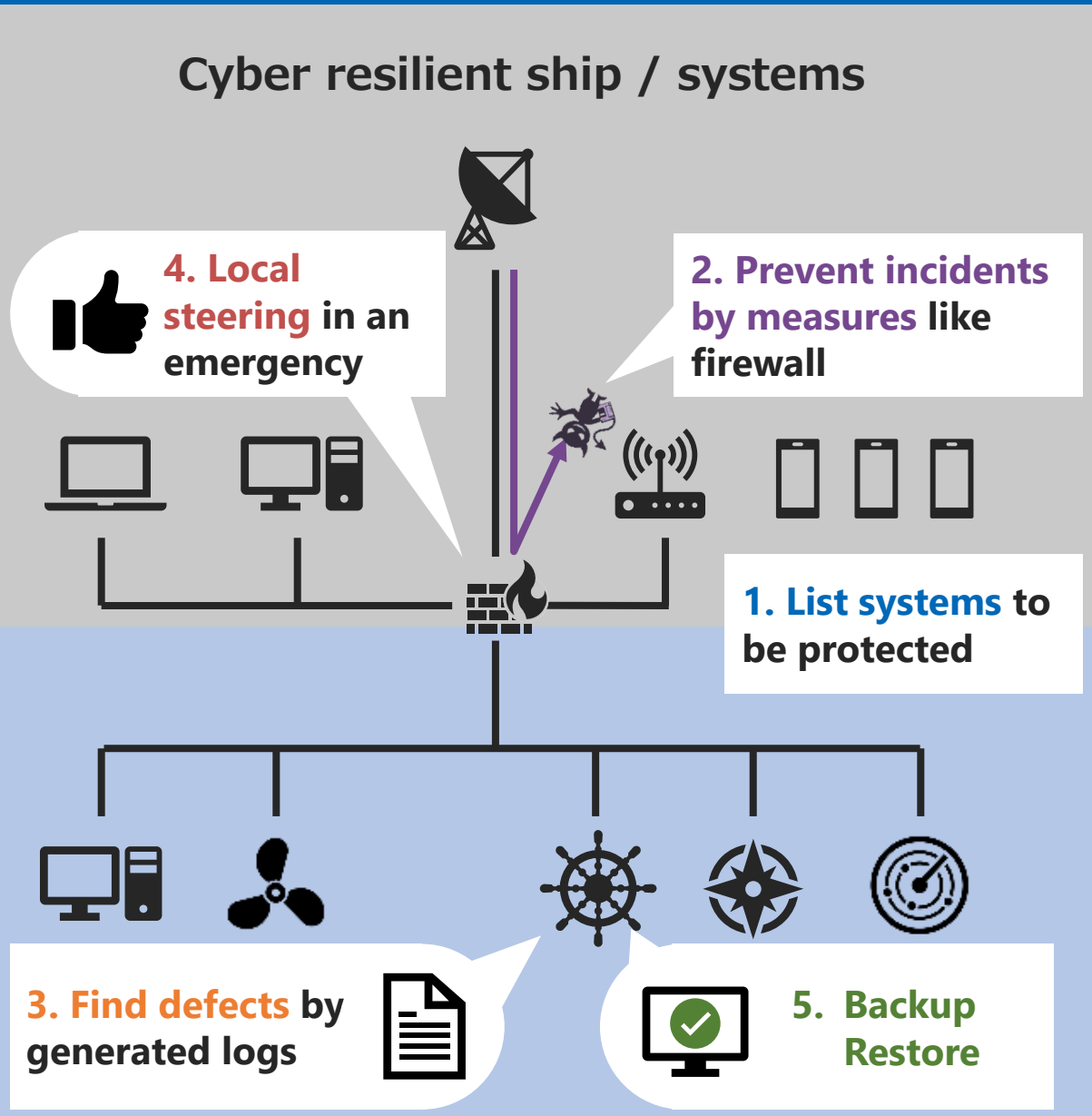
To **establish measures to minimize the impact** when a cyber incident is detected

Recover

To **restore to an operational state** after disruption or failure due to a cyber incident

1. Overview of IACS UR E26

ClassNK



Identify
- List and manage systems to be protected

Protect
- Prevent incidents by measure like firewall

Detect
- Discover anomalies through logs and displays.

Respond
- Isolation in case of emergency
- Switch to Local steering control

Recover
- Restore equipment with backup data

Applicable Ships

The following ships contracted for construction on or after 1 July 2024 are subject to the application

- Passenger ships (incl. high-speed craft) for international voyages
- **Cargo ships of 500 GT and upwards for international voyages**
- High speed craft of 500 GT and upwards for 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)

💡 **Not applicable for**

Non-international vessels and **ships contracted before July 1st, 2024**

Scope ①: Applicable OT Systems

CBSs used for the operation of the following functions and systems on applicable ships:

(CBS = Computer-based system)

- **Propulsion**
- **Steering**
- **Anchoring** and **mooring**
- **Electrical power generation** and **distribution**
- **Fire detection** and **extinguishing systems**
- **Bilge** and **ballast systems, loading computer**
- **Watertight integrity** and **flooding detection**
- **Lighting**

- **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.)
- **Navigational systems** required by statutory regulations
- **Internal and external communication systems** required by class rules and statutory regulations

Scope ①: Applicable OT Systems

Please refer to the guidelines for specific examples

Propulsion

Engine control systems	Engine remote control systems
Main boiler control systems	CPP control systems
Electric propulsion control systems	Fuel supply system control unit (e.g., FGSS control systems)
Machinery alarm and monitoring systems (including data loggers)	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)	Electric power converters (for electric propulsion ship)
Battery management systems (consisting of lithium-ion batteries with total capacities of 20 kWh or more, and associated equipment)	

Fire detection and extinguishing systems

Fire detection and alarm systems	Fixed foam fire extinguishing systems
Fixed CO_2 fire extinguishing systems	Fixed deck foam systems
Fixed local application fire-fighting systems	Water-spraying systems
Dry chemical fire-extinguishing equipment	

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
Reliquefication 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)

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

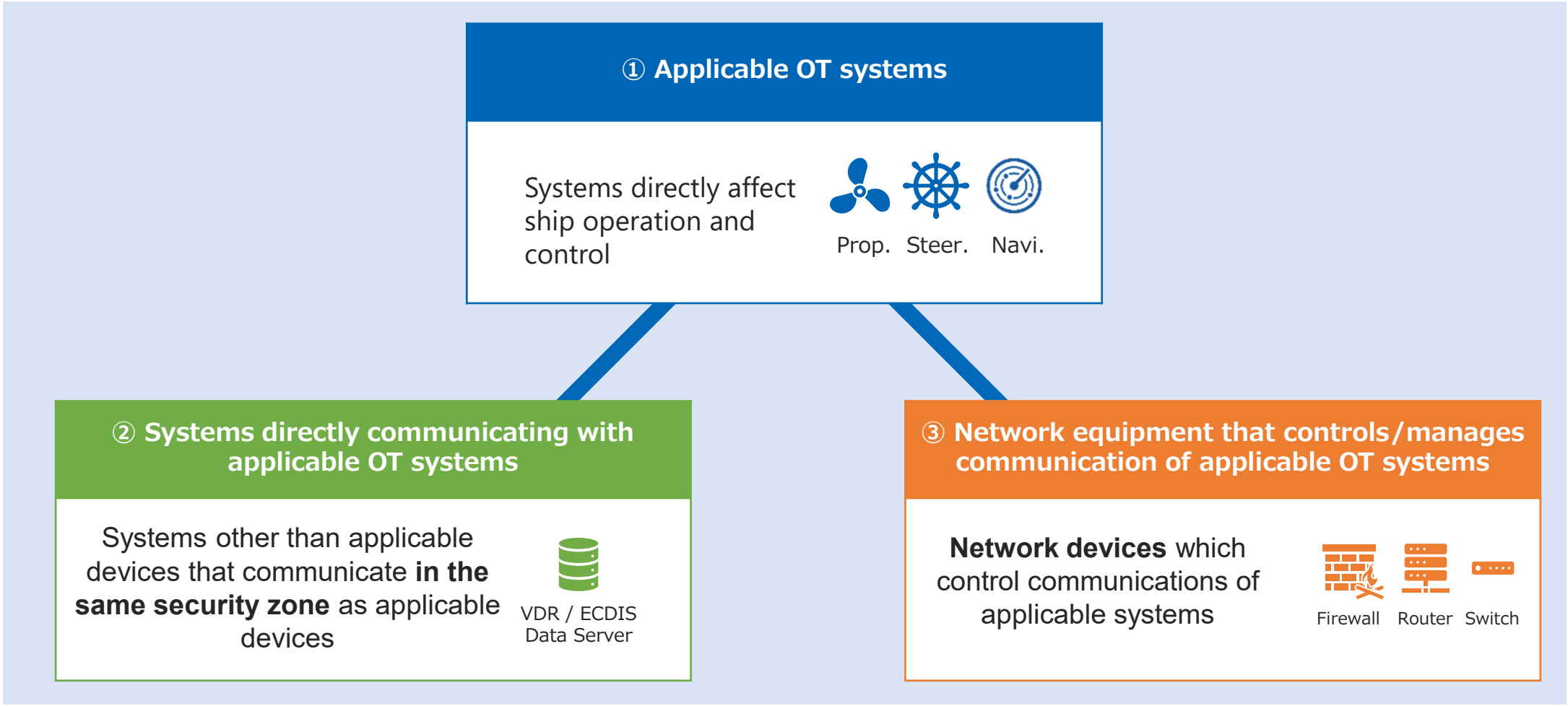
General emergency alarm	Public addressor
NAVTEX receiver	VHF DSC device
EGC receiver	DSC device
VHF DSC continuous watch device	DSC continuous watch device
GMDSS radio installation	

Others

Dynamic positioning systems (DPS)

2. Scope of Application – Applicable Systems/Equipment

Scope ②③: Systems and Network Equipment associated with ① are also in scope



Systems/equipment in categories ①, ②, and ③ above basically require approval under IACS UR E27

Exclusion Case 1: Even systems in Scope ① can be excluded if they meet the exclusion criteria

Mandatory Criteria

(1) System is isolated (no IP-network connections)
(2) No accessible physical interface ports; unused ports logically disabled
(3) Located in physically access-controlled areas
(4) Not an integrated control system serving multiple ship functions in scope

Criteria to be considered

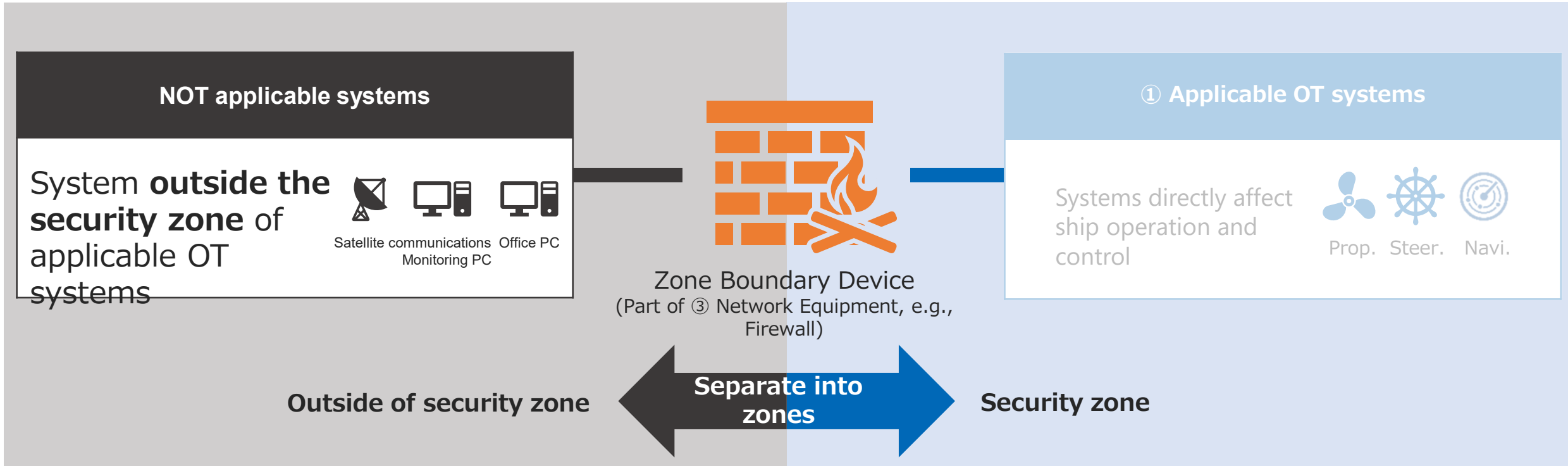
(1) Should not serve Category III functions
(2) Known vulnerabilities, threats, and impacts are duly considered in the risk assessment
(3) Attack surface is minimized

(Even if not fully satisfied, it may be accepted if the NK finds it acceptable.)

💡 The exclusion must be justified by the shipyard in the "Risk assessment for exclusion of computer-based system" document and approved by NK.

Exclusion Case 2: Systems not directly communicating with Scope ① systems are out of scope

Either no communication path is provided, or zones are separated by controlling/managing communication with a zone boundary device.



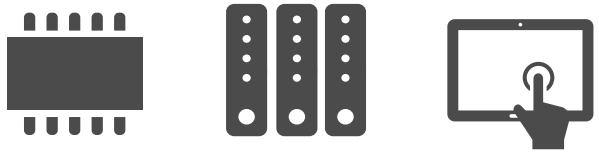
Exclusion Case 3: Systems that do not use computers are out of scope

What is a CBS under the rules?

A programmable electronic device, or an interoperable set of programmable electronic devices, organized to achieve one or more specified purposes such as collection, processing, maintenance, use, sharing, dissemination, or disposition of information

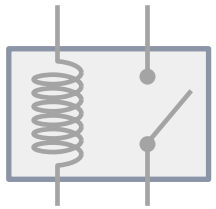
Applicable

Including systems using microcomputers, PLCs, embedded PCs, etc.

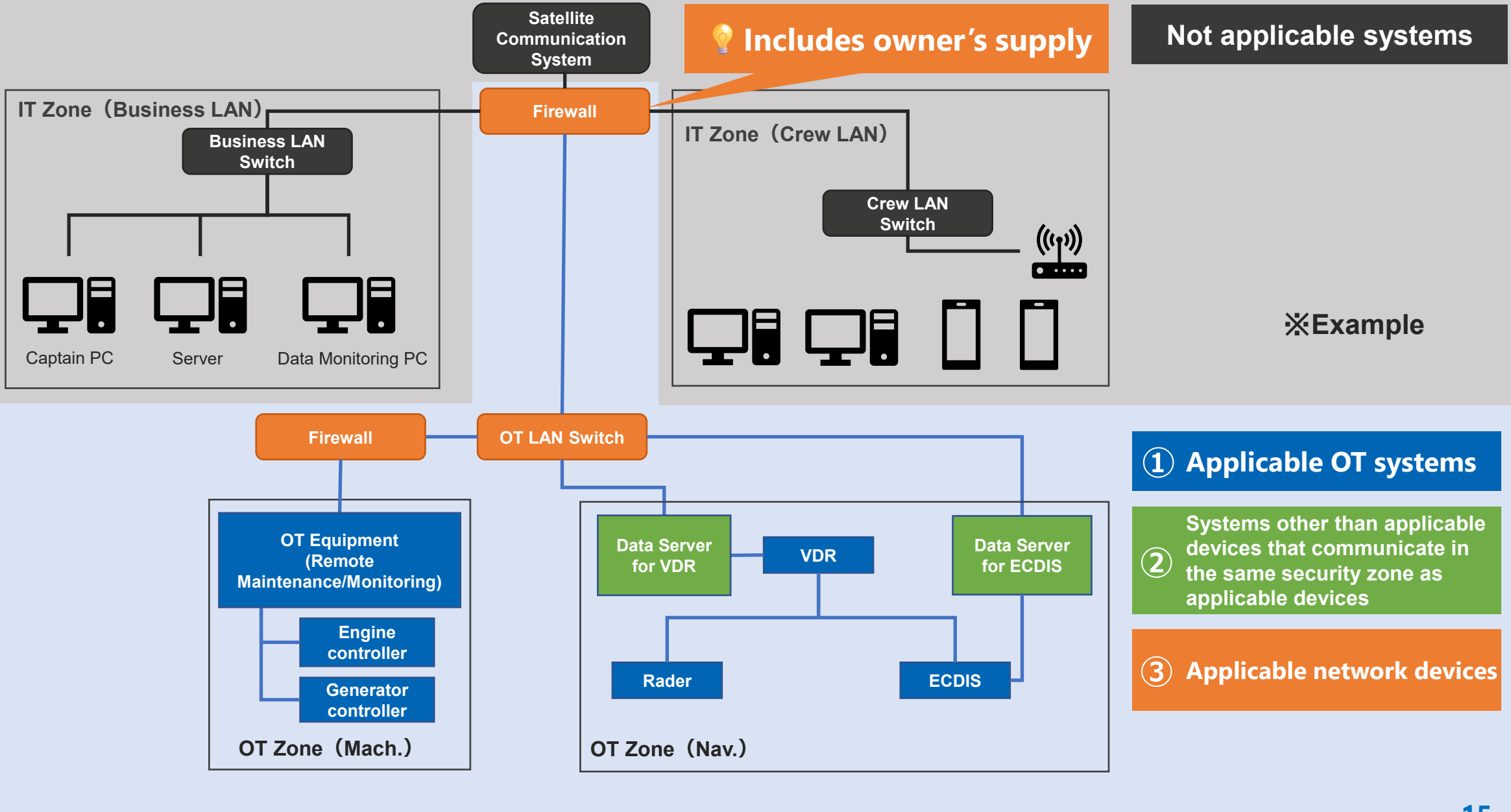


Not applicable

Relay sequence systems, etc.



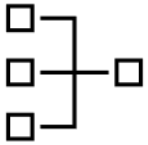
1. Scope of Application – Applicable Systems/Equipment



Design Phase

Commissioning Phase

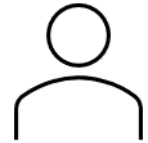
Identify CBSs in scope → **Design security functions of ships** → **Update design as needed** → **Survey**



Design ship's network and **make documents to identify CBSs in scope**

Prepare documents related to **security capabilities and design** based on supplier's documents

Update the documents in steps ① and ② **Submit the Test Procedure** to NK.



Conduct **witnessed survey** in accordance with "Ship Cyber Resilience Test Procedure".

Document submit to NK

"Vessel Asset Inventory"
"Zone and Conduit Diagram"
"Risk Assessment for the Exclusion of Computer-based Systems"

Document submit to NK

"Cybersecurity Design Description"
"Description of Compensating Countermeasures"

Document submit to NK

"Ship Cyber Resilience Test Procedure"

Documents to be submitted from the shipyard

- Ship asset inventory
- Zones and Conduit Diagram
- Cyber Security Design Description
- Risk assessment for exclusion of computer-based systems
- Description of compensating countermeasures
- Ship cyber resilience test procedure

Vessel Asset Inventory

Outline List of CBSs, network equipment, etc. installed on the ship

System	Detailed Machinery / Systems	Security Zone	Location	Hardware Component			Software Component		Updated Log
				Name	Model/Type	・・・	Model/Type	・・・	
Main propulsion	RCS	Machinery Zone	W/H	W/H HMI	・・・	・・・	・・・	・・・	2024.x.x
			C/R	C/R HMI	・・・	・・・	・・・	・・・	2024.x.x
Main propulsion	AMS	Machinery Zone	C/R	Main computer	・・・	・・・	・・・	・・・	2024.x.x
			W/H Accommodations	Extension panel	・・・	・・・	・・・	・・・	2024.x.x
Navigation	ECDIS	Navigation Zone	W/H	HMI	・・・	・・・	・・・	・・・	2024.x.x
			W/H	Main unit	・・・	・・・	・・・	・・・	2024.x.x

These are the same as the information included in the CBS asset inventory created by suppliers.

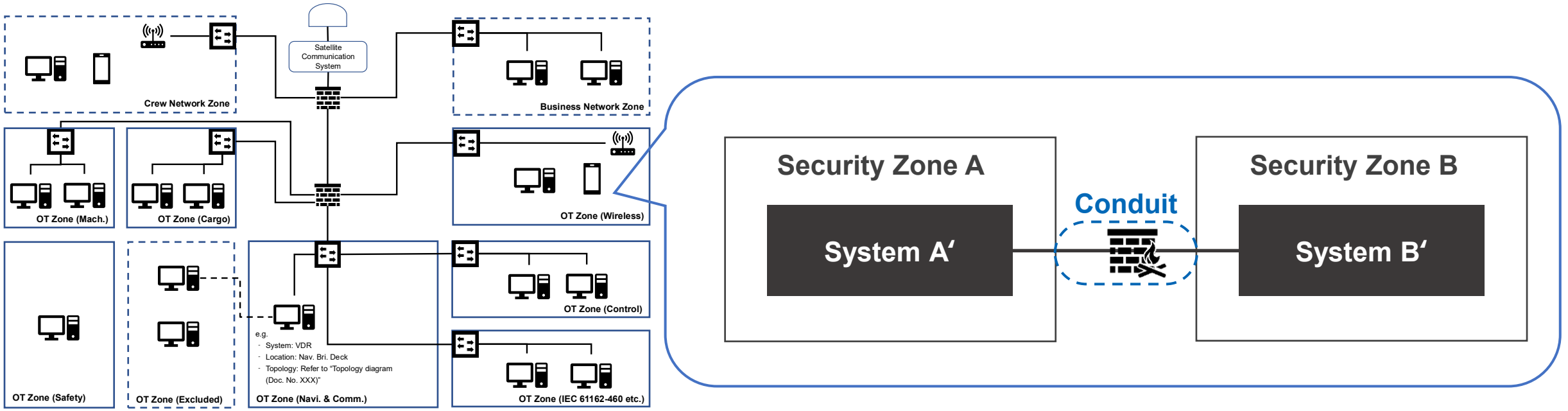
- Describe all applicable CBSs. **Shipowner supplies** (data servers, etc.), are to be included.
- Submit it at an **early stage**.
- If unclear at the design phase, indicate as "TBD / To Be Determined" and submit to NK. At the last, it is to be completely updated before the survey at the commissioning phase.

Zones and Conduit Diagram

Outline Diagrams indicate network configuration onboard including relation of

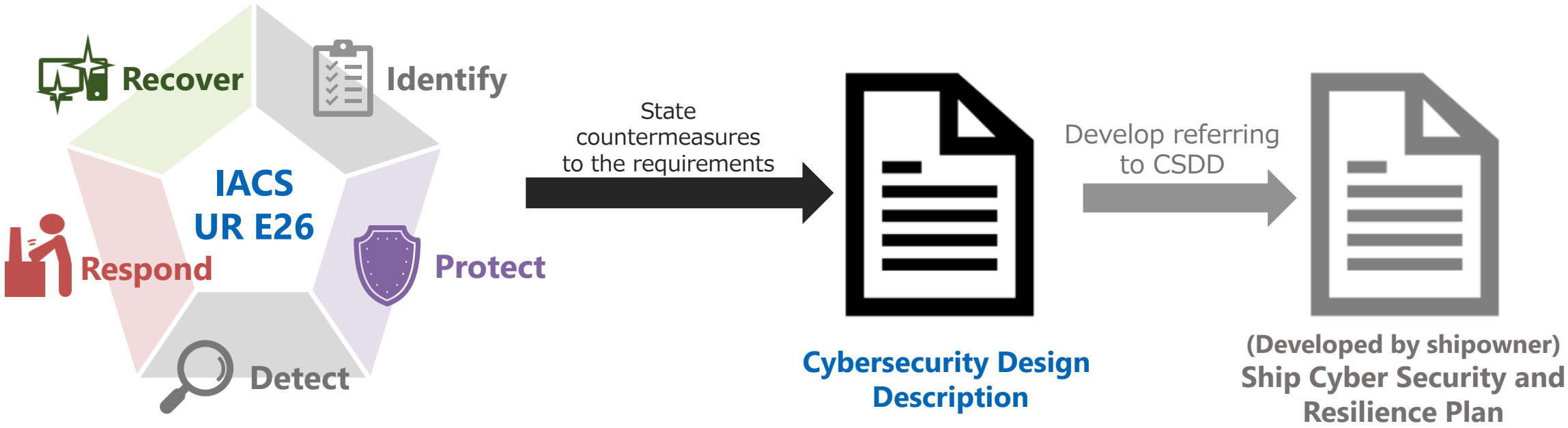
Security zones: areas which have same security levels

Conduits: communication between zones



Cybersecurity Design Description

Outline Document of countermeasures for Protect, Respond and Recover requirements



✓ Help Shipowners to prepare “Ship Cyber Security and Resilience Program”

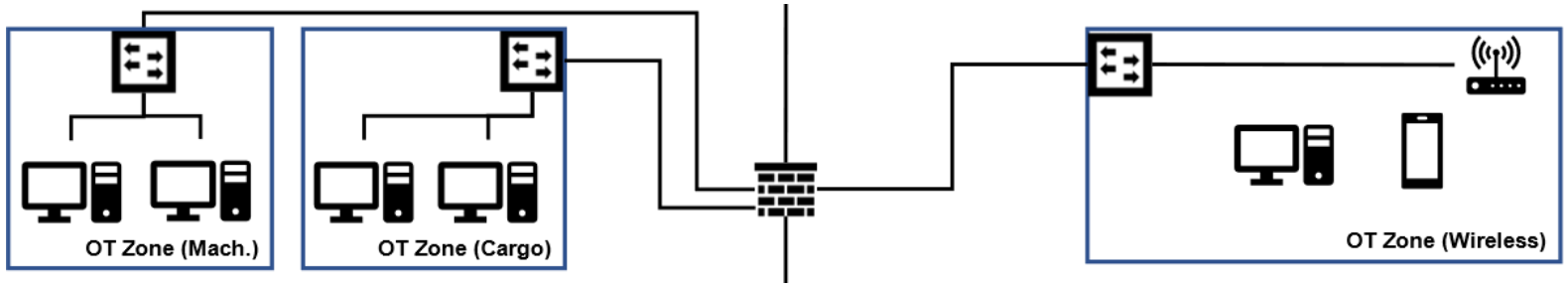
Cyber Security Design Description

Outline Document of countermeasures for Protect, Respond and Recover requirements to help Shipowners to prepare “Ship Cyber Security and Resilience Program”

e.g., **UR E26 4.2.1 - Protect “Security zones and network segmentation”**

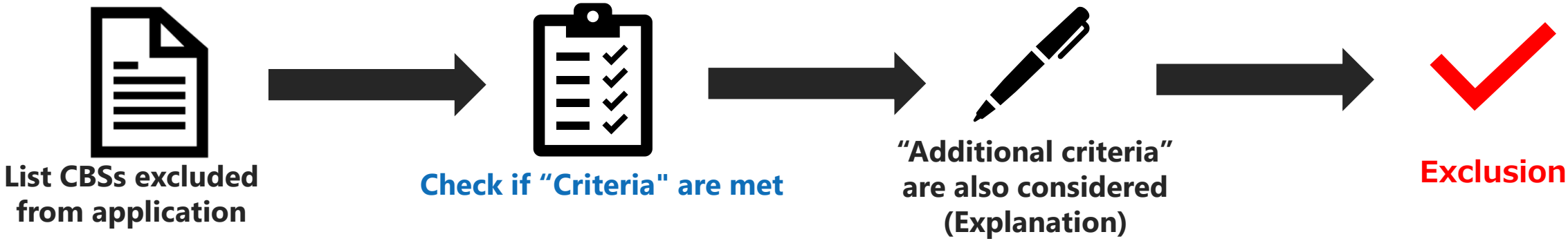
Cybersecurity Design Description

- Specify the names, uses, and purposes of the CBS included in each security zone
- Identify network communications within the same security zone
  ⇒ Purpose of communication, communication protocol, and data flow
- Identify network communications between the different security zone
  ⇒ What traffic is allowed by a zone border device, such as a firewall



Risk Assessment for the Exclusion of Computer-based Systems

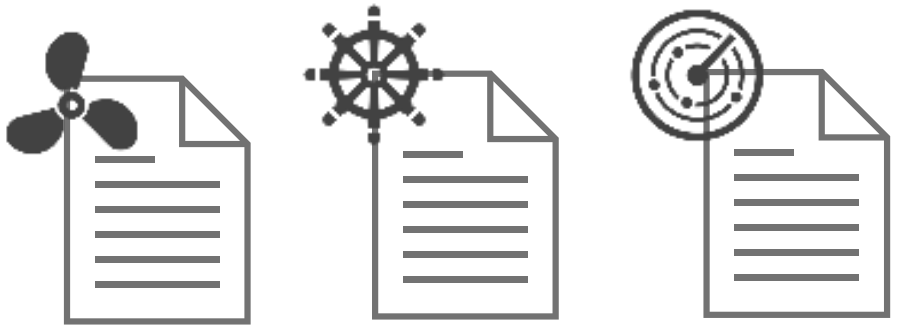
Outline Document proving that the security risk of the excluded CBSs is sufficiently low



- ✓ If explanation is deemed appropriate by NK, no need to fully met for “Additional criteria”
- ✓ The shipyard can do risk assessment ship-by-ship (It is only for CBSs to exclude)

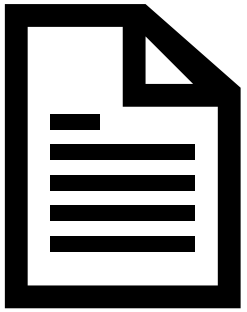
Description of Compensating Countermeasures

Outline Summary of the requirements met by Compensating Countermeasures



Description of Security Capabilities for each CBS (UR E27)

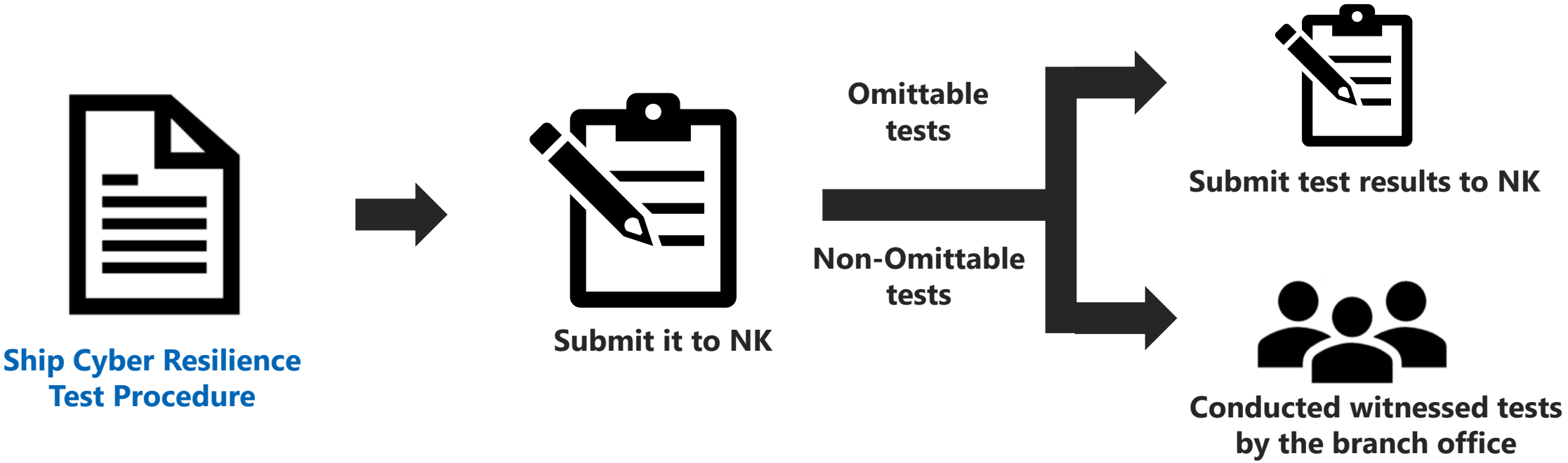
Compile compensating countermeasures



Description of Compensating Countermeasures

- Identify CBSs that **meet security requirements by Compensating Countermeasures**.
- Describe the **missing security functions** and **their Compensating Countermeasures.**
- **Reference to "Description of Security Capabilities"** as necessary

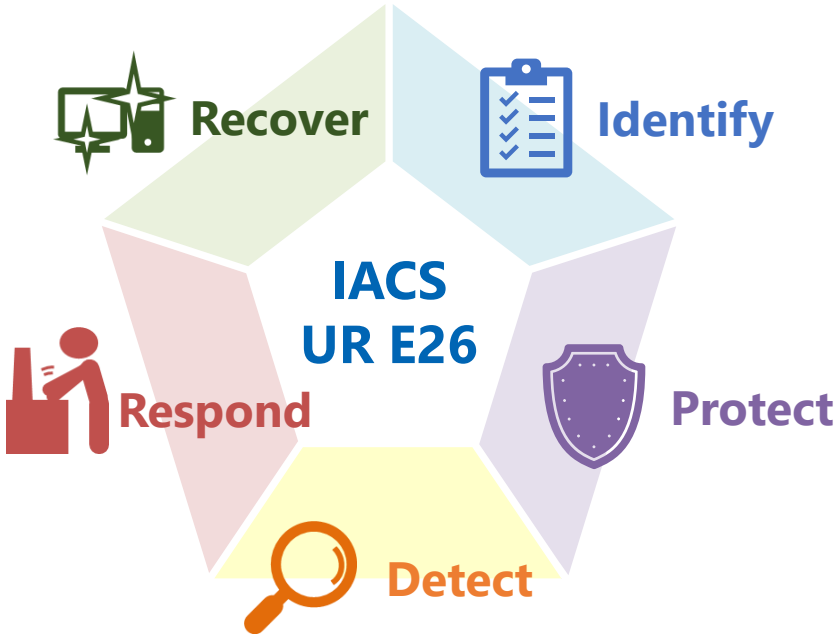
Survey process



- Some requirements **may be omitted** depending on the test results of the security function test in accordance with UR E27.
- **Non-omittable tests, not conducted in UR E27** must be conducted.
- All those tests are to be included in this document

Ship Cyber Resilience Test Procedure

Outline Test plan for verifying security function of network and each CBSs



・Compile test plans of CBSs
・Add network related items

Ship Cyber Resilience Test Procedure

- **Concrete descriptions** of test items, test procedures, criteria
- Used in the witnessed tests conducted by shipyards (in construction) and shipowner (in special surveys)

Ship Cyber Resilience Test Procedure

Outline Test plan for verifying security function of network and each CBSs

e.g., **UR E26 4.2.2 - Protect “Network protection safeguards”**

Ship Cyber Resilience Test Procedure

Test procedures for the following are described

- Denial of Service (DoS) to zone boundary protection devices
- Denial of Service (DoS) from inside each network segment
- Analytic evaluation / port scanning that unnecessary functions, ports, protocols, services in the CBSs have been removed

Zone boundary protection devices	Devices forming zone boundary defined in UR E26
Denial of Service (DoS)	Interruption of device functions by submitting enormous data

Ship Cyber Resilience Test Procedure

Outline Test plan for verifying security function of network and each CBSs

e.g., **UR E26 4.3.1 - Detect “Network operation monitoring”**

Ship Cyber Resilience Test Procedure

Test procedures for the following are described

- Network disconnections will activate alarm and that the event is recorded
- Excessive network traffic is detected, and that alarm and record is generated
- The CBS will respond in a safe manner to network storm scenarios
- Generation of audit records
- IDS is passive and will not affect intended operation of the CBSs (if applicable)

Please be attention on the following

- Scope will be determined based on **network configuration**
- Please submit the following **in early stage** (**TBD items** are acceptable)
  - Vessel asset inventory
  - Zones and conduit diagram
  - Risk Assessment for the Exclusion of Computer-based Systems
- **Shipowners supply items** are to be included
- **Ship cyber security and resilience program** related contents are to be included
- The documents are to be **handed to shipowners**.
- **NK Witnessed tests are necessary** based on the test procedures