

Cybersecurity in Smart Ship

2024.11.12

Korean Register

Park Kaemyoung

(kaemyoung@krs.co.kr)

Contents

- I. The Concept of Smart Ship
- II. International trends in maritime cybersecurity
- III. Cybersecurity in Smart Ship

I. The Concept of Smart Ship

I. Concept of Smart Ship

i Definition of Smart Ship

- A next-generation digital ship that enables autonomous operation, economic operation, and safe operation by applying cutting-edge information technology to ships built based on information and communication technology (ICT).
- Smart vessel that utilizes information and communication technology (ICT) to operate easily and safely at minimum cost

i Concept of Smart Ship

- Vessel capable of monitoring in-ship/exterior information and operation information
- Vessels capable of safe cargo transport and tracking
- Vessels that are easy to repair and maintain -> Ships that can be operated economically
- Vessels that can be controlled and controlled remotely (on land) while satisfying tightened environmental regulations
- (Future-Final Goal) Future ships capable of autonomous operation



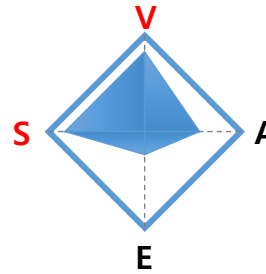
I. Concept of Smart Ship

Development of Smart Ship



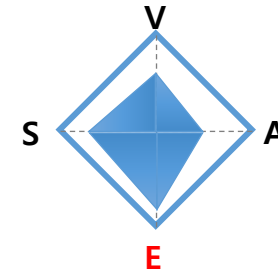
Ref. : ISTOCK

Conventional Ship
(~ Early 2000)



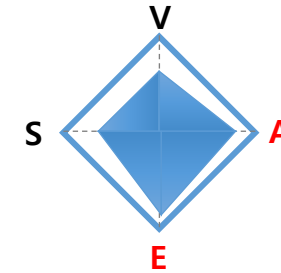
Ref. : Japan Marine United Corporation

Eco Ship
(2012~2017)



Ref. : DNVGL

Smart Ship
(2017~2030)

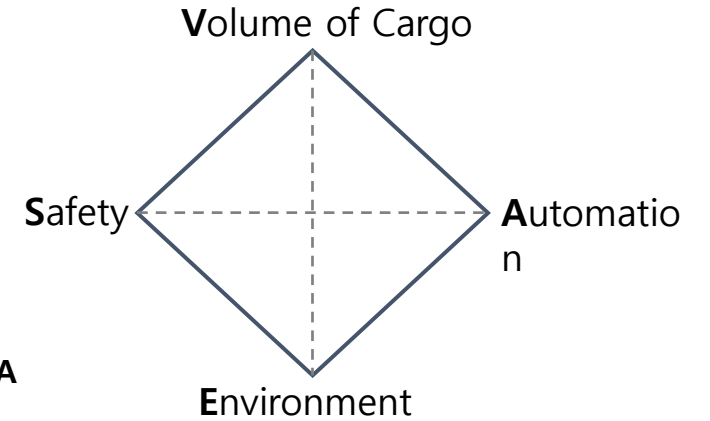
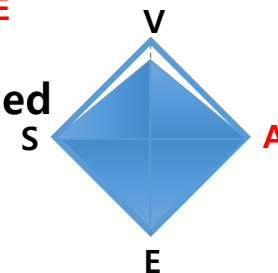


Information & Communication Technology to the ship



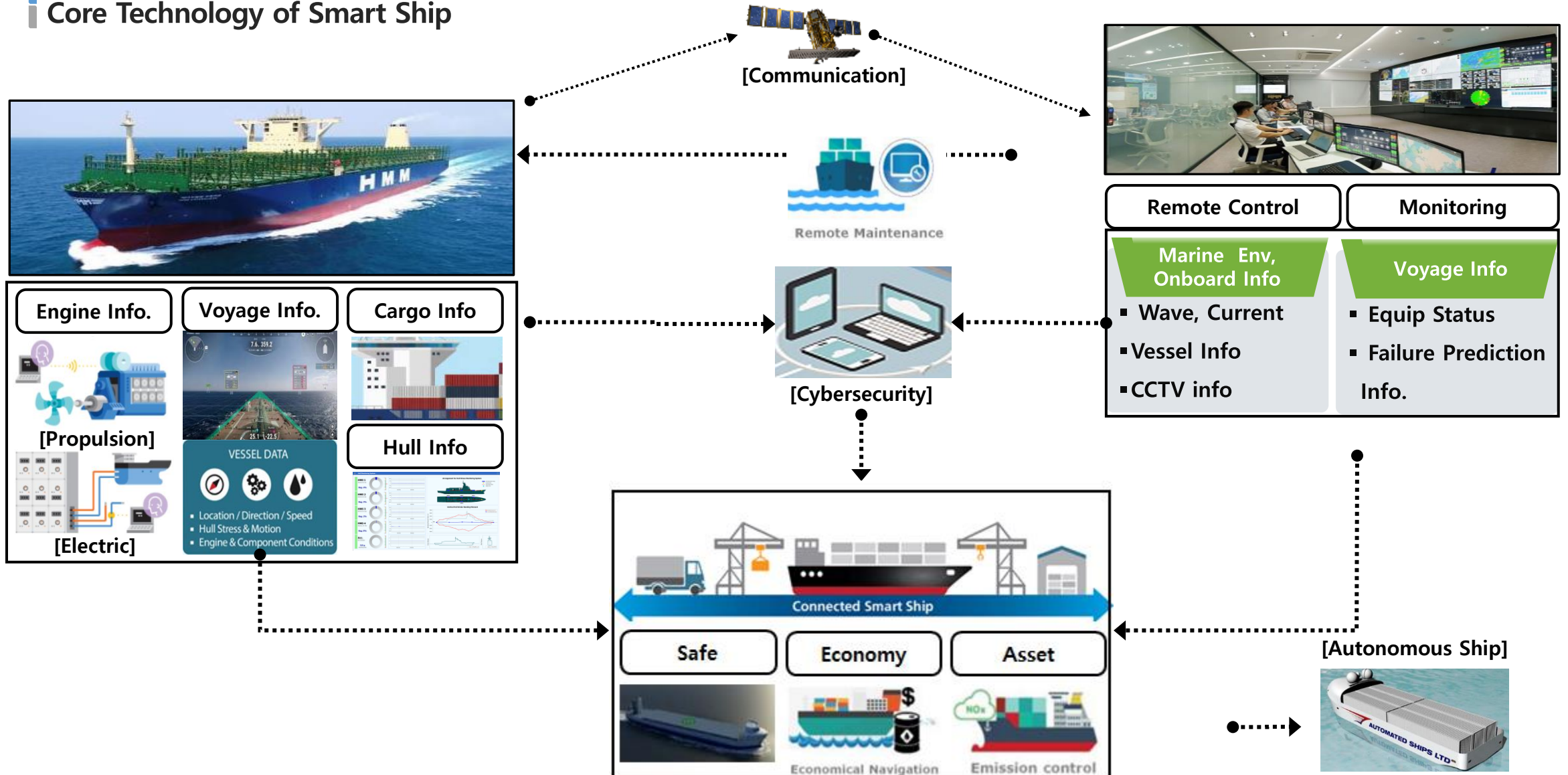
Ref. : Rolls-Royce

Unmanned Ship
(2030~)



I. Concept of Smart Ship

Core Technology of Smart Ship



I. Concept of Smart Ship

Future of Smart Ship

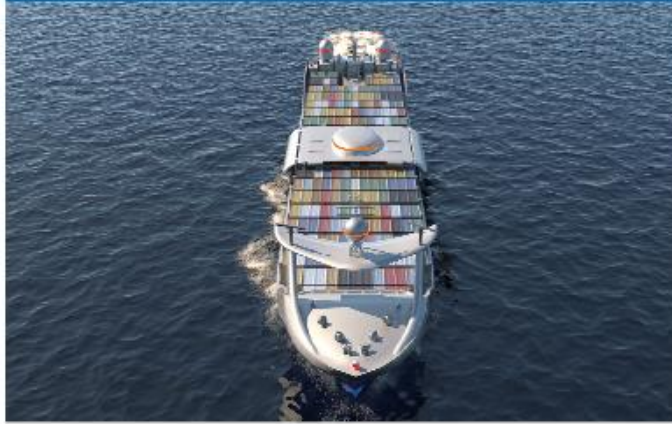
Smart Ship



Comprehensive technology that applies advanced equipment and ICT to ships of meaning




Partial Autonomous Ship



Integrating IOT, platform, and control technology into existing ships The system replaces the role the crew was playing Vessels that can be operated with only minimum crew








Fully Autonomous Ship



Fully autonomous operation that can be operated without human intervention Ship

I. Concept of Smart Ship

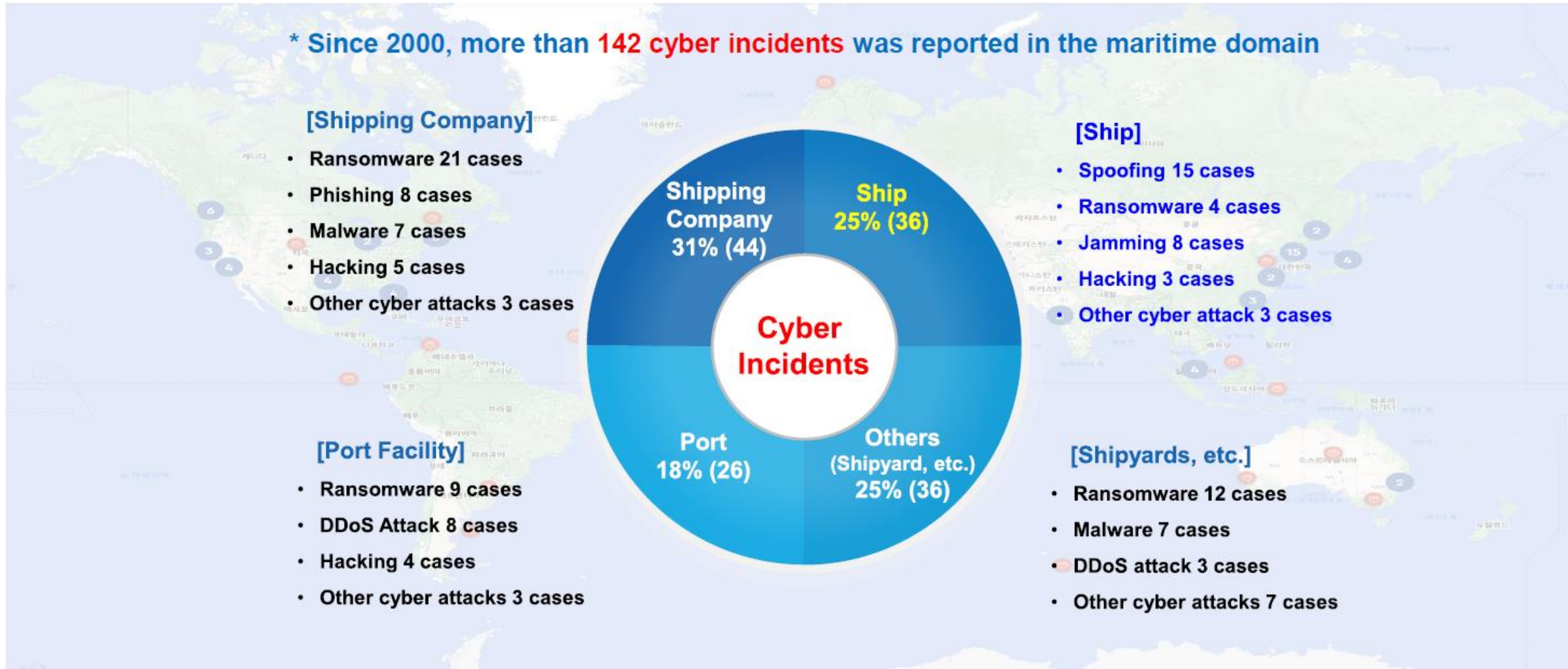
Smart Ship from Class

ABS [Guidance]	DNV [Guideline]	ClassNK [Guideline]	Korean Register [Guidance]
Smart Functions for Marine Vessels and Offshore Units (3 rd Edit 2020)	Smart ship – descriptive notation (DNVGL-CG-0508, 2018)	Digital Smart Ships (1 st Edit 2020)	Guidance for Smart System (2024)
 GUIDE FOR SMART FUNCTIONS FOR MARINE VESSELS AND OFFSHORE UNITS JULY 2020	 CLASS GUIDELINE DNVGL-CG-0508 Edition November 2018 Smartship – descriptive notation	August 2020  Guidelines for Digital Smart Ships [First Edition] [English] 	 2024 Guidance for Smart Systems
SMART(XX, YY, etc,)	Smartship(XX, YY, etc,)	DSS(XX, YY, etc,)	Smart(XX, YY, etc)

II. International trends in maritime cybersecurity

II. International trends in maritime cybersecurity

Analysis for cyber incidents in maritime domain



II. International trends in maritime cybersecurity

Since 2017, International regulations on ship cyber security have been strengthened

1. IMO and Administrations



2017 MSC-FAL.1/Circ.3 - GUIDELINES ON MARITIME CYBER RISK MANAGEMENT.

* Include UR E26 rev.1 and E27 Rev.1 at MSC 108

2017 Res. MSC.428(98)* - MARITIME CYBER RISK MANAGEMENT IN SAFETY MANAGEMENT SYSTEMS.

* Mandatory for more than 24 flag states (USCG, Marshall Island, Singapore, Australia, Cyprus, Vanuatu, etc.)



2020 USCG CVC-WI-027(1) - Vessel Cyber Risk Management Work Instruction

3. Shippers Association



2017 TMSA 3 13 Maritime Security 1.2, 2.3, 2.4, 3.2 and 4.5

2018 SIRE VIQ 7 7 Cyber Security 7.14, 15, 16 and 17

2022 SIRE 2.0 7.5 Cyber Security



2017 Inspection and Assessment Report for Dry Cargo Ships / 4.7 Cybersecurity

2021 Inspection Ship Questionnaire (RISQ) / 12 Security 12.2, 12.7 and 12.8

2. Shipping Association



2016 Guidelines on Cyber Security Onboard Ships

2020 4th Version of Guidelines on Cyber Security Onboard Ships



2019 Implementation Guide for Cyber Security on Vessels v1.0.

4. Classification Societies



2020 Rec.166 – Recommendation on Cyber Resilience

2020 Rec.171 - Recommendation on incorporating cyber risk management into Safety Management Systems

2022 UR E26 – Cyber Resilience of Ships

UR E27 – Cyber Resilience of on-board systems and equipment

2023 UR E26 Rev.1 & E27 Rev.1 : Mandatory for SOLAS ships contracted for construction on and after 1 July 2024

II. International trends in maritime cybersecurity

IMO : International Maritime Organization 

MSC-FAL1/Circ.3 – Guidelines on Maritime Cyber Risk Management

- Urgent need to raise awareness on cyber risk threats and vulnerabilities
- **High-level recommendations on maritime cyber risk management** to safeguard shipping from current and emerging cyber threats and vulnerabilities
- **Five Functional elements** that support effective cyber risk management.

Resolution 428(98)

The resolution encourages administrations to ensure that cyber risks are appropriately addressed in existing **safety management systems (as defined in the ISM Code)** no later than the first annual verification of the company's Document of Compliance **after 1 January 2021**.

IMO continues to express interest in cyber risk management for ships. Currently, resolution MSC.428(98) is recommended as non-mandatory by each flag state, but it is highly likely that it will develop into a mandatory requirement in the future. Currently, it is a mandatory requirement in the United States, Marshall Island, Singapore, Australia, Cyprus, and Vanuatu.

II. International trends in maritime cybersecurity

IMO : International Maritime Organization 

(Goal) To support safe and secure shipping, which is operationally resilient to cyber risks

Identification

- Define personnel roles and responsibilities for cyber risk management and identify the systems, assets, data and capabilities that, when disrupted, pose risks to ship operations

Protect

- Implement risk control processes and measures, and contingency planning to protect against a cyber-event and ensure continuity of shipping operations

Detect

- Develop and implement activities necessary to detect a cyber-event in a timely manner

Respond

- Develop and implement activities and plans to provide resilience and to restore systems necessary for shipping operations or services impaired due to a cyber-event

Recover

- Identify measures to back-up and restore cyber systems necessary for shipping operations impacted by a cyber-event

II. International trends in maritime cybersecurity

IACS Requirements for cyber resilience

- IACS Unified Requirements (URs)

- UR E26 rev.1: Cyber Resilience of Ships
- UR E27 rev.1: Cyber Resilience of Systems

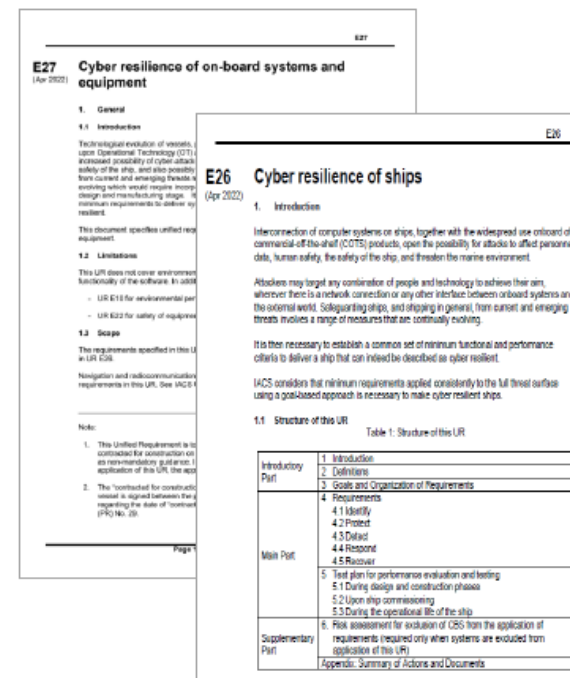
- Applied ships

- Cargo ships of 500GT and upwards engaged in international voyages, which contracts for **newbuilding on or after 1 July 2024**

- Organization of URs and stakeholders

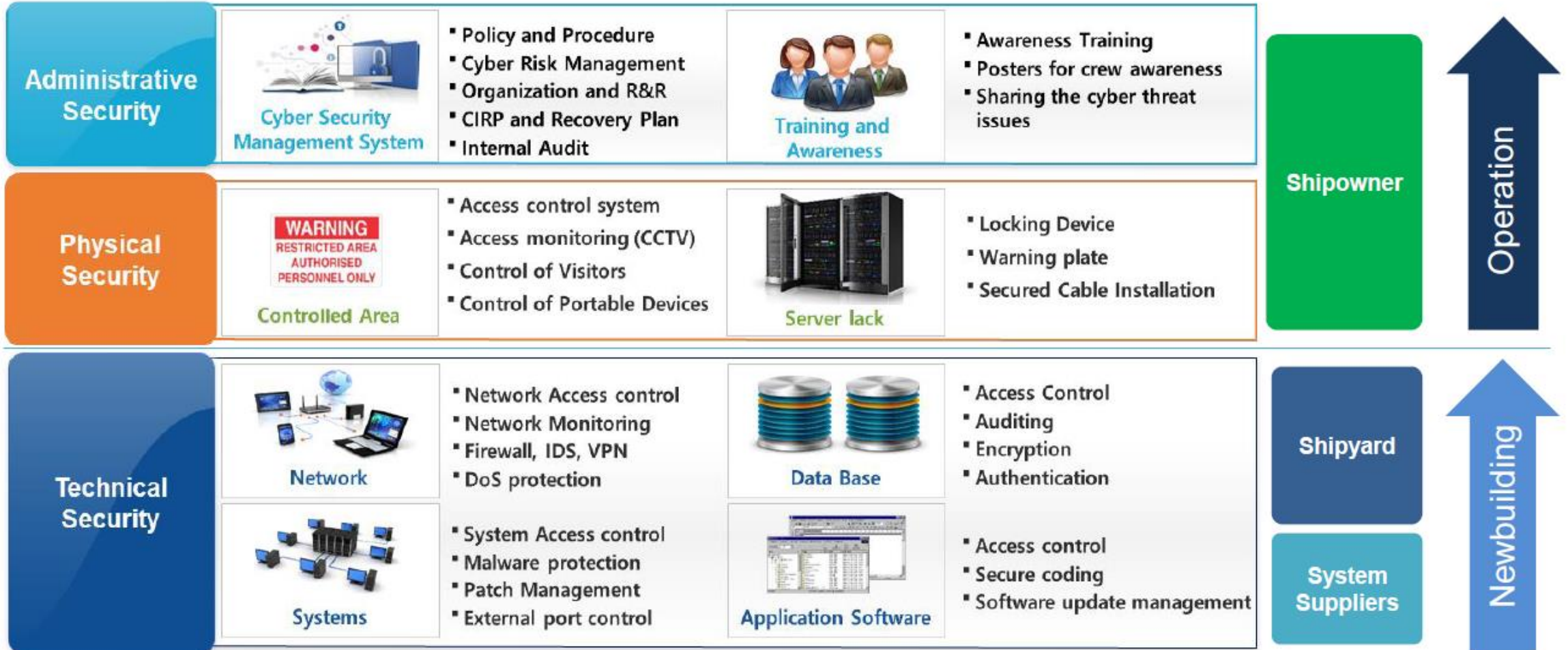
UR	Requirements	Phase	Stakeholder
UR E27 rev.1	Cyber security functions for systems	Newbuilding	Suppliers
UR E26 rev.1	Design, integration and testing for cyber resilience of ships	Newbuilding	Shipyards*
UR E26 rev.1	Management and operation of cyber resilience of ships	Operation	Shipowner

* Shipyards may delegate the role of cyber resilience design, integration, and testing to external systems integrators.



II. International trends in maritime cybersecurity

Concept of Implementation on Ship Cyber Resilience



II. International trends in maritime cybersecurity

Framework of Cyber Resilience of Ships



Identify (4.1)	<ul style="list-style-type: none"> Inventory of CBSs and networks onboard 	Document
Protect (4.2)	<ul style="list-style-type: none"> Security zone Network protection safeguards Antivirus, antimalware, antispam and other protections from malicious code Access control Wireless communication Remote access control and communication with untrusted networks Use of Mobile and Portable Devices 	Network design and item configuration
Detect (4.3)	<ul style="list-style-type: none"> Network operation monitoring Diagnostic functions of CBS and networks 	Install solution (NMS & SIEM)
Respond (4.4)	<ul style="list-style-type: none"> Incident response plan Local, independent and/or manual operation Network isolation Fallback to a minimal risk condition 	
Recovery (4.5)	<ul style="list-style-type: none"> Recovery plan Backup and restore capability Controlled shutdown, reset, roll-back and restart 	Document, set up system configuration

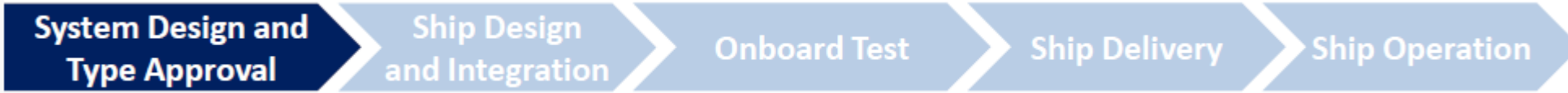
II. International trends in maritime cybersecurity

UR E26 rev.1 : Cyber Resilience of Ships

No.	Document (E26)	Systems integrator			Shipowner			
		Design	Construction	Commissioning	Operation	1 st AS	AS	SS
1	Approved supplier documentation		Maintain	Maintain	Maintain			
2	Zones and conduit diagram	Submit	Maintain	Maintain	Maintain			
3	Cyber security design description	Submit	Maintain	Maintain	Maintain			
4	Vessel asset inventory	Submit	Maintain	Maintain	Maintain			
5	Risk assessment for the exclusion of CBSs	Submit	Maintain	Maintain	Maintain			
6	Description of compensating countermeasures	Submit	Maintain	Maintain	Maintain			
7	Ship cyber resilience test procedure		Submit	Demonstrate	Maintain			Demonstrate
8	Ship cyber security and resilience program <ul style="list-style-type: none"> - Management of change (MoC) - Management of software updates - Management of firewalls - Management of malware protection - Management of access control - Management of confidential information - Management of remote access - Management of mobile and portable devices - Detection of security anomalies - Verification of security functions - Incident response plans - Recovery plans 				Maintain	Submit	Demonstrate	

II. Cybersecurity in Smart Ship

III. Cybersecurity in Smart Ship



Type Approval of Security functions for OT* Systems

* OT: Operational Technology

- Security function requirements: IACS UR E27 rev.1 Sec.4
- Implement basic 30 Security functions
 - (e.g.) ID & Password, Malware Protection, Use control for portable devices, System backup, system recovery, etc.
- Implement additional 11 Security functions in case of remote connection use
 - (e.g.) Multifactor Authentication, Limit the number of login attempts, secure communication, etc.



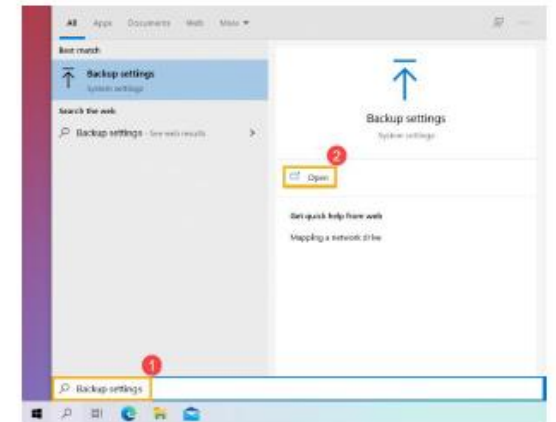
[ID and password authentication]



[Anti-virus program]

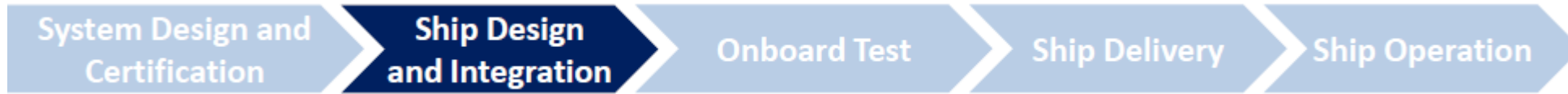


[Installation of USB Port Blocker]




[System backup function]

III. Cybersecurity in Smart Ship



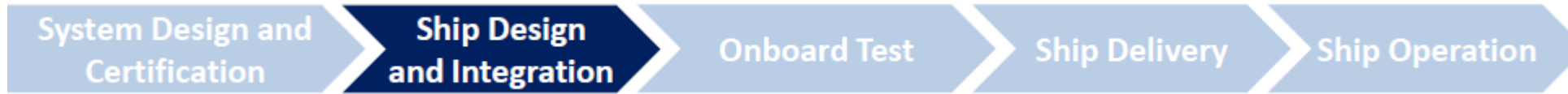
Identify OT systems in the scope (1/3)

- Identify essential OT systems to be managed in the scope of cyber resilience
- Development of Vessel Asset Inventory
 - List of OT systems onboard in the scope
 - Hardware and software information, network devices and security devices(Firewall, IDS, etc)

	Asset List							
	Example asset list which can be populated with a list of critical assets including type (hardware/software), owner (shore), custodian (on vessel) and criticality based on existing impact assessments within the SMS.							
Asset Serial	Asset	Type/Description	Version	Owner	Custodian	Location	Date of Last Check	Criticality
1	Dell Inspiron 17 Laptop	Hardware	Windows 10	J Doe	A Smith	Bridge	01/11/2019	Low
2								
3								
4								
5								
6								
7								
8								
9								
10								

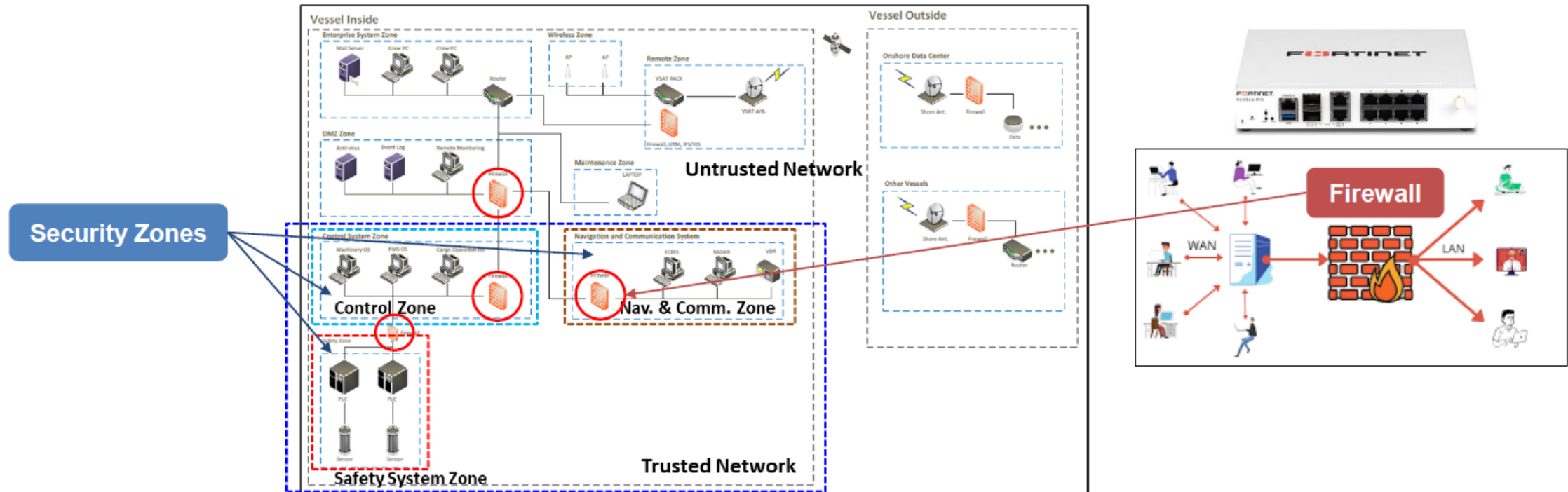
[Example of Vessel Asset Inventory]

III. Cybersecurity in Smart Ship

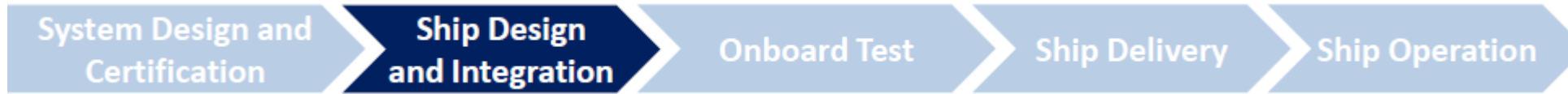


Network Segmentation and Safeguard (2/3)

- Step 1: Define security zones for protection
 - (e.g.) Machinery control system zone, navigation and communication zone, safety zone, DMZ zone, etc.
- Step 2: Network segmentation based on security zones
- Step 3: Implement safeguards such as firewalls and DoS protection

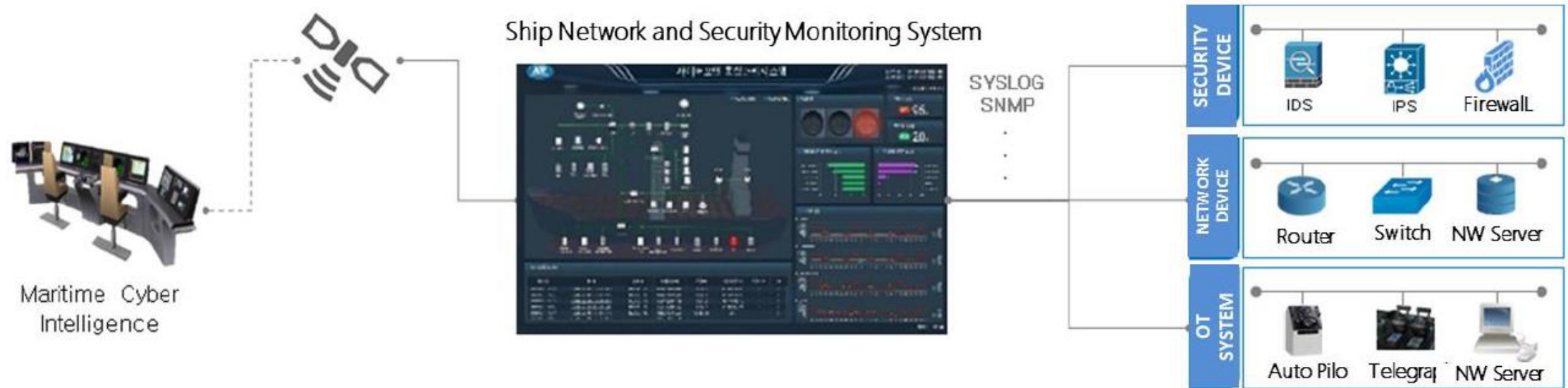


III. Cybersecurity in Smart Ship



Network Monitoring System (3/3)

- Monitor and alarms any malfunction or abnormal condition in network system
- Network system: Firewall, Router, Switch(Managed)

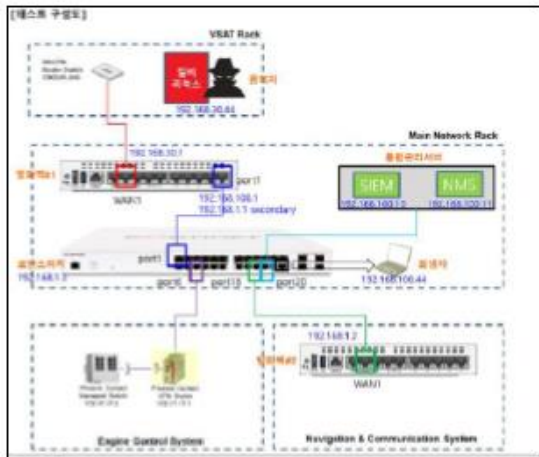


III. Cybersecurity in Smart Ship



Onboard test for cyber resilience

- Carry out onboard test for cyber resilience of ship
- Examples of check points
 - System inspection (Security configuration, SW update status, etc.)
 - Network test (network segregation, network protection, network monitoring, etc)
 - Access control test (Management of ID and Password, remote connection, control of exposed USB ports, etc)



[Test setup]



[On-board test]

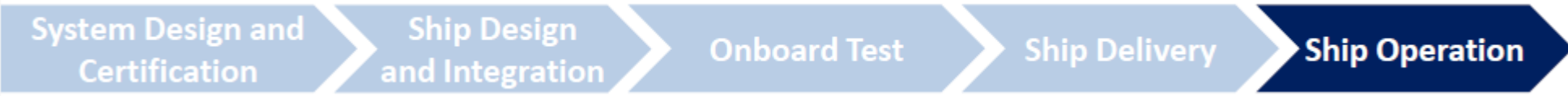


[Test tool(e.g. Kali Linux)]



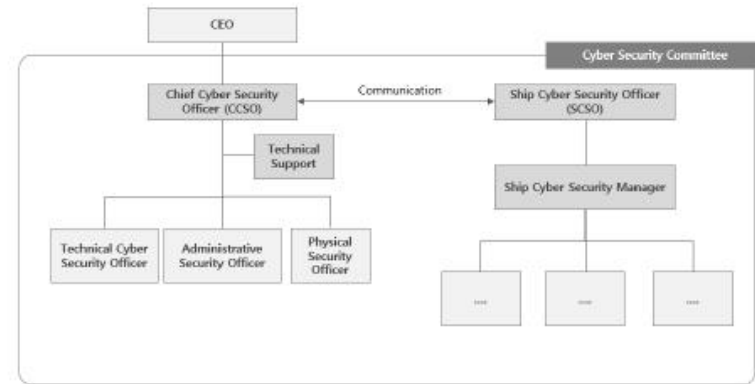
[Network monitoring system]

III. Cybersecurity in Smart Ship



Establishment of Ship Cyber Security Management System (CSMS)

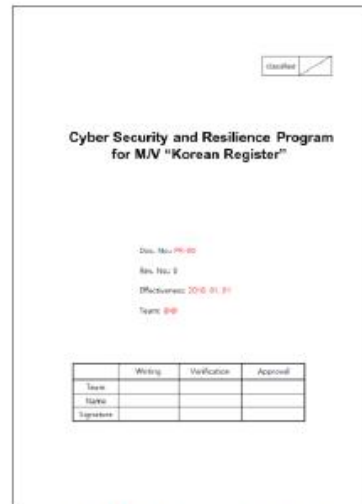
- **Policy and Procedures for CSMS (i.e. Cyber Security and Resilience Programme(CSRP) in UR E26)**
 - Management Process for Ship Cyber Resilience (UR E26 rev.1)
 - Cyber Risk Management Process (Covered by Res.MSC.428(98))
 - Organization and R&R (Covered by Res.MSC.428(98))
 - Crew awareness training (Covered by Res.MSC.428(98))
- **Cyber Incident Response Plan**
- **Recovery plans**



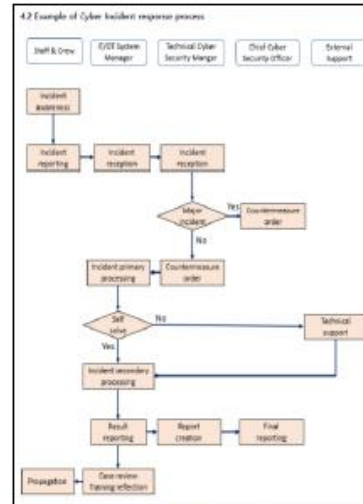
[Organization for CSMS]



[CSMS Policy]



[CSMS Procedure]



[CIRP]

Cyber Security Officer (CySO)

Key Responsibilities:

- Coordinating with the Company security officer (CSO) on aspects relating to physical, personnel and process security; and
- Ensuring the timely, periodic review and maintenance of the CSMS/CSRP; and
- Implementing and exercising the CSRP.

Where the CySO has insufficient knowledge of all cyber security issues and incidents, they should seek specific cyber security advice from an appropriate professional resource.

Note: The professional resource may be provided by the Company or provided as a professional support contract arranged by the Company.

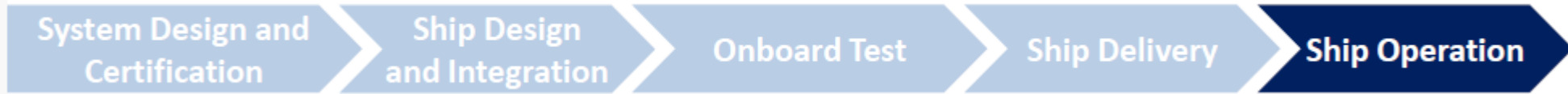
The CySO should maintain awareness of legal and regulatory changes that could affect the cyber security of ship assets and where necessary, adjust policies, processes and procedures to comply with these changes.

Note: The awareness of legal and regulatory changes may be monitored by the Company or provided through a professional support contract arranged by the Company, to be delivered to the CySO as a periodic update.

NOTE: Where the ship operates both within national waters and in foreign waters, including the high seas, the CySO should understand the jurisdiction issues regarding law enforcement and cyber security incidents, however the line of jurisdiction is a complex area for cyber security and maritime offences and expert legal advice should be sought in the event of an incident. Such consultation should form an integral incident recording process.

[Roles and Responsibility]

III. Cybersecurity in Smart Ship



Operation of Ship Cyber Security Management System (CSMS)

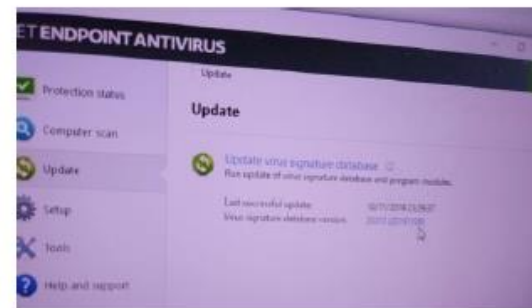
- **Update of documents and manuals**
 - CSMS procedure, CIRP, Recovery Plan, etc.
- **Ship Cyber Risk Management**
 - Cyber Risk Assessment in annual basis
 - Adopt mitigation controls for high cyber risks
- **Awareness Training**
 - Crew training plan and training record
- **Management of Changes of OT systems**
 - SW update and HW changes
 - Update Vessel Asset Inventory
- **Network system management**
 - Firewall management, network monitoring status
- **Patch update**
 - Update of Antivirus program or security patch
- **Access control**
 - Management of ID and Password for systems
 - Access control for Visitors
 - Control of Mobile or Portable Device including USB media

ID	Asset	Asset Name / Location	Asset Class / Function	Asset Owner	Asset Status	Asset Location	Asset Value	Asset Risk	Asset Mitigation	Asset Control	Asset Audit	Asset Review
1001	Control Room	Control Room	Control Room	Control Room	Control Room	Control Room	Control Room	Control Room	Control Room	Control Room	Control Room	Control Room
1002	Engine Room	Engine Room	Engine Room	Engine Room	Engine Room	Engine Room	Engine Room	Engine Room	Engine Room	Engine Room	Engine Room	Engine Room
1003	Galley	Galley	Galley	Galley	Galley	Galley	Galley	Galley	Galley	Galley	Galley	Galley
1004	Accommodation	Accommodation	Accommodation	Accommodation	Accommodation	Accommodation	Accommodation	Accommodation	Accommodation	Accommodation	Accommodation	Accommodation
1005	Stores	Stores	Stores	Stores	Stores	Stores	Stores	Stores	Stores	Stores	Stores	Stores

[Cyber Risk Assessment Report]



[Crew training plan]



[Update of antivirus program]



[Installation of USB Port Blocker]

III. Cybersecurity in Smart Ship

Risk-based Cybersecurity Approach – Smart System

CONTENTS

CHAPTER 1 GENERAL	1
Section 1 General	1
Section 2 Class Notations	2
CHAPTER 2 CLASSIFICATION SURVEYS	3
Section 1 Classification Surveys	3
CHAPTER 3 FUNCTIONAL REQUIREMENTS FOR SMART SYSTEMS	5
Section 1 Smart Infrastructure	5
Section 2 Structural Health Monitoring(SHM)	7
Section 3 Machinery Health Monitoring(MHM)	9
Section 4 Energy Efficiency Management(EEM)	10
Section 5 Intelligent Navigation	11
CHAPTER 4 SCALABLE TECHNOLOGY	13
Section 1 Virtual Reality(VR)	13
Section 2 Augmented Reality(AR)	13

Section 1 Smart Infrastructure

101. General

1. The purpose of smart infrastructure is to perform smart system functions through hardware and software installed to implement smart system functions.
2. The smart infrastructure includes the necessary components to collect, manage and relay data.
3. The smart infrastructure shall be capable of collecting and storing information received from one or more source systems.
4. The smart infrastructure shall meet the relevant requirements for data quality management in this guidance.
5. Electrical and electronic equipment on the bridge shall be installed so that electromagnetic interference does not affect the proper function of navigational systems and equipment.
6. Screen displays and indications installed on the bridge shall be installed so as not to obstruct the navigator's view even at night. *(2024)*

102. Configuration and functional requirements of smart systems

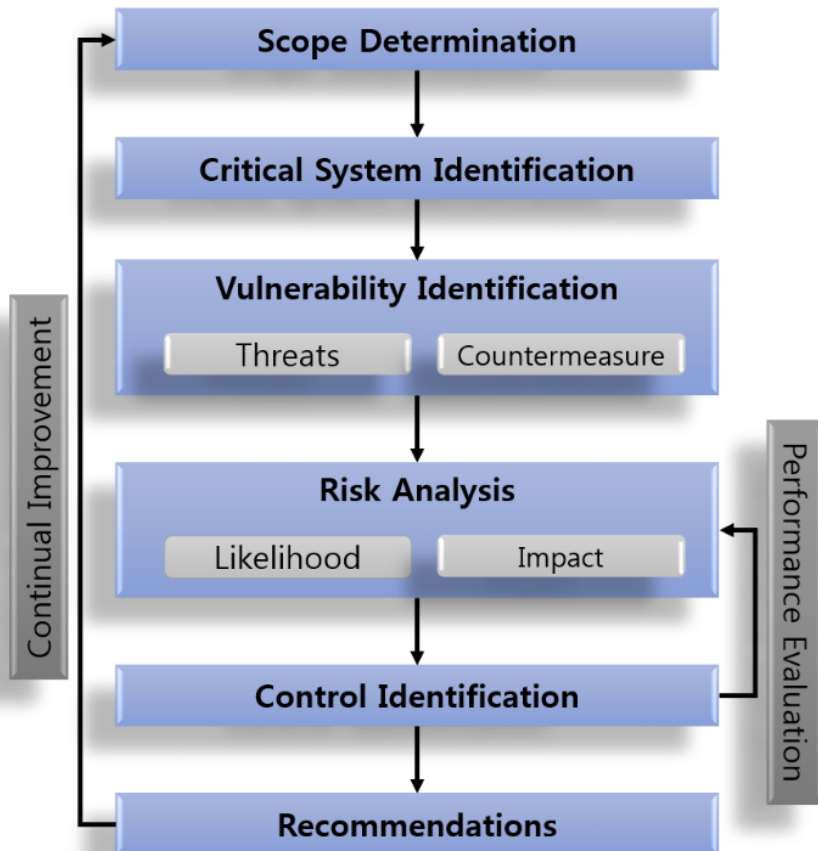
The infrastructure for implementing the functions of a smart system may include the following configurations and functions, but is not limited to.

1. Sensor for smart system functions

- (1) Internal and external data are received through sensors installed to implement smart system functions.
- (2) Hardware and software installed to interface with the on-board system shall have the following functions:
 - (A) Data interface to support certain number and type of input/output channels;
 - (B) Configurable and expandable input/output channels, in terms of number and type of channels;
 - (C) Connection to the data network and communication function when smart system function is implemented;
 - (D) Time stamping and time synchronization for the data collected; and
 - (E) Monitoring and alarming for data transmission

III. Cybersecurity in Smart Ship

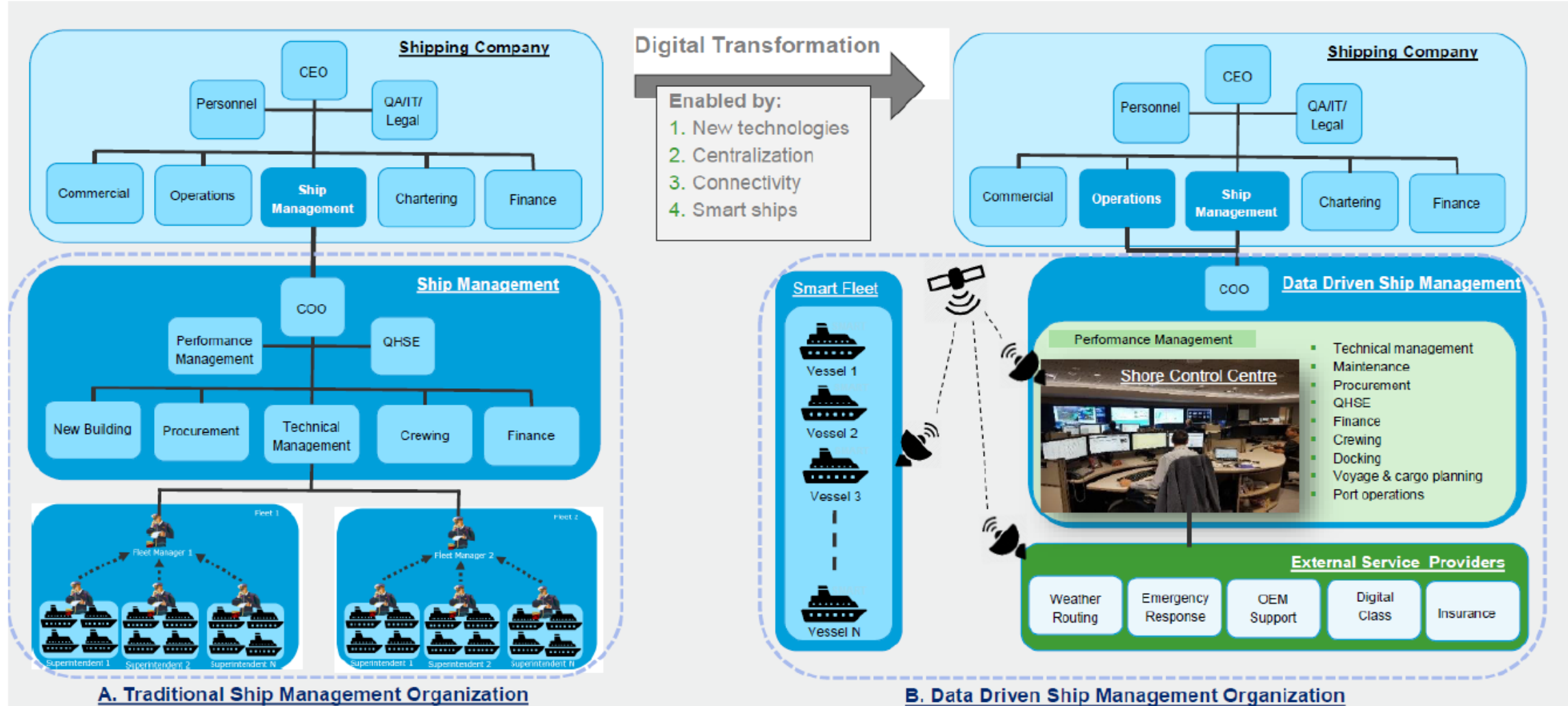
Risk-based Cybersecurity Approach – Risk Assessment



*	Scope Determination
01	Communication System <ul style="list-style-type: none">• Starlink• 6G Satellite
02	Smart Equipment <ul style="list-style-type: none">• Autonomous Navigation Control System• Smart Safe Navigation System• Smart Economic Navigation System• Smart Eco-friendly navigation system
03	On shore <ul style="list-style-type: none">• Remote Vessel Navigation System

III. Cybersecurity in Smart Ship

Data-Driven Ship Operation in Smart ship



III. Cybersecurity in Smart Ship

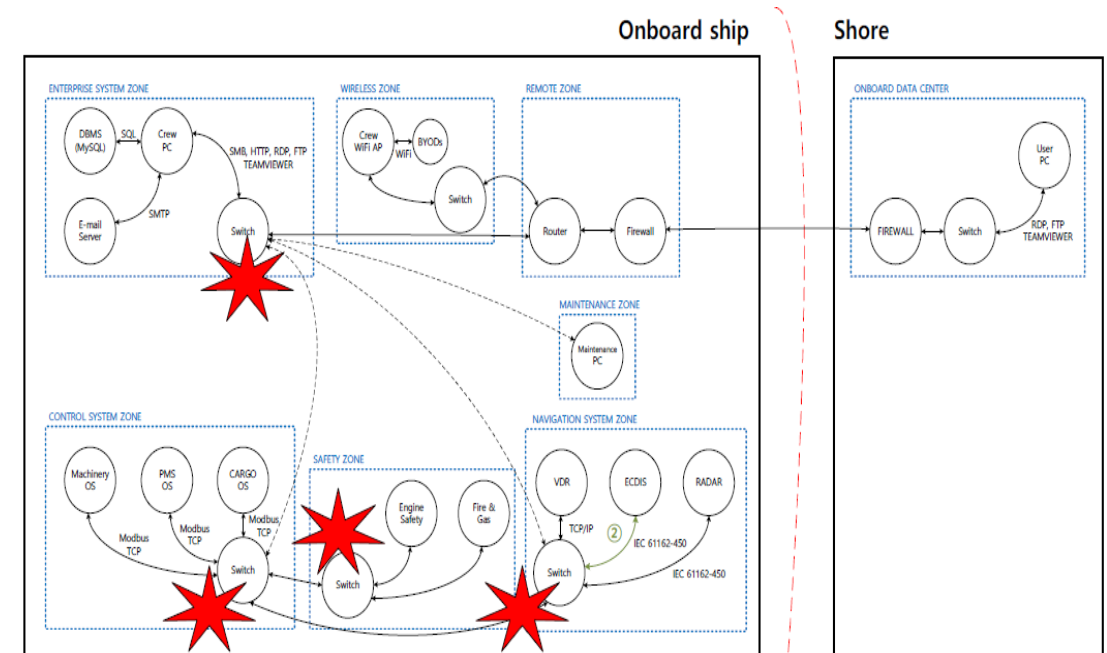
Risk-based Cybersecurity Approach – Asset List Including Data & Data Flow

2.2. Alarm Monitoring System

No.	Component Name	Type	Manufacturer	Model	Location	Port (of the Asset equipment)			
						USB	LAN	Serial	CAN
1	SPOWS1	Operation Station	HP		ECC	2	2	-	-
2	SPOWS2	Operation Station	HP		ECC	2	2	-	-
3	SPOWS3	Operation Station	HP		C/E's RM	2	2	-	-
4	SPOWS4	Operation Station	HP		BCC	2	2	-	-

No.	Component Name	IP Address	Subnet Mask	Malware Protection Means	Interface to other Systems	Interface Method	OS		
							Name	Version	Last update
1	SPOWS1			-	-		Windows 10	Professional or Higher Ver	-
2	SPOWS2			-	VDR	Serial	Windows 10	Professional or Higher Ver	-
3	SPOWS3			-	-		Windows 10	Professional or Higher Ver	-
4	SPOWS4			-	-		Windows 10	Professional or Higher Ver	-

No.	Component Name	Software			Firmware			Access Control	Maintenance Method	Scope of E26
		Name	Version	Last update	Name	Version	Last update			
1	SPOWS1				N/A	N/A	N/A	P	L	O
2	SPOWS2				N/A	N/A	N/A	P	L	O
3	SPOWS3				N/A	N/A	N/A	P	L	O
4	SPOWS4				N/A	N/A	N/A	P	L	O



New Asset List : Including Data & Information

Data Flow Diagram

III. Cybersecurity in Smart Ship

Data-Driven Ship, Data-Driven Treats

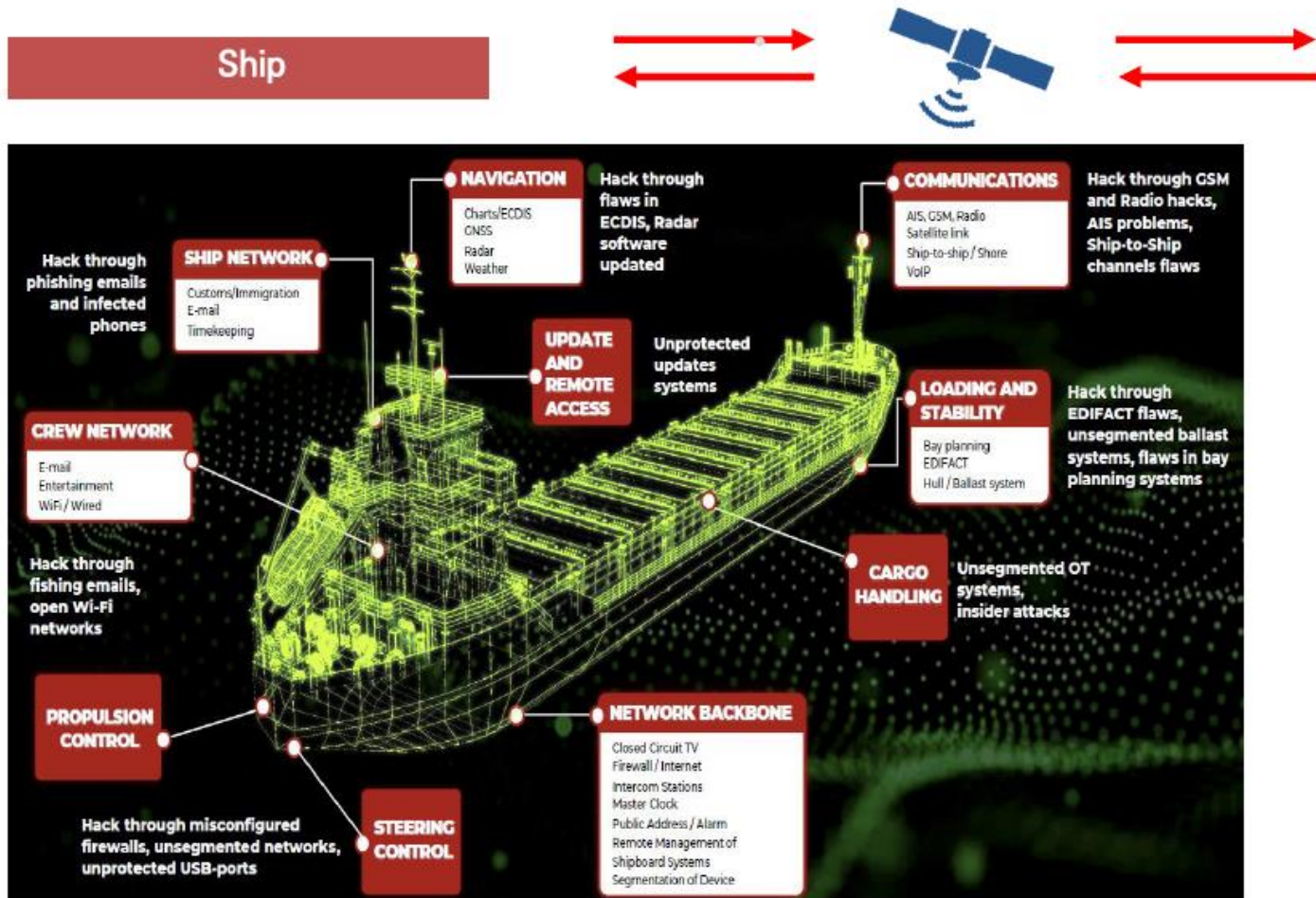


Image source : Reperion

Data-Driven Ships



Voyage Planning



Machinery Maintenance



Energy Efficiency Management

Shore Center



III. Cybersecurity in Smart Ship

Data-Driven Ship, Data-Driven Treats

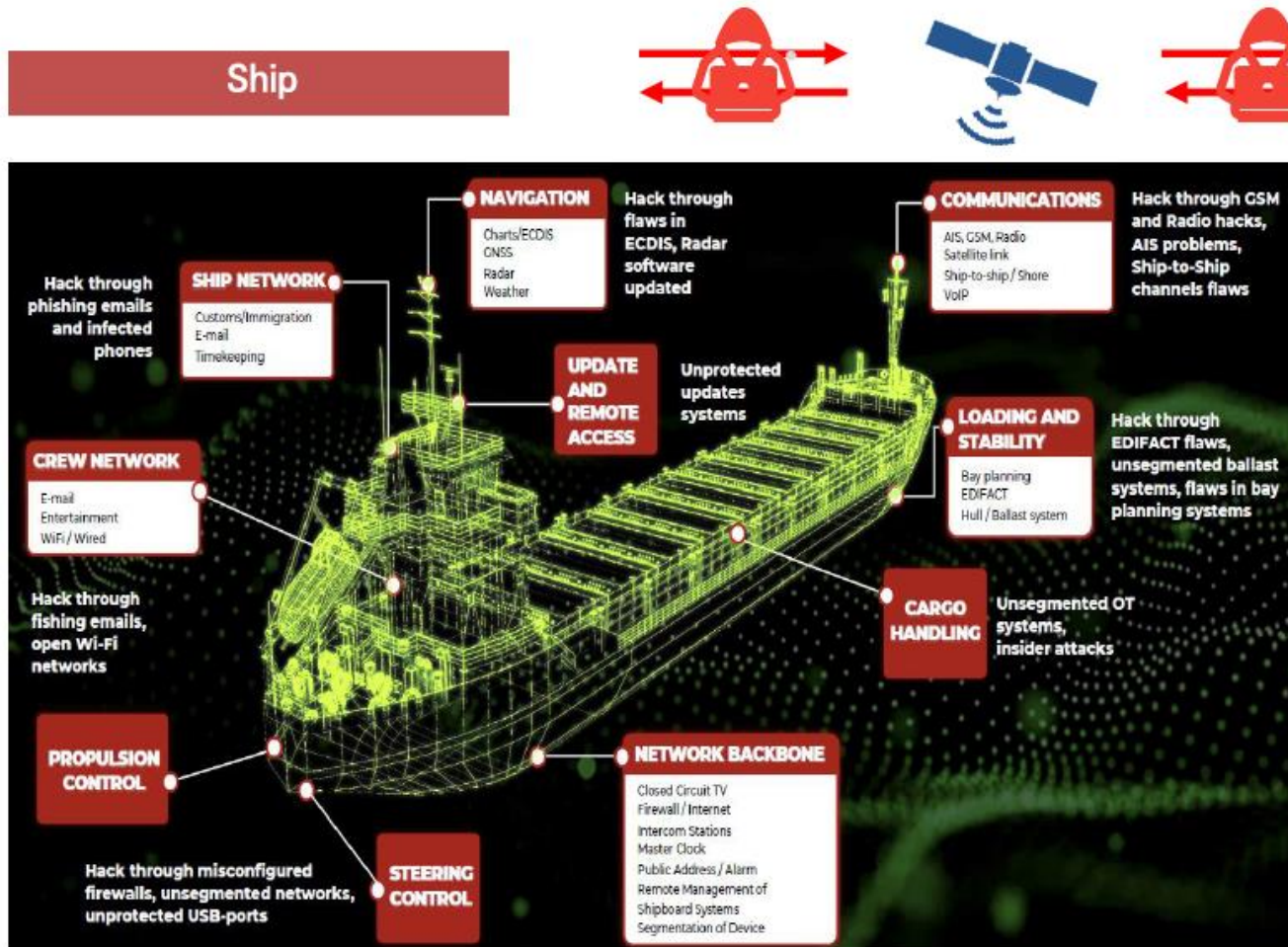


Image source : Reperion

Data-Driven Threats



Unauthorized Alteration of Voyage Plans



Exploiting IoT Devices



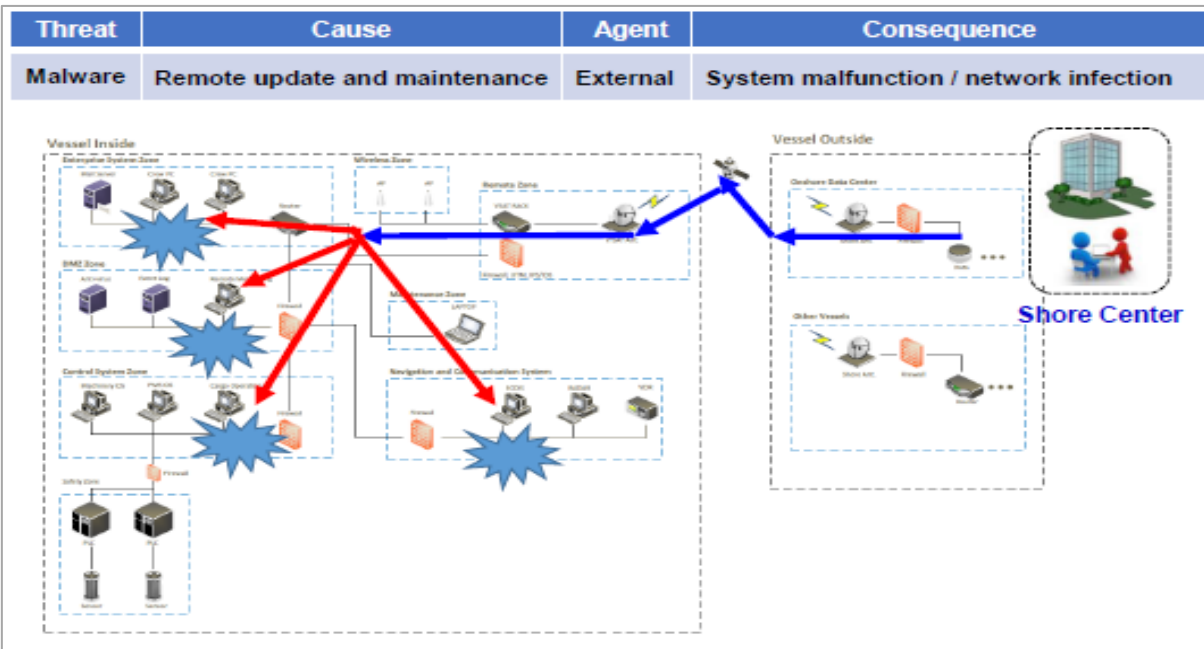
Theft of Sensitive Data Management

Shore Center



III. Cybersecurity in Smart Ship

Data-Driven Ship, Data-Driven Treats – Cyberattack Scenarios



Identify cyber threats

No. (old No.)	Top 10 2016	Top 10 2014
1 (3)	Social Engineering and Phishing*	Malware Infection via Internet and Intranet
2 (2)	Infiltration of Malware via Removable Media and External Hardware	Infiltration of Malware via Removable Media and External Hardware
3 (1)	Malware Infection via Internet and Intranet	Social Engineering
4 (5)	Intrusion via Remote Access	Human Error and Sabotage
5 (4)	Human Error and Sabotage	Intrusion via Remote Access
6 (6)	Control Components Connected to the Internet	Control Components Connected to the Internet
7 (7)	Technical Malfunctions and Force Majeure	Technical Malfunctions and Force Majeure
8 (9)	Compromising of Extranet and Cloud Components	Compromising of Smartphones in the Production Environment
9 (10)	(D)DoS Attacks	Compromising of Extranet and Cloud Components
10 (8)	Compromising of Smartphones in the Production Environment	(D)DoS Attacks

Ref. : BSI Industrial Control System Security – Top 10 Threats and Countermeasures 2016

III. Cybersecurity in Smart Ship

Data-Driven Ship, Data-Driven Treats – Cyberattack Scenarios

MITRE ATT&CK summarizes cyber threat cases in the form of a kill chain

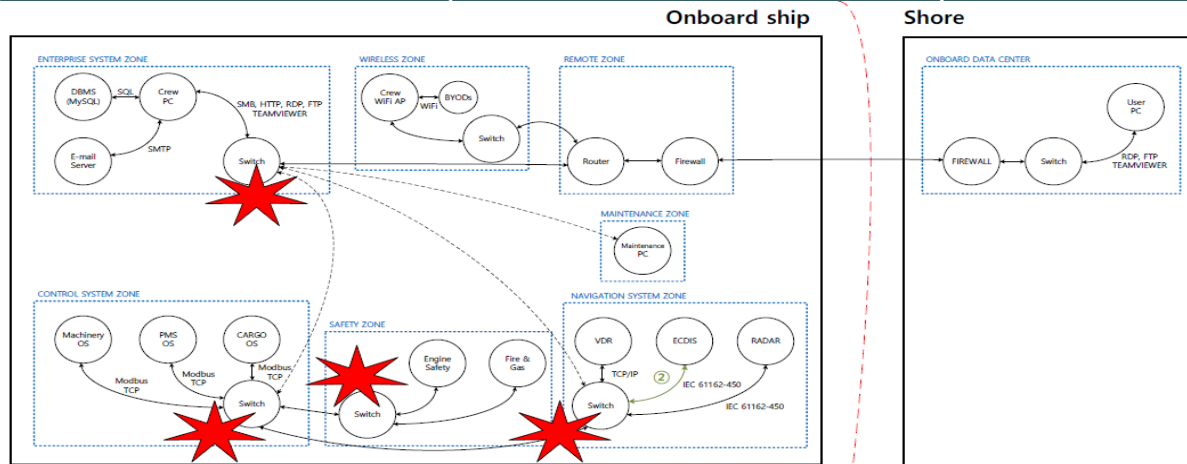
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
9 techniques	10 techniques	17 techniques	12 techniques	32 techniques	13 techniques	22 techniques	9 techniques	15 techniques	16 techniques	8 techniques	13 techniques
<ul style="list-style-type: none"> Drive-by Compromise Exploit Public-Facing Application External Remote Services Hardware Additions Phishing Replication Through Removable Media Supply Chain Compromise Trusted Relationship Valid Accounts 	<ul style="list-style-type: none"> AppleScript JavaScript/JScript PowerShell Python Unix Shell Visual Basic Windows Command Shell Exploitation for Client Execution Inter-Process Communication Native API Scheduled Task/Job Shared Modules Software Deployment Tools System Services User Execution Windows Management Instrumentation 	<ul style="list-style-type: none"> Account Manipulation BITS Jobs Boot or Logon Autostart Execution Boot or Logon Initialization Scripts Browser Extensions Compromise Client Software Binary Create Account Create or Modify System Process Event Triggered Execution Exploitation for Privilege Escalation Group Policy Modification Hijack Execution Flow External Remote Services Hijack Execution Flow Office Application Startup Pre-OS Boot Scheduled Task/Job Server Software Component Traffic Signaling Valid Accounts 	<ul style="list-style-type: none"> Abuse Elevation Control Mechanism Access Token Manipulation Boot or Logon Autostart Execution Boot or Logon Initialization Scripts Create or Modify System Process Event Triggered Execution Exploitation for Privilege Escalation Group Policy Modification Hide Artifacts Hijack Execution Flow Process Injection Scheduled Task/Job Valid Accounts Masquerading Modify Authentication Process Modify Registry Obfuscated Files or Information Pre-OS Boot Process Injection Rogue Domain Controller 	<ul style="list-style-type: none"> Abuse Elevation Control Mechanism Access Token Manipulation BITS Jobs Deobfuscate/Decode Files or Information Direct Volume Access Execution Guardrails Exploitation for Defense Evasion File and Directory Permissions Modification Group Policy Modification Hide Artifacts Hijack Execution Flow Impair Defenses Indicator Removal on Host Scheduled Task/Job Indirect Command Execution Invalid Code Signature Masquerade Task or Service Match Legitimate Name or Location Rename System Utilities Right-to-Left Override Space after Filename 	<ul style="list-style-type: none"> Brute Force Credentials from Password Stores Exploitation for Credential Access Forced Authentication Input Capture Man-in-the-Middle Modify Authentication Process Network Sniffing OS Credential Dumping Steal or Forge Kerberos Tickets Steal Web Session Cookie Two-Factor Authentication Interception Unsecured Credentials 	<ul style="list-style-type: none"> Account Discovery Application Window Discovery Browser Bookmark Discovery Domain Trust Discovery File and Directory Discovery Network Service Scanning Network Share Discovery Network Sniffing Password Policy Discovery Peripheral Device Discovery Permission Groups Discovery LSA Secrets LSASS Memory NTDS Proc Filesystem Security Account Manager Software Discovery System Information Discovery System Network Configuration Discovery System Network Connections Discovery System Owner/User Discovery System Service Discovery System Time Discovery Virtualization/Sandbox Evasion 	<ul style="list-style-type: none"> Domain Account Email Account Local Account Exploitation of Remote Services Internal Spearphishing Lateral Tool Transfer Remote Service Session Hijacking Distributed Component Object Model Remote Desktop Protocol SMB/Windows Admin Shares SSH VNC Windows Remote Management Replication Through Removable Media Software Deployment Tools Taint Shared Content Use Alternate Authentication Material Pass the Hash Pass the Ticket 	<ul style="list-style-type: none"> Archive Collected Data Audio Capture Automated Collection Clipboard Data Data from Information Repositories Data from Local System Data from Network Shared Drive Data from Removable Media Data Staged Email Collection Input Capture Man in the Browser Man-in-the-Middle Screen Capture Video Capture Archive via Custom Method Archive via Library Archive via Utility Application Layer Protocol Communication Through Removable Media Data Encoding Data Obfuscation Dynamic Resolution Encrypted Channel Fallback Channels Ingress Tool Transfer Multi-Stage Channels Non-Application Layer Protocol Non-Standard Port Protocol Tunneling Proxy Remote Access Software Traffic Signaling Web Service 	<ul style="list-style-type: none"> Automated Exfiltration Data Transfer Size Limits Data Encrypted for Impact Data Manipulation Defacement Disk Wipe Endpoint Denial of Service Exfiltration Over Other Network Medium Firmware Corruption Inhibit System Recovery Network Denial of Service Resource Hijacking Scheduled Transfer Service Stop System Shutdown/Reboot 	<ul style="list-style-type: none"> Account Access Removal Data Destruction Data Encrypted for Impact Data Manipulation Defacement Disk Wipe Endpoint Denial of Service Exfiltration Over Other Network Medium Firmware Corruption Inhibit System Recovery Network Denial of Service Resource Hijacking Service Stop System Shutdown/Reboot 	

Threat scenarios used by APT 1 in its attack

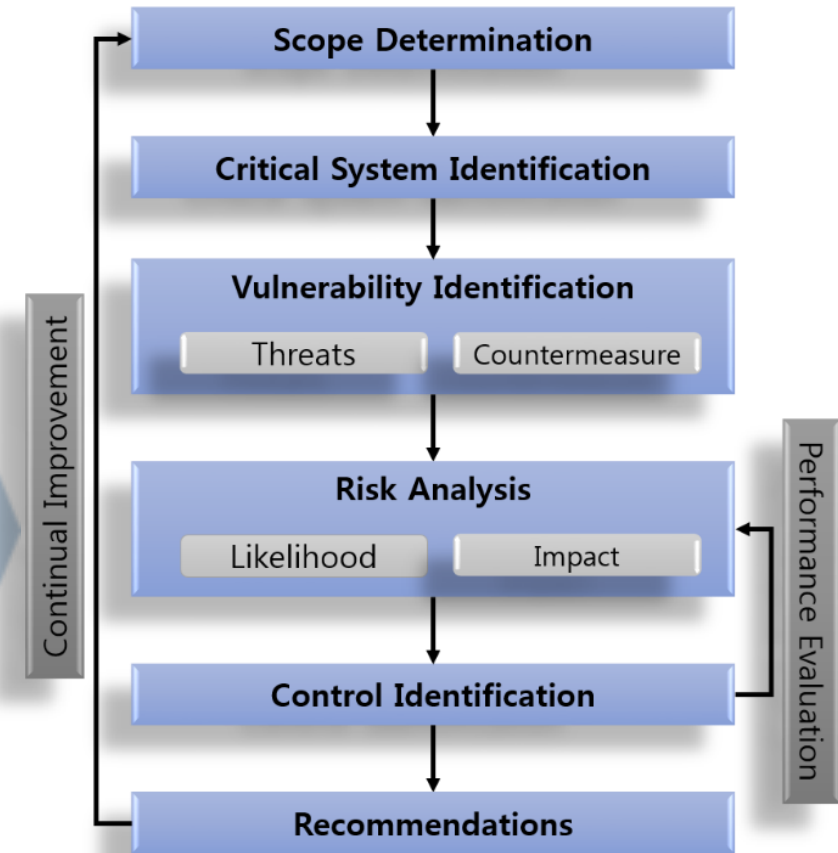
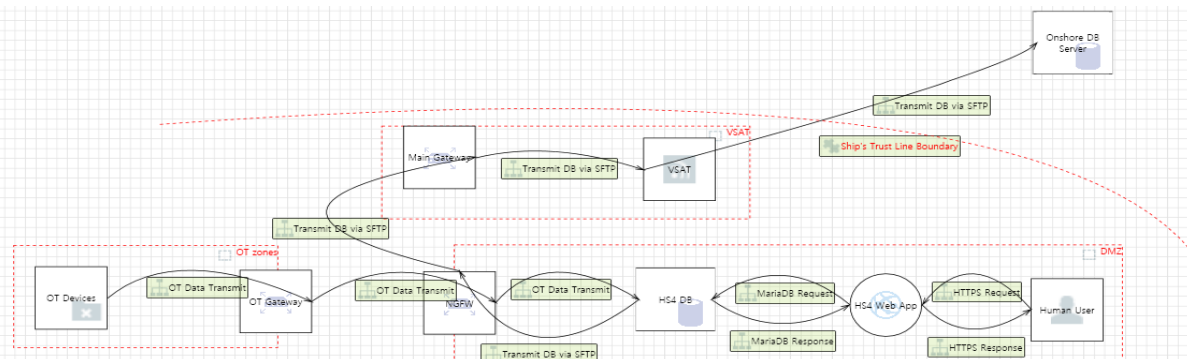
III. Cybersecurity in Smart Ship

Cybersecurity Risk Modeling

Smart Ship Platform DFD Modeling



Threat Modeling Tool



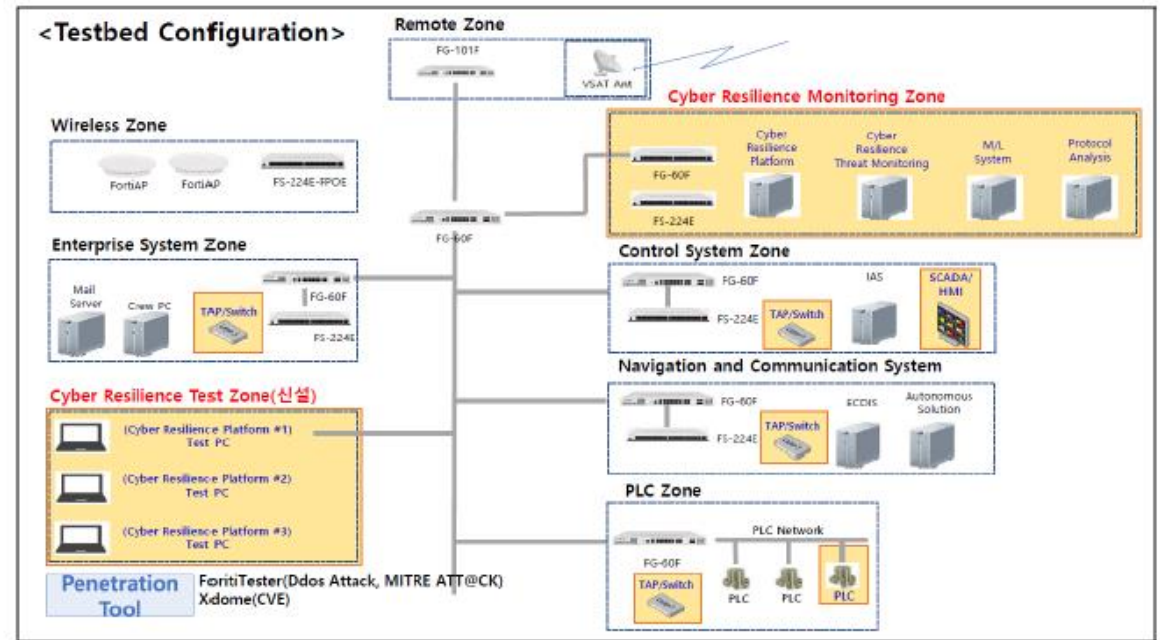
III. Cybersecurity in Smart Ship

Smart Ship Cybersecurity Testbed

Smartship Cyber Security Testbed Operation ('23~'27.12)



Technical verification through testbed

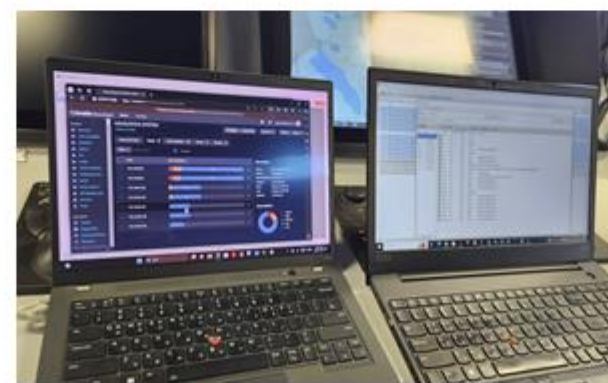


III. Cybersecurity in Smart Ship

Smart Ship Cybersecurity Testbed



Vulnerability diagnostics and penetration testing tools



Ship Equipment Testing Equipment



III. Cybersecurity in Smart Ship

Smart Ship Cybersecurity Testbed

Vulnerability Analysis Tool

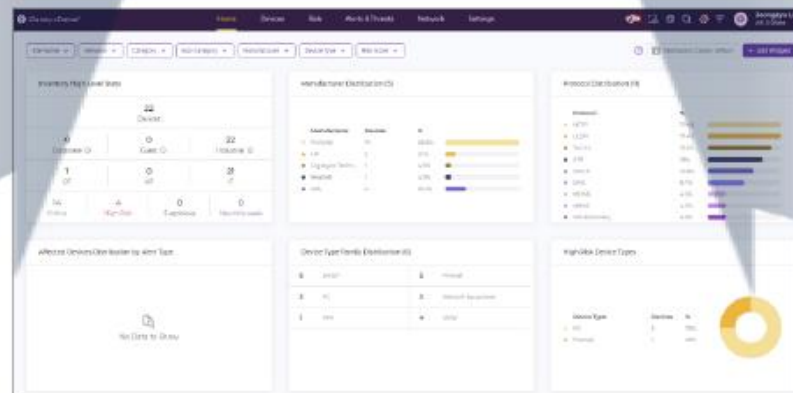


Device/Protocol	Test 1	Test 2	Test 3	Test 4	Test 5	Test 6	Test 7	Test 8	Test 9	Test 10	Test 11	Test 12	Test 13	Test 14	Test 15	Test 16	Test 17	Test 18	Test 19	Test 20
Device A	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass
Device B	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass
Device C	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass
Device D	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass
Device E	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass

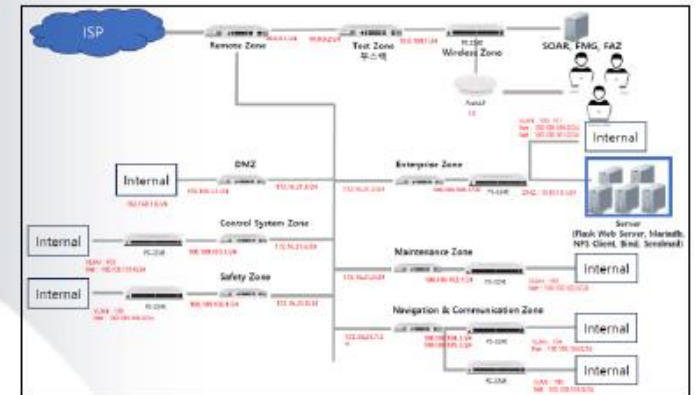
Ship Cyber Resilience Document Control & Design Platform



Ship Cyber Resilience Onboard Platform (SIEM, IDS, etc)



Cyber Security Testbed





Thank you

Contact

- ADD**
- 36, Myeongji ocean city 9-ro, Gangseo-gu, Busan 46762 Republic of Korea
- E-mail**
- kaemyoung@krs.co.kr