Approach to Risk Assessment for Ship Cybersecurity

2024.06.20

Korean Register
Kaemyoung Park

Contents

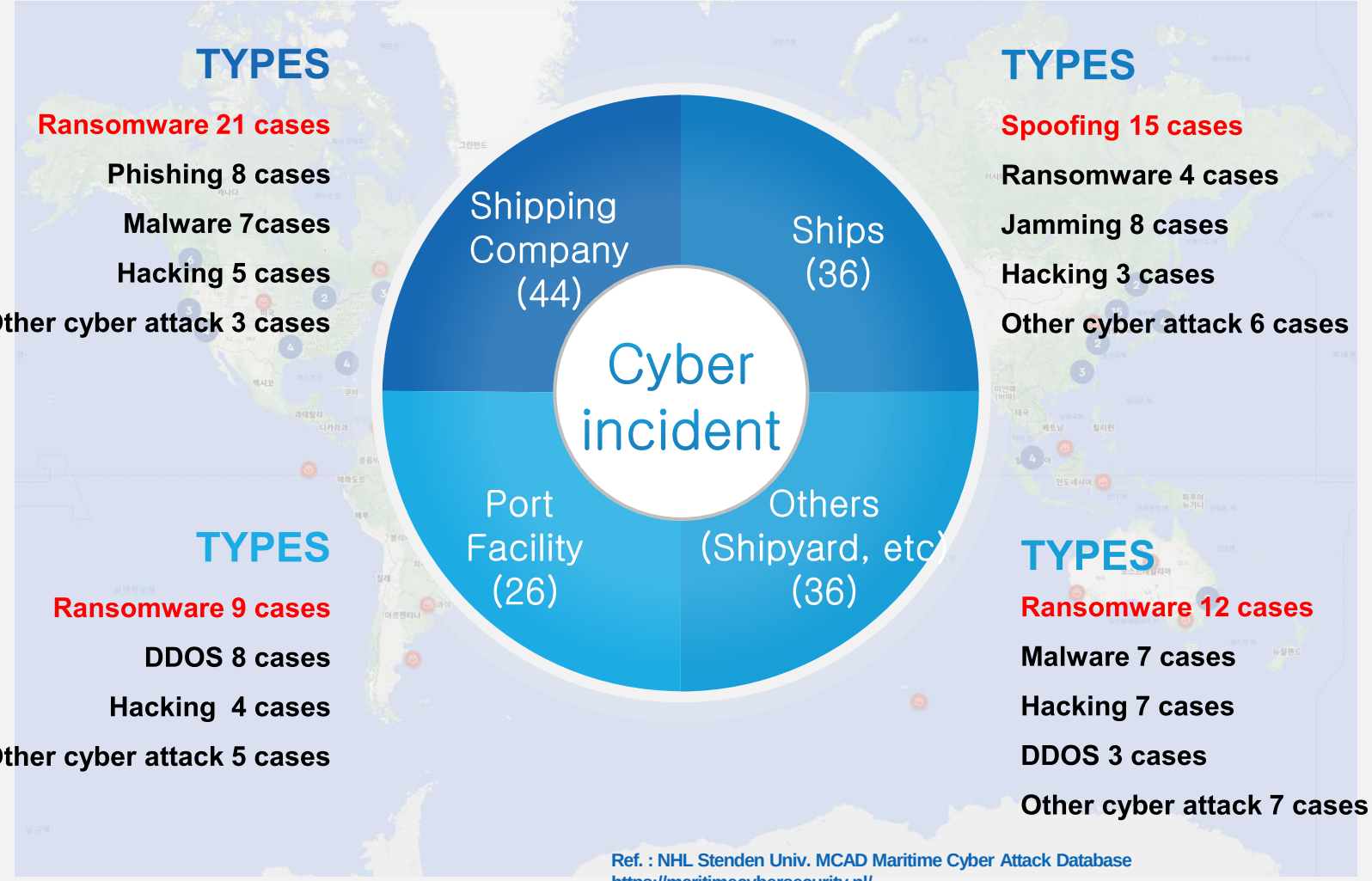
I

Cyber Security in Maritime

I. Cyber Security in Maritime

Cyber Incidents

Since 2000, more than 140 cyber incidents in the maritime sector have been reported, including ships, ports, and shipyards.

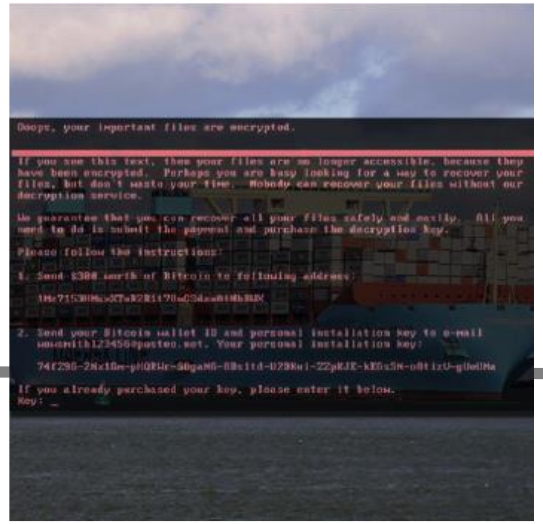


Ref. : NHL Stenden Univ. MCAD Maritime Cyber Attack Database
https://maritimecybersecurity.nl/

I. Cyber Security in Maritime

2017

$300 million in losses
(Ransomeware)



The world's largest shipping company, "Maersk," suffered damage from the 'NotPetya' ransomware attack. This resulted in cargo processing delays at APM terminals within the Maersk group and 76 ports in the United States, India, Spain, and the Netherlands.

2018

Ransomware attack cases

Starting from the Port of Barcelona, a ransomware cyber attack occurred in the same manner to the Port of San Diego in the United States in about two weeks. It was reported that the damage was at the level of paralysis of the internal IT network, but experts predicted that it would have been accompanied by damage to bail bonds.

Ransomware attack cases

Switzerland's MSC and France's CMA CGM both suffered malware and ransomware attacks, and in the case of France, 'Ragnar Locker' ransomware attacked MS's OS system.

2023

Ransomware attack cases

Cyber-ransom attack hits Japan's Nagoya port

Beef Central, July 10, 2023

Nagoya is Japan's largest port. Photo: Port of Nagoya

The attack disrupted cargo packing procedures and forced the suspension of operations at the container terminal, reported

Bloomberg

I. Cyber Security in Maritime

1. IMO and Administrations

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

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

* Over 23 flag states like USCG, Marshall Island, Singapore, Australia, Cyprus, Vanuatu require it as mandatory.

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

2. Shipping Association

2016 Guidelines on Cyber Security Onboard Ships

2017, 2018. 2nd and 3rd Version of 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.

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

4. Classification Societies

2018 Cyber Security Rec.153~164

2020 Rec.166 – Recommendation on Cyber Resilience

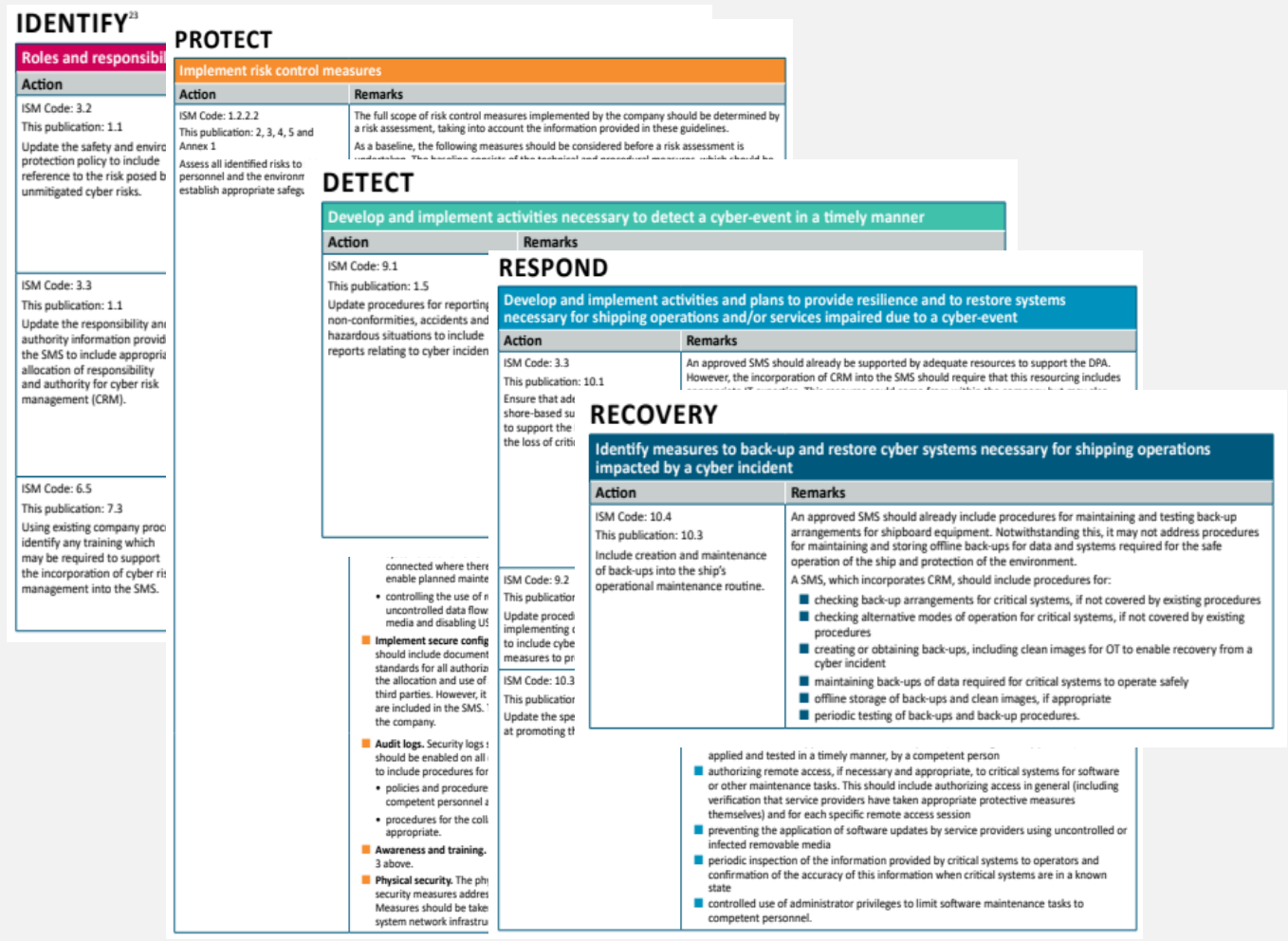
2022 UR E26 – Cyber Resilience of Ships

UR E27 – Cyber Resilience of onboard systems and equipment

2024 Guidance for Cyber Resilience

IMO : International Maritime Organization, USCG : US Coast Guard, BIMCO : Baltic and International Maritime Council, DCSA : Digital Container Shipping Association, OCIMF : Oil Companies International Marine Forum , IACS : International Association of Classification Societies

I. Cyber Security in Maritime



IDENTIFY[23]

Roles and responsibi	
Action	
ISM Code: 3.2 This publication: 1.1 Update the safety and enviro protection policy to include reference to the risk posed b unmitigated cyber risks.	
ISM Code: 3.3 This publication: 1.1 Update the responsibility an authority information provid the SMS to include appropri allocation of responsibility and authority for cyber risk management (CRM).	
ISM Code: 6.5 This publication: 7.3 Using existing company proc identify any training which may be required to support the incorporation of cyber ri management into the SMS.	

PROTECT

Implement risk control measures	
Action	**Remarks**
ISM Code: 1.2.2.2 This publication: 2, 3, 4, 5 and Annex 1 Assess all identified risks to personnel and the environm establish appropriate safeg	The full scope of risk control measures implemented by the company should be determined by a risk assessment, taking into account the information provided in these guidelines. As a baseline, the following measures should be considered before a risk assessment is

DETECT

Develop and implement activities necessary to detect a cyber-event in a timely manner	
Action	**Remarks**
ISM Code: 9.1 This publication: 1.5 Update procedures for reporting non-conformities, accidents and hazardous situations to include reports relating to cyber inciden	

connected where there enable planned mainte
- controlling the use of r uncontrolled data flow media and disabling US

Implement secure config should include document standards for all authoriz the allocation and use of third parties. However, it are included in the SMS. the company.

Audit logs. Security logs should be enabled on all to include procedures for
- policies and procedure competent personnel a
- procedures for the coll appropriate.

Awareness and training. 3 above.

Physical security. The ph security measures addres Measures should be take system network infrastru

RESPOND

Develop and implement activities and plans to provide resilience and to restore systems necessary for shipping operations and/or services impaired due to a cyber-event	
Action	**Remarks**
ISM Code: 3.3 This publication: 10.1 Ensure that ad shore-based su to support the the loss of criti	An approved SMS should already be supported by adequate resources to support the DPA. However, the incorporation of CRM into the SMS should require that this resourcing includes
ISM Code: 9.2 This publicatior Update proced implementing to include cybe measures to pr	
ISM Code: 10.3 This publicatior Update the spe at promoting th	

RECOVERY

Identify measures to back-up and restore cyber systems necessary for shipping operations impacted by a cyber incident	
Action	**Remarks**
ISM Code: 10.4 This publication: 10.3 Include creation and maintenance of back-ups into the ship's operational maintenance routine.	An approved SMS should already include procedures for maintaining and testing back-up arrangements for shipboard equipment. Notwithstanding this, it may not address procedures for maintaining and storing offline back-ups for data and systems required for the safe operation of the ship and protection of the environment. A SMS, which incorporates CRM, should include procedures for: ■ checking back-up arrangements for critical systems, if not covered by existing procedures ■ checking alternative modes of operation for critical systems, if not covered by existing procedures ■ creating or obtaining back-ups, including clean images for OT to enable recovery from a cyber incident ■ maintaining back-ups of data required for critical systems to operate safely ■ offline storage of back-ups and clean images, if appropriate ■ periodic testing of back-ups and back-up procedures.

applied and tested in a timely manner, by a competent person
- authorizing remote access, if necessary and appropriate, to critical systems for software or other maintenance tasks. This should include authorizing access in general (including verification that service providers have taken appropriate protective measures themselves) and for each specific remote access session
- preventing the application of software updates by service providers using uncontrolled or infected removable media
- periodic inspection of the information provided by critical systems to operators and confirmation of the accuracy of this information when critical systems are in a known state
- controlled use of administrator privileges to limit software maintenance tasks to competent personnel.

I. Cyber Security in Maritime

Effective date : 2021 2nd half year.

12 Security

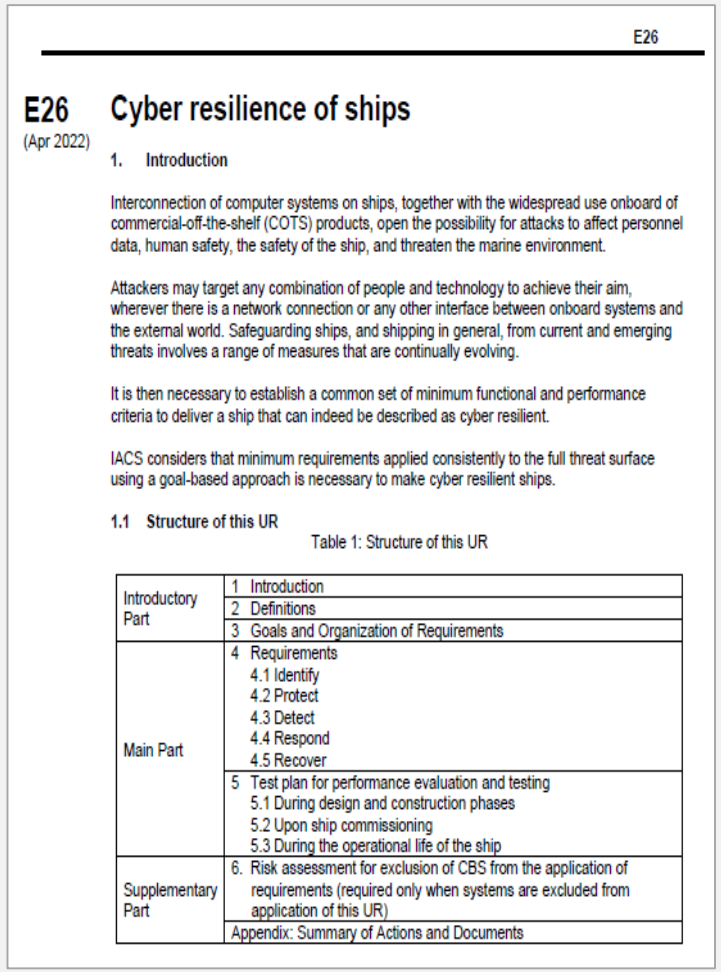
12.2 Has a Ship Security Officer (SSO) been appointed and trained adequately to perform the duties of SSO and **have all crew received security-related training and instructions?**

12.7 **Are cyber security policies and procedures being incorporated in the safety management system and was the cyber security management system evaluated and certified by Class?**

12.8 **Are measures in place for controlling the use of removable media** such as USB memory sticks, CDs, DVDs, and diskettes on shipboard computers?

I. Cyber Security in Maritime

IACS UR 26(Cyber resilience of ships)



E26

E26 (Apr 2022) **Cyber resilience of ships**

1. Introduction

Interconnection of computer systems on ships, together with the widespread use onboard of commercial-off-the-shelf (COTS) products, open the possibility for attacks to affect personnel data, human safety, the safety of the ship, and threaten the marine environment.

Attackers may target any combination of people and technology to achieve their aim, wherever there is a network connection or any other interface between onboard systems and the external world. Safeguarding ships, and shipping in general, from current and emerging threats involves a range of measures that are continually evolving.

It is then necessary to establish a common set of minimum functional and performance criteria to deliver a ship that can indeed be described as cyber resilient.

IACS considers that minimum requirements applied consistently to the full threat surface using a goal-based approach is necessary to make cyber resilient ships.

1.1 Structure of this UR

Table 1: Structure of this UR

Introductory Part	1 Introduction
	2 Definitions
	3 Goals and Organization of Requirements
Main Part	4 Requirements 4.1 Identify 4.2 Protect 4.3 Detect 4.4 Respond 4.5 Recover
	5 Test plan for performance evaluation and testing 5.1 During design and construction phases 5.2 Upon ship commissioning 5.3 During the operational life of the ship
Supplementary Part	6. Risk assessment for exclusion of CBS from the application of requirements (required only when systems are excluded from application of this UR)
	Appendix: Summary of Actions and Documents

Identify (4.1)

- Inventory of CBSs and networks onboard

Document

Protect (4.2)

- 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)

- Network operation monitoring
- Diagnostic functions of CBS and networks

Respond (4.4)

- Incident response plan
- Local, independent and/or manual operation
- Network isolation
- Fallback to a minimal risk condition

Recovery (4.5)

- Recovery plan
- Backup and restore capability
- Controlled shutdown, reset, roll–back and restart

Document, set up system configuration

I. Cyber Security in Maritime

Certification

- Ship Cyber Security Compliance Certification
- Company Cyber Security Compliance Certification
- Cyber Security Type Approval
- Computer-based System Conformity Certification

Consulting

- Cyber Security Risk Assessment
- Establishment of Cyber Security Management System
- Ship Network Design
- Vulnerability Diagnosis and Penetration Test

Training

- Customized Training Service
- Training Tools(USB, Pad)
- Web-based untact training platform

Platform

- Maritime Cyber Intelligence
- Security Management Platform for shipping company
- Security Management Platform for ships

II

Cyber Risk on Ships

II. Cyber Risk on Ships

What is Cyber Risk?

Cyber Security

Protects **intentional** disruption, compromise, or exploitation of a computer network or control system **by non-authorized personnel**.

Cyber Safety

protects **accidental** disruption of a computer network or control system **by an owner, operator, other actor**, or as an **unintended** consequence of a mishap within a connected cyber system.

Asset

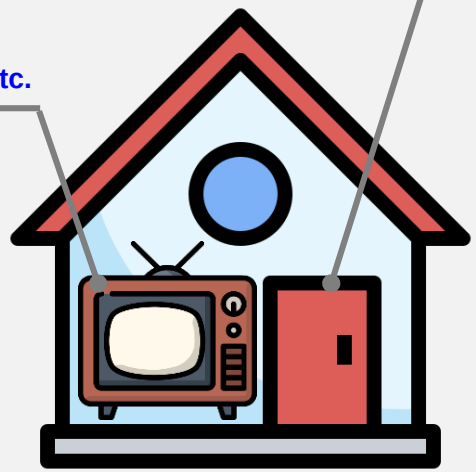
- **All resources worth protecting**
- **Information, documents, software, personnel, services, etc.**
- **Ship navigation system, ECDIS, IAS, etc.**

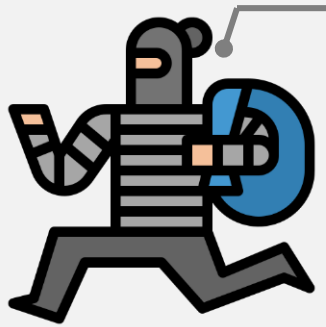
Vulnerability

- **Weaknesses of assets that result in losses due to threats**
- **Easy passwords, unauthorized confidential documents, etc.**

Threat

- **Causes or acts that may harm cyber assets**
- **Un-authorized access, fire, theft, malware, ransomware, etc.**





RISK = ASSET x VULNERABILITY x THREAT

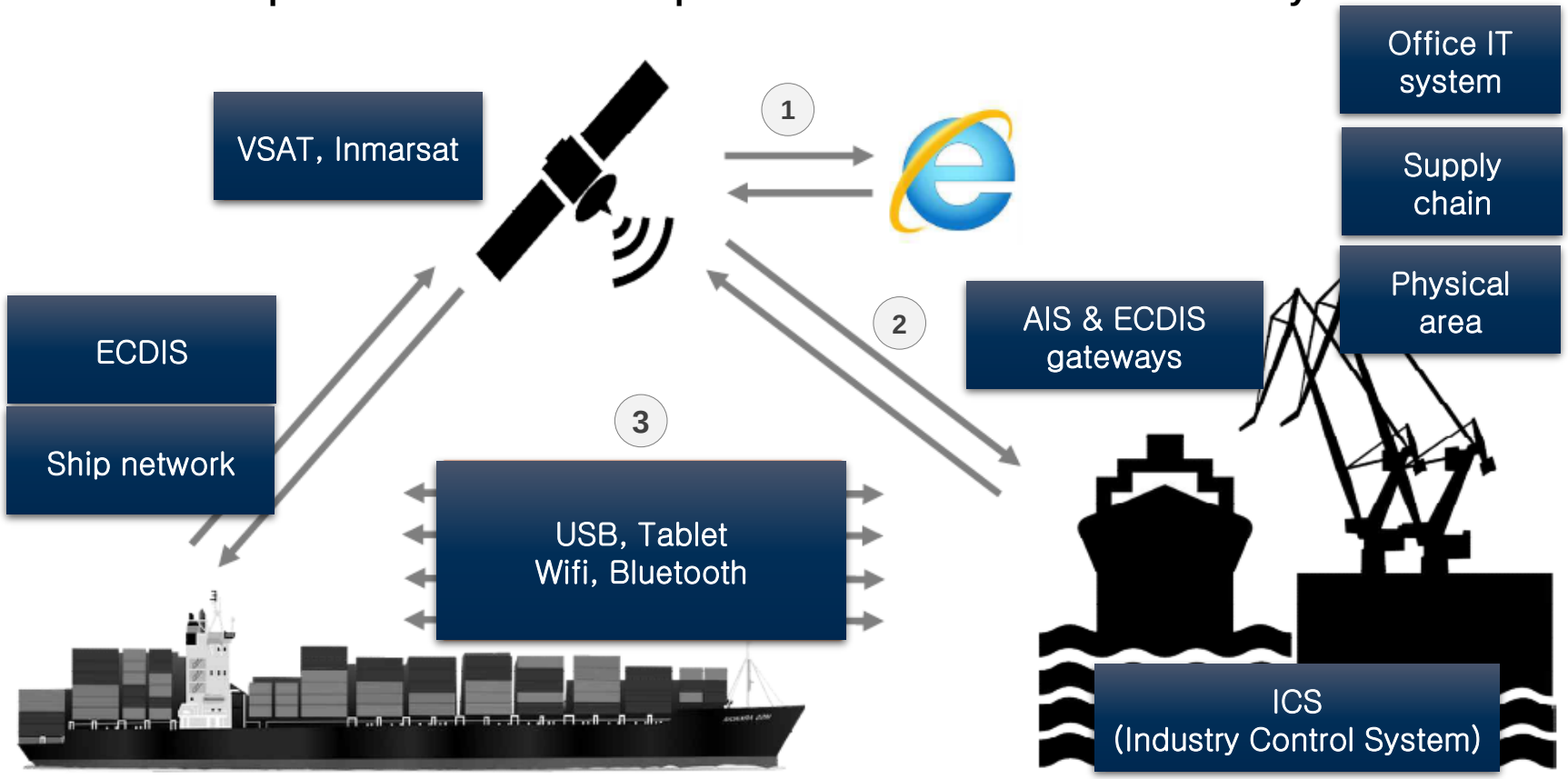
Possibility to use external vulnerabilities to exploit vulnerabilities that exist within the asset

II. Cyber Risk on Ships

Scenario 1. Malicious code downloaded to vessel due to unsafe website visits by crew.

Scenario 2. Infected by malicious code by opening a URL or attachment in the mail infected with malicious code from a port or shipping company

Scenario 3. Spread malware on the ship's network due to infected USB use by sailors.



II. Cyber Risk on Ships

MANUFACTURER

CYBER SECURITY TYPE

APPROVAL

SHIPYARD

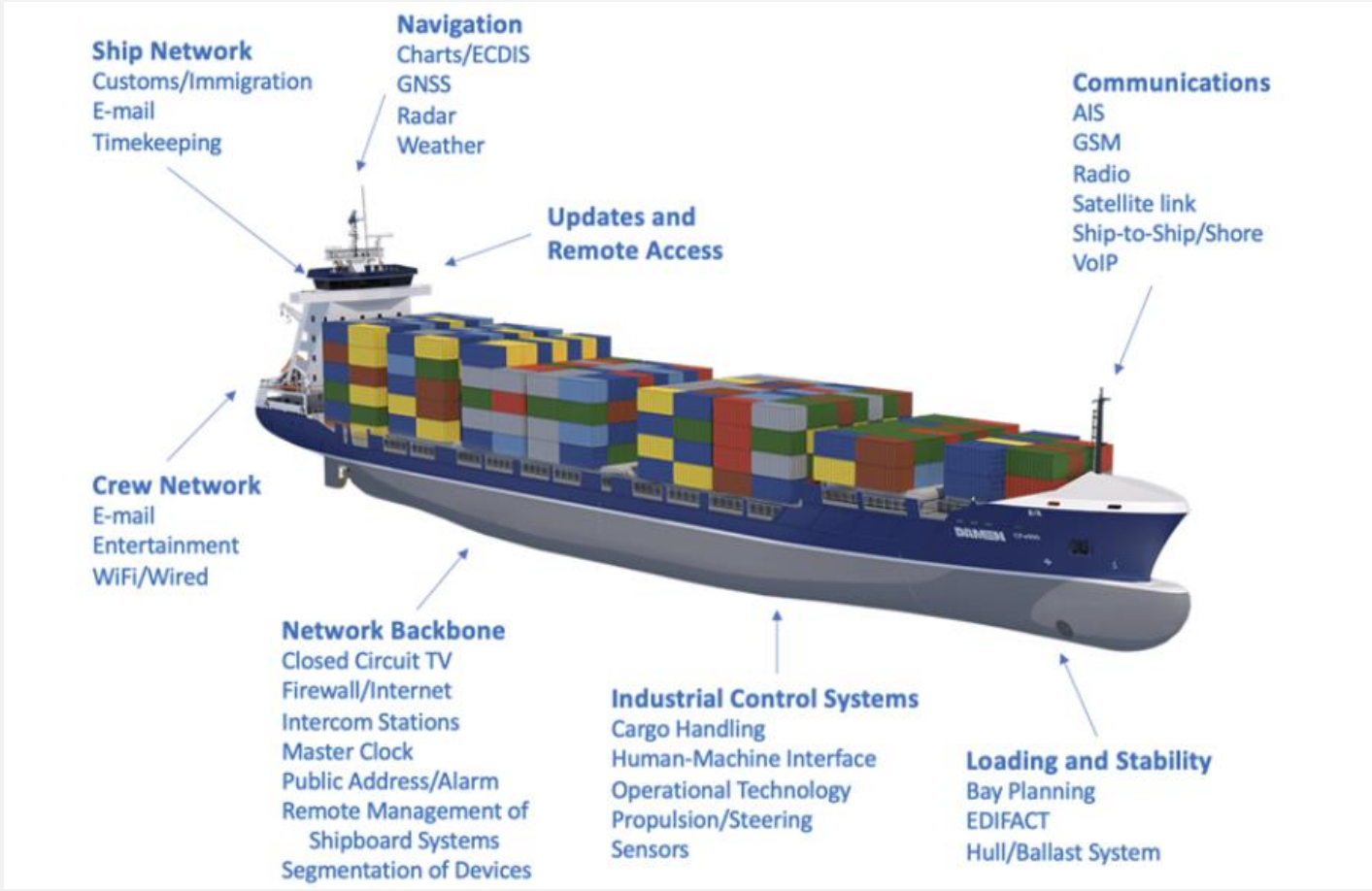
- RISK ASSESSMENT
- VULNERABILITY DIAGNOSIS

SHIP OWNER

- CYBER SECURITY POLICY
- PROCEDURE, TRAINING
- RISK ASSESSMENT

II. Cyber Risk on Ships

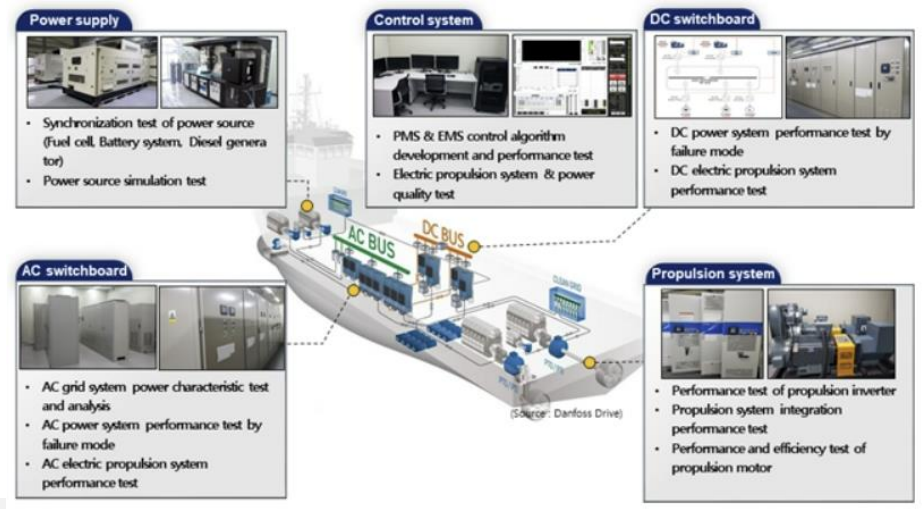
CPS(Cyber Physical System) on Ship



Navigation System

Engine Control System

Industrial Control System



II. Cyber Risk on Ships

KOREAN REGISTER.
Checklist for Ship Remote Cyber Security
Initial Survey

CSS- Work ID- CCT-C0010-20-

Ship Name : Songa Breeze
Date : 25th, January, 2021 07:30 GMT
Surveyor : LIM. Jeoung-kyu
Surveyor :
Verified

Code	Capability	Check items	Result
101	Share security issues	• Check cyber security issues listed in Safety Management System • Check crew cyber security awareness posters	
302 1	Establish and manage security policy	• Check cyber security policy(if necessary) • Check cyber security policy poster • Check cyber security key contacts poster • Check COMPUTER & PERSNAL DEVICES POLICY Poster	
302 2	R&R of security organization	• Check cyber security organizational chart onboard poster • Check R&R onboard poster	
303 1	Security training plan	• Check cyber security training record • Check cyber Security training plan poster	
303 2	Security training for the person on and off the ship	N/A(same as 303.1)	N/A
303 3	Specialized security training	• Check how KR's cyber security ERP module for specialized security training	
304 1	Threat list management	N/A(Document Reviewed)	N/A
304 2	Risk management plan	N/A(Document Reviewed)	N/A
304 3	Vulnerability diagnosis	N/A(Document Reviewed)	N/A
304 4	Risk Management	• Check cyber security risk assessment report • Check risk assessment workflow in Safety Management System • Check cyber security risk assessment poster	
304 5	Apply protection measures	N/A(Same as 307.1)	N/A
304 6	Share risk assessment results	N/A(Document Reviewed)	N/A
305 1	Asset identification	N/A(Document Reviewed)	N/A
305 2	Role and responsibility of asset management	• Check cyber asset and responsible personnel onboard	
305 3	Classification of data importance	N/A(Document Reviewed)	N/A
307 4	Data storage	• Check data backup devices installed in VSAT unit	
306 1	Access control policy	To be verified with Songa Shipmanagement in Glasgow	TBD

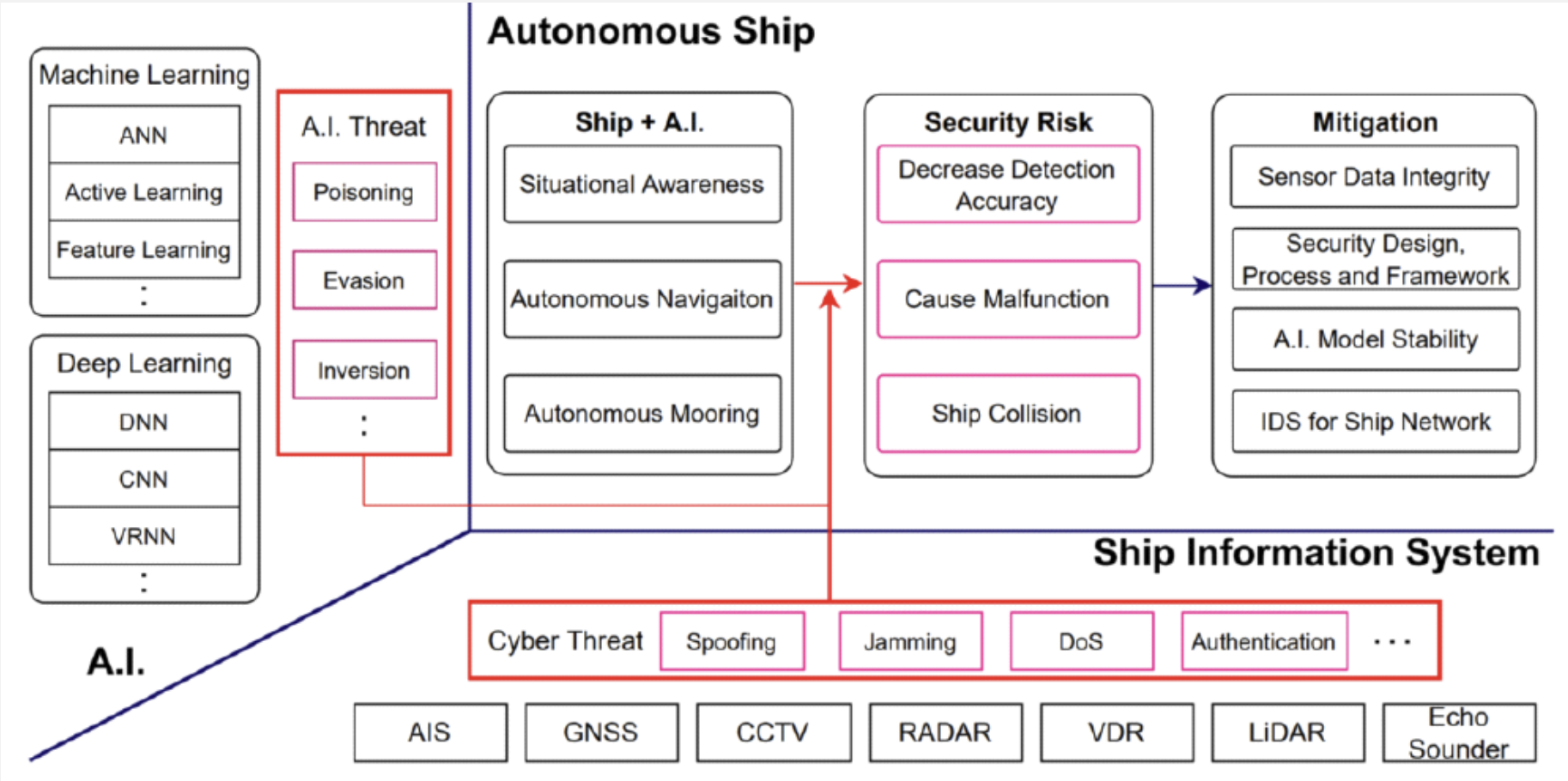
Form CCT.CHK 1 / 4 (2020.11)

Form CCT.CHK 2 / 4 (2020.11)

Form CCT.CHK 3 / 4 (2020.11)

Form CCT.CHK 4 / 4 (2020.11)

II. Cyber Risk on Ships

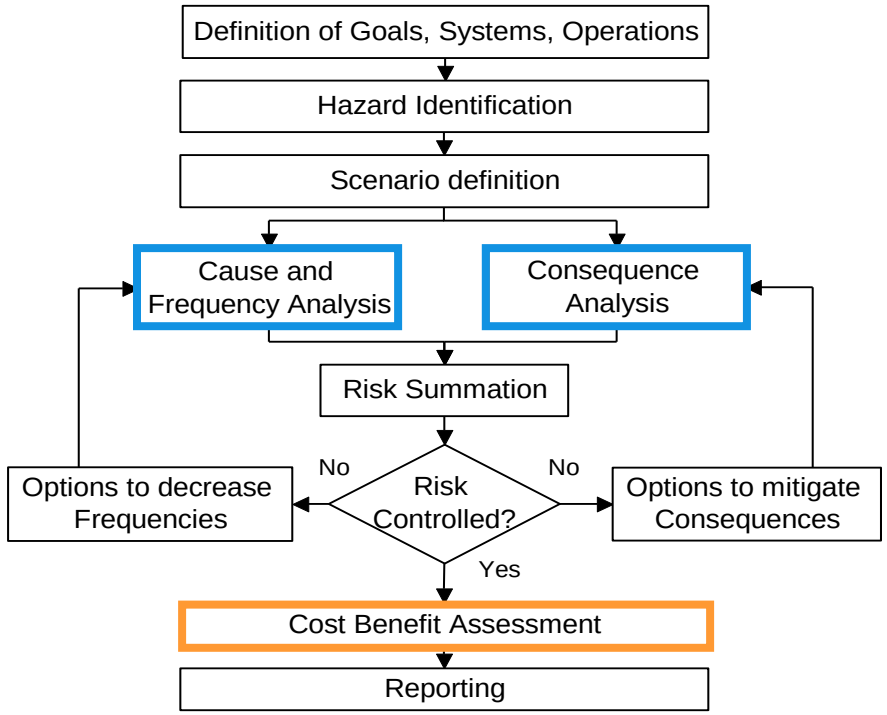


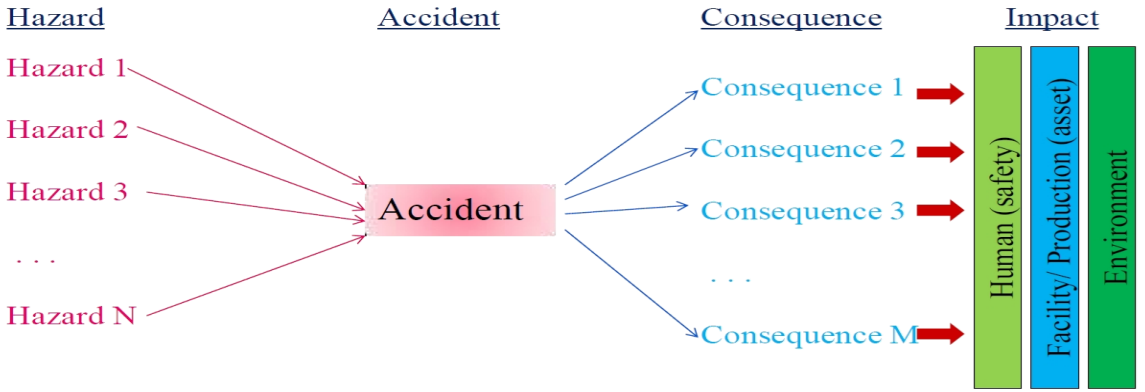
Refer : Korea Institute of Information Security and Cryptology, Artificial Intelligence for Autonomous Ship: Potential Cyber Threats and Security (Yoo, Ji-Woon, 2022년)

II. Cyber Risk on Ships

선박 리스크평가 엔지니어링(Risk Assessment Engineering)

FSA(Formal Safety Assessment) – IMO에서 개발한 선박 및 해양구조물과 같은 해양시스템을 위한 안전성평가 방법론으로 인명, 해상환경 및 재산보호를 포함하여 해상의 안전향상을 기하기 위한, 리스크와 비용-이익평가를 사용한 조직적이고 체계적인 안전평가 방법 (2001년 MSC 74차 회의에서 'FSA Guideline' 채택)





위험도 (Risk)* = 빈도 (Frequency) X 결과 (Consequence)

*위험도는 단위 시간당 손실로 표현됨 (인명, 재산, 환경, 명성)

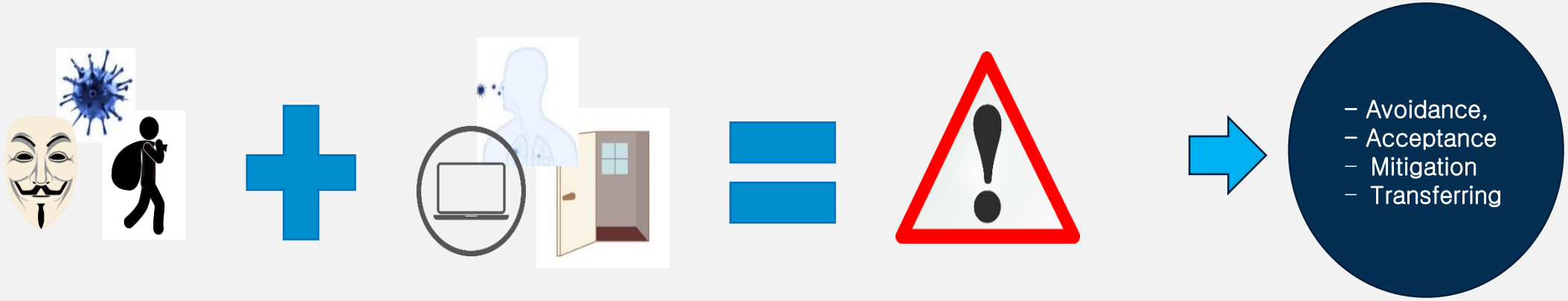
III

Risk Assessment for Ship Cybersecurity

III. Risk Assessment for Ship Cybersecurity

Cyber Risk Management

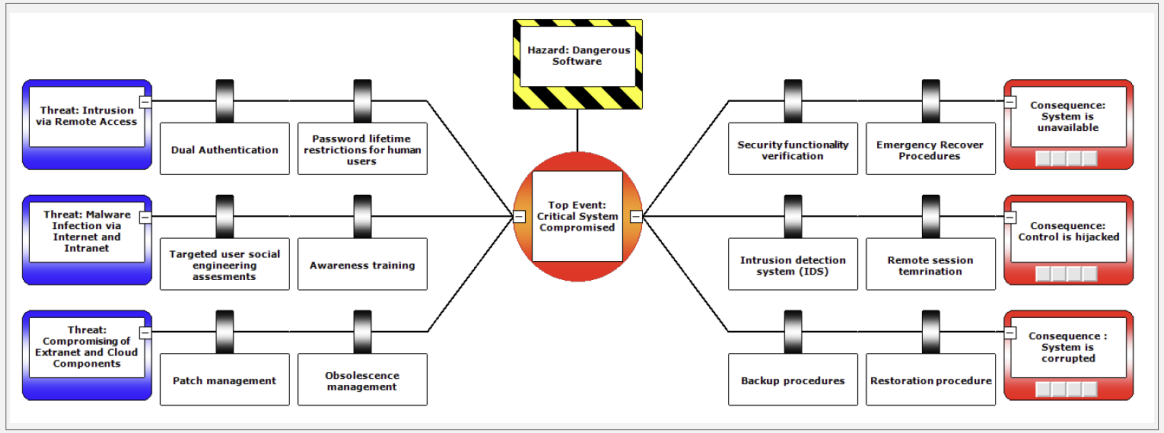
cyber risk management means the process of identifying, analysing, assessing, and communicating a cyber-related risk and accepting, avoiding, transferring, or mitigating it to an acceptable level, considering costs and benefits of actions taken to stakeholders. (refer : IMO MSC-FAL.1/Circ.3, Guidenlines on Maritime cyber risk management)



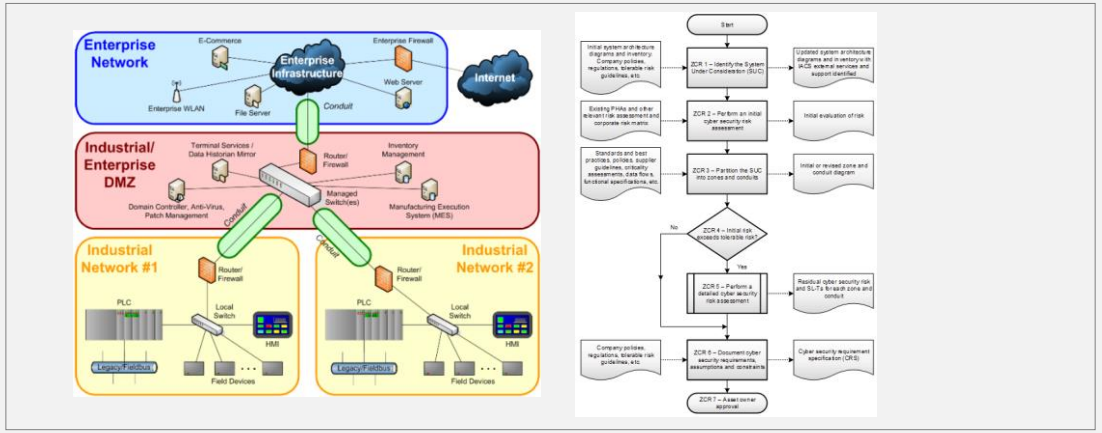
Threat **Vulnerability** **Risk**

III. Risk Assessment for Ship Cybersecurity

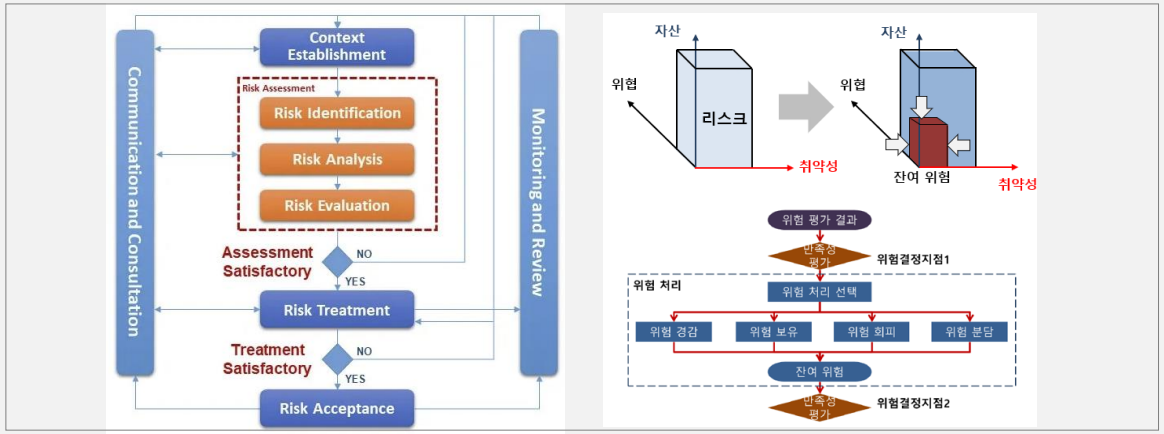
Cyber Risk Assessment Methodology



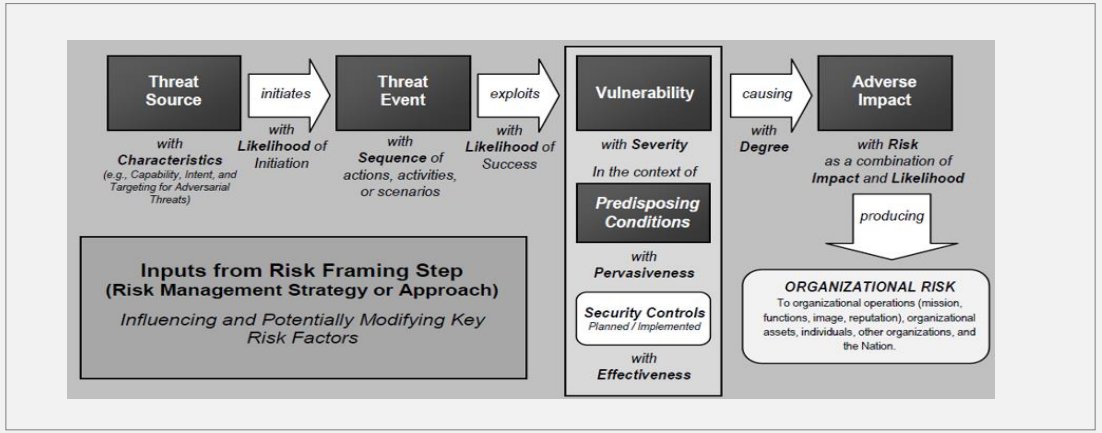
Bow-Tie Method



IEC 62443 3-2 'ICS Risk Assessment'

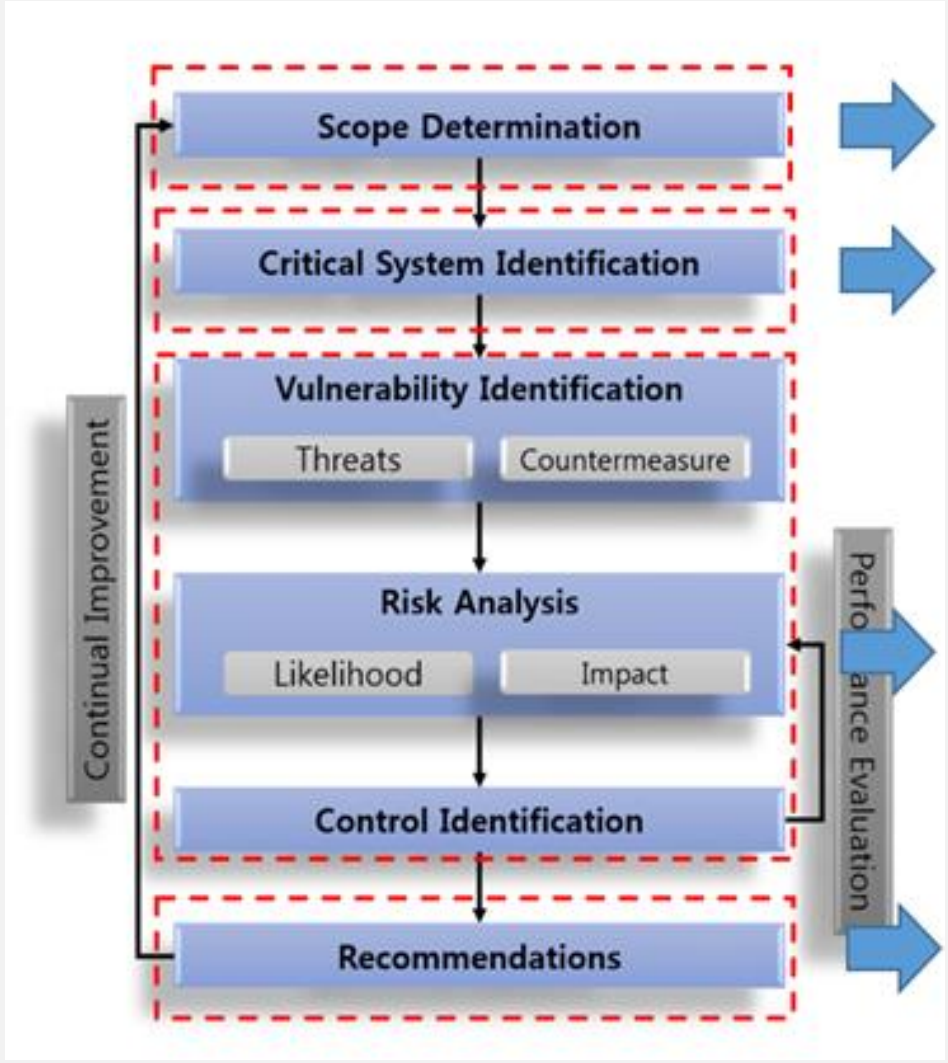


ISO 27005 'Information Security Risk Management'

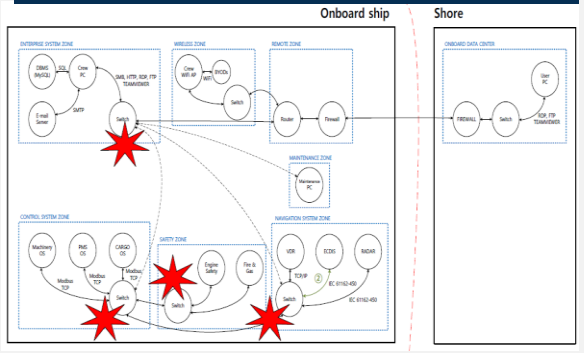


NIST SP 800-30 'Guide for Conducting Risk Assessments'

III. Risk Assessment for Ship Cybersecurity



Data Flow Diagram

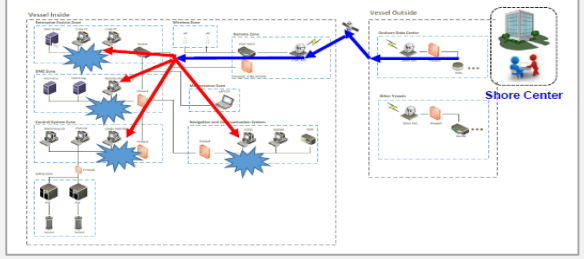


Cyber threat identification

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

Threat	Cause	Agent	Consequence
Malware	Remote update and maintenance	External	System malfunction / network infection



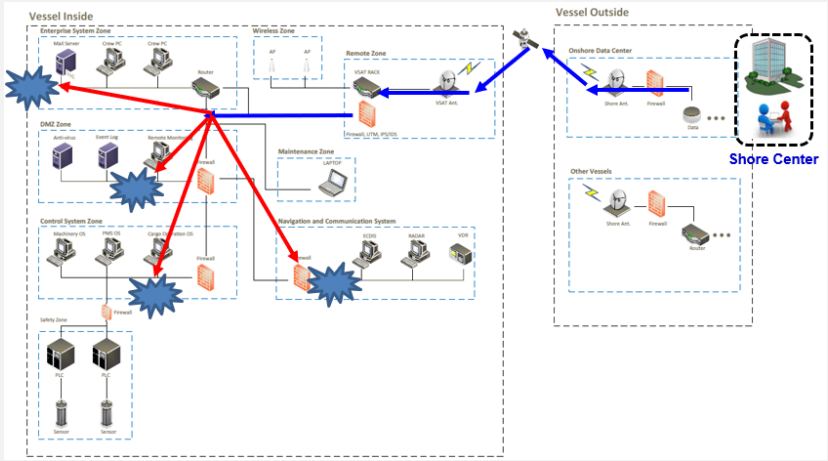
Identify cyber attack scenarios

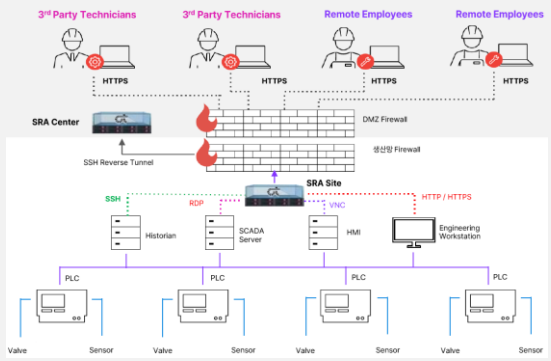
Risk analysis and improvement suggestions

III. Risk Assessment for Ship Cybersecurity

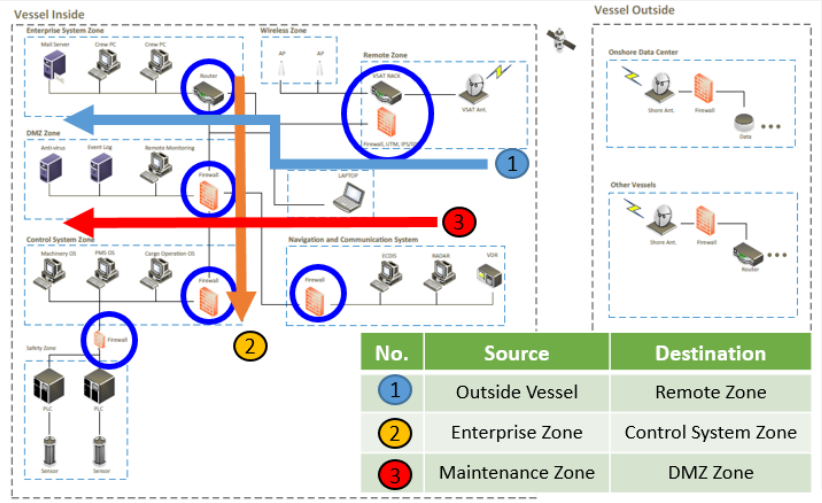
Verification of ship cyber risk management framework

Ship cyber attack scenarios and measures (e.g. remote maintenance)



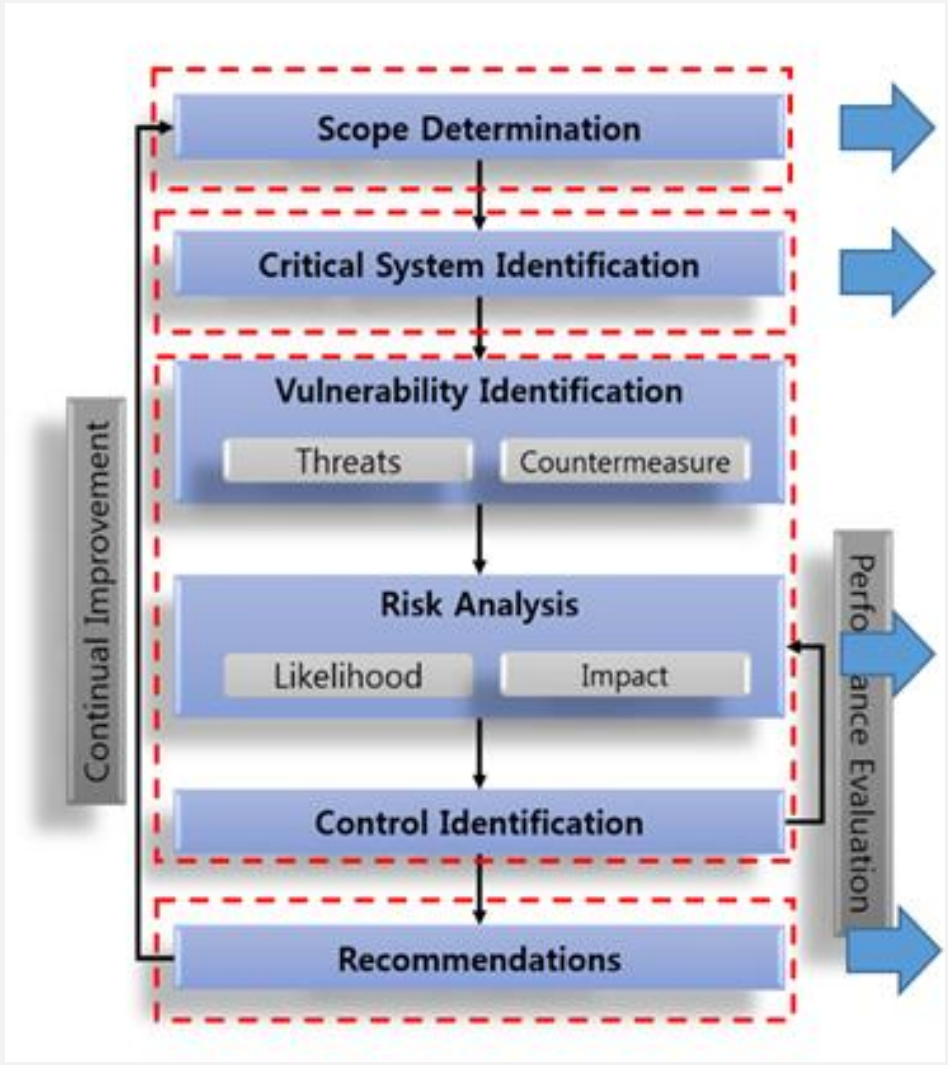


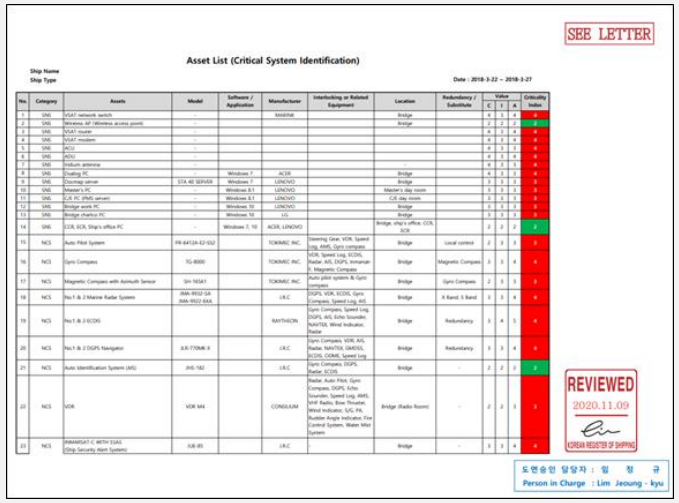
Perform tool-based ship penetration testing (MITER ATT@CK)

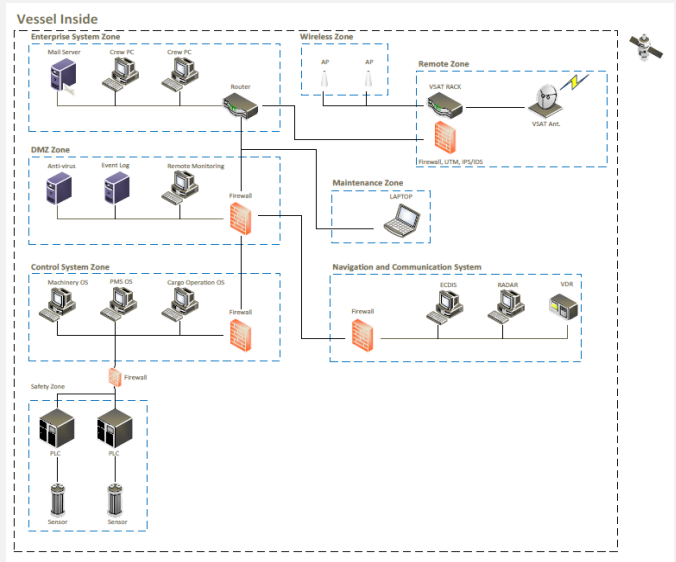


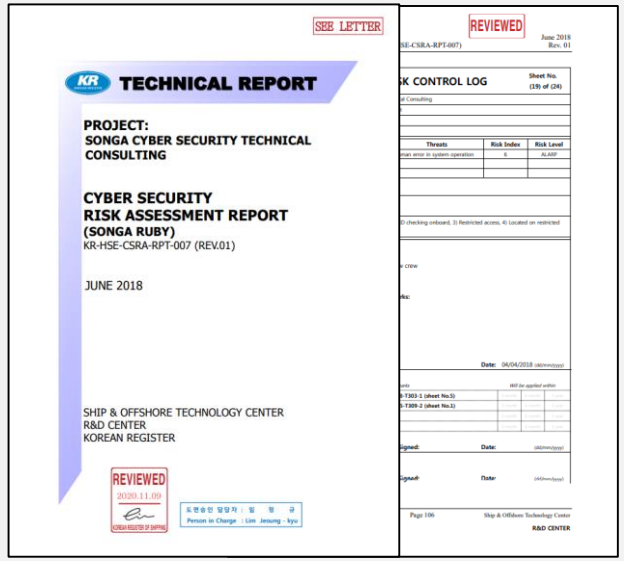
No.	Source	Destination
1	Outside Vessel	Remote Zone
2	Enterprise Zone	Control System Zone
3	Maintenance Zone	DMZ Zone

III. Risk Assessment for Ship Cybersecurity

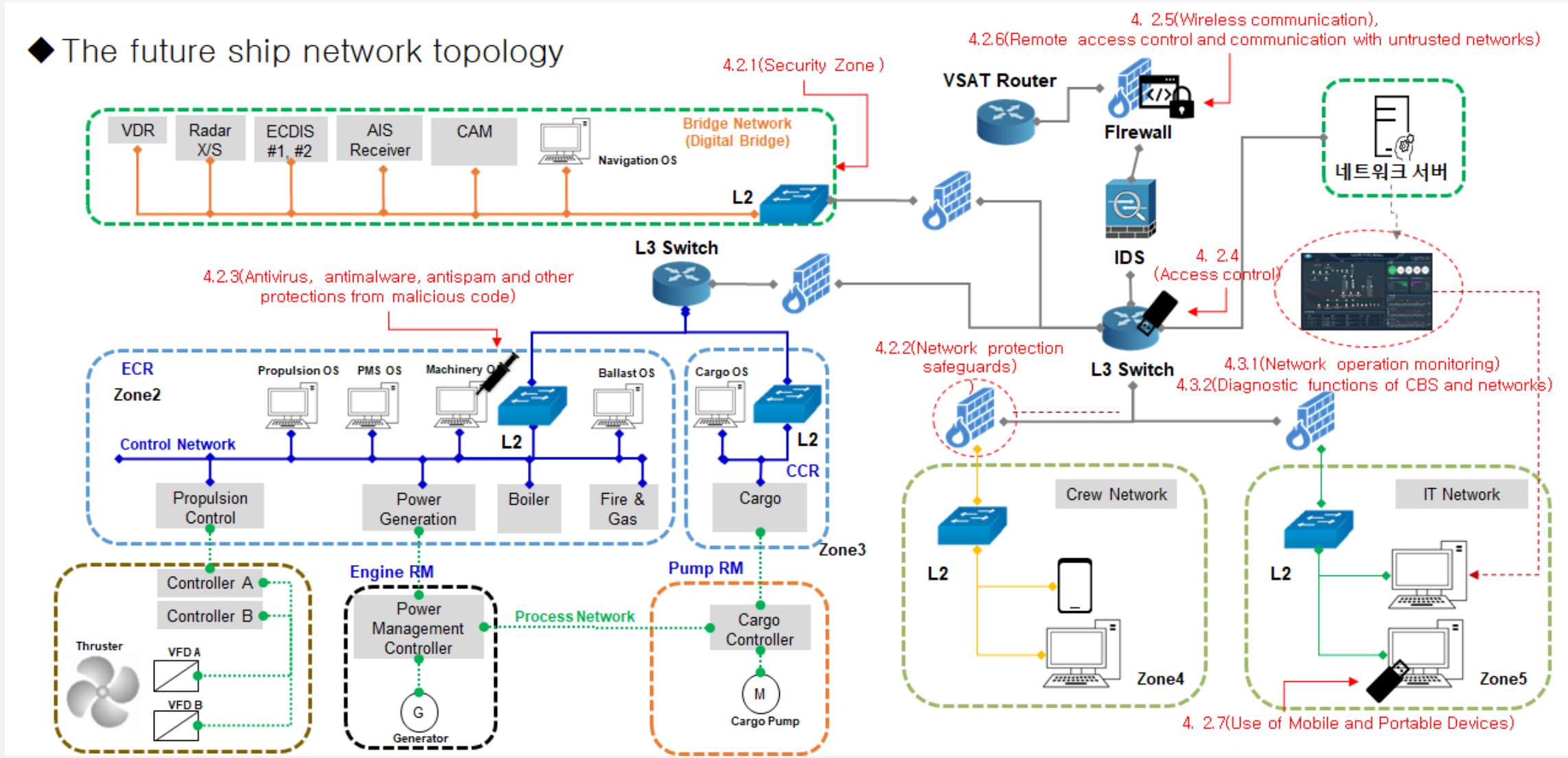






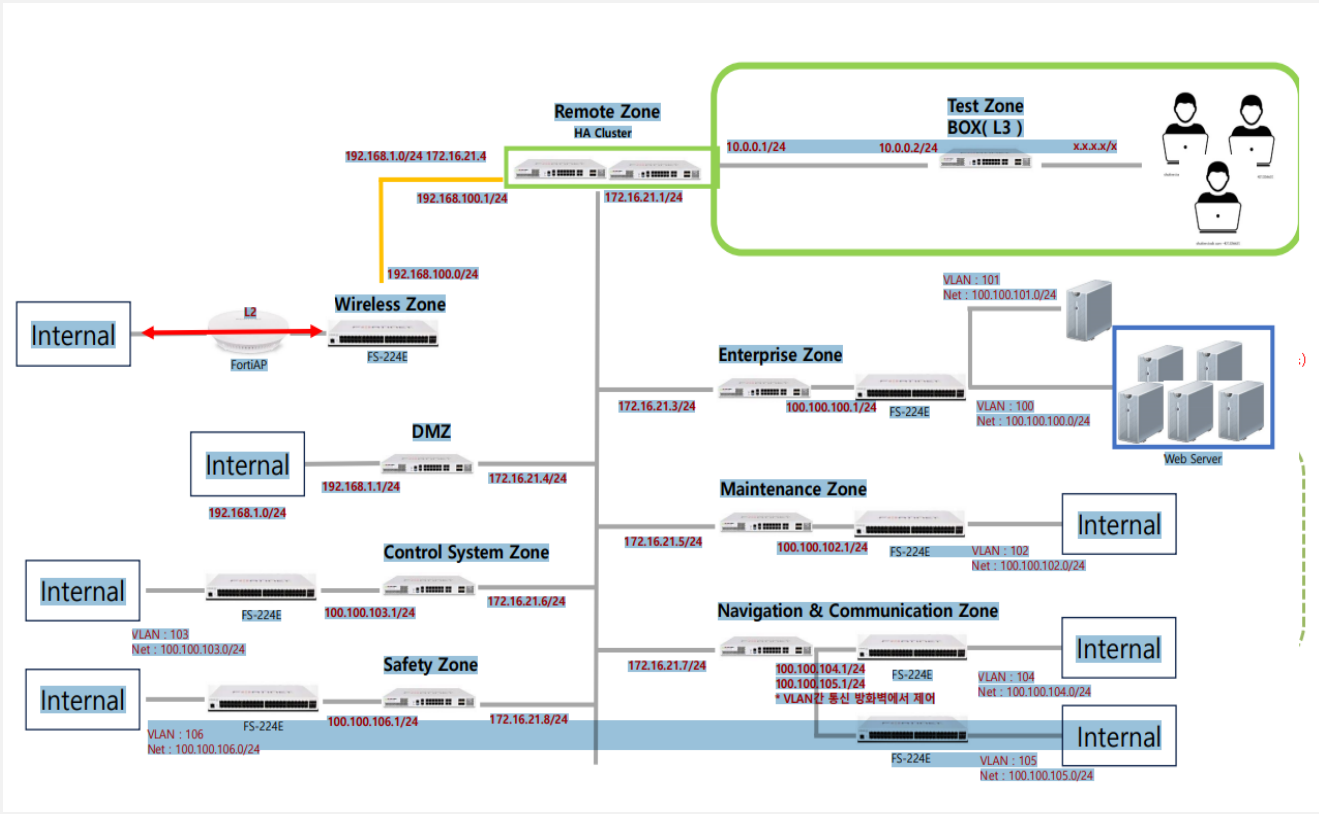


III. Risk Assessment for Ship Cybersecurity



III. Risk Assessment for Ship Cybersecurity

Test Bed



감사합니다

Thank you

Contact

ADD • 36, Myeongji ocean city 9-ro, Gangseo-gu, Busan 46762 Republic of Korea

E-mail • kaemyoung@krs.co.kr