Journal of the Korean Society of Marine Environment & Safety
Research Paper
Vol. 30, No. 3, pp. 263-274, May 31, 2024, ISSN 1229-3431(Print) / ISSN 2287-3341(Online) https://doi.org/10.7837/kosomes.2024.30.3.263

Cyber Threat and Vulnerability Analysis-based Risk Assessment for Smart Ship

Jeoungkyu Lim* · Yunja Yoo**†

* Senior Researcher, Cyber Certification Team, Korean Register, Busan 46762, Korea
** Professor, Division of Navigation Convergence Studies, Korea Maritime and Ocean University, Busan 49112, Korea

Abstract : *The digitization of ship environments has increased the risk of cyberattacks on ships. The smartization and automation of ships are also likely to result in cyber threats. The International Maritime Organization (IMO) has discussed the establishment of regulations at the autonomous level and has revised existing agreements by dividing autonomous ships into four stages, where stages 1 and 2 are for sailors who are boarding ships while stages 3 and 4 are for those not boarding ships. In this study, the level of a smart ship was classified into LEVELs (LVs) 1 to 3 based on the autonomous levels specified by the IMO. Furthermore, a risk assessment for smart ships at various LVs in different risk scenarios was conducted The cyber threats and vulnerabilities of smart ships were analyzed by dividing them into administrative, physical, and technical security; and mitigation measures for each security area were derived. A total of 22 cyber threats were identified for the cyber asset (target system). We inferred that the higher the level of a smart ship, the greater the hyper connectivity and the remote access to operational technology systems; consequently, the greater the attack surface. Therefore, it is necessary to apply mitigation measures using technical security controls in environments with high-level smart ships.*

Key Words : *Risk assessment, Cyber asset, Cyber threat, Vulnerability analysis, Smart ship*

1. Introduction

The International Maritime Organization (IMO) initiated discussions on Maritime Autonomous Surface Ships (MASS), which are representative digitalized ships, at the 99th Maritime Safety Committee (MSC) in 2018. It conducted a regulatory scoping exercise (RSE) for autonomous ships and submitted the necessary MSC reports (IMO, 2018a). The MSC has defined the autonomy rating of MASS in four stages − in stages 1 and 2, sailors board ships, and in stages 3 and 4, they do not board − and discussed the regulatory scope and MASS code of each autonomous level. In addition, recognizing the need for cybersecurity owing to the introduction and operation of these digitized ships, the IMO has presented the Guidelines on Maritime Cyber Risk Management in 2017 and recommended that ships use safety management systems (SMSs) to manage potential cyber risks from January 1, 2021 (IMO, 2017).

Supporting the industry-wide efforts of the IMO to manage maritime cyber risks, shipowners such as BIMCO and others (BIMCO et al., 2020) developed guidelines on using cyber security onboard ships for protecting ships and cyber assets against cyber threats. They also divided the cyber risk management approach into the following stages: identify threats, identify vulnerabilities, assess risk exposure, develop protection and detection measures, establish response plans, and respond to and recover from cyber security incidents, as illustrated in Figure 1 (BIMCO et al., 2020).

The Oil Companies International Maritime Forum (OCIMF) requires compliance with Tanker Management and Self-Assessment (TMSA), a safety management evaluation standard, for checking the cybersecurity management capabilities of tanker ship operators (need to be modified). Several classification societies have also presented guidelines related to cybersecurity (ABS, 2016; BV, 2018; DNV-GL, 2018; KR, 2017; NK, 2019; OCIMF, 2022). Cyber environments that can pose cyber risks in the ship sector

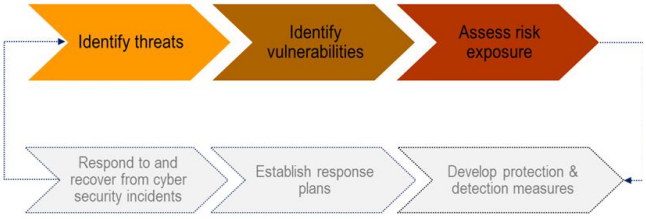

Fig. 1. Cyber risk management approach as set our in the guidelines by BIMCO and others (BIMCO et al., 2020).

* First Author: jklim@krs.co.kr
† Corresponding Author: yjyoo@kmou.ac.kr, 051-410-4286

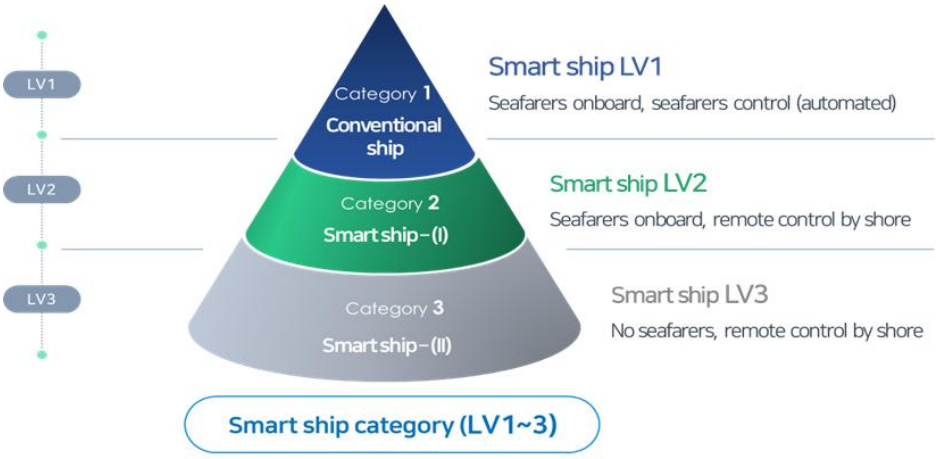

Fig. 2. Smart ship category LEVELs (LV) 1-3 obtained by applying the IMO autonomous-level classification adapted from (IMO, 2018a).

consist of information technology (IT) systems represented by network components, such as personal computers, laptops, tablet personal computers (PCs), and router switches; and operational technology (OT) systems represented by gyrocompasses, Electronic Chart Display and Information Systems (ECDISs), and navigation-related sensors (BIMCO et al., 2020). An increased expansion of cyberspace against cyberattacks is expected at the second and third stages of autonomous LEVELs (LVs), where remote control functions are applied when introducing and operating autonomous ships, and cyber risks are expected to increase (BSI, 2022; ENISA, 2023).

In 2020, the Korean government began an autonomous ship technology development project and plans to develop technologies that include demonstrations and operations by 2025. As a part of existing developments in cybersecurity technology, ship network security equipment technology can be applied in the third stage of autonomous ships (KASS, 2023). Regarding MASS ships at autonomous LVs 2 and 3, they will be operated through remote control centers on shore. Vulnerability analysis is required for cyber risks at the autonomous level, monitoring technology is needed for the cyber threats facing smart ships, and cyberattack response training is required for remote operators. In addition, it is necessary to perform vulnerability analysis through cyber risk assessment as well as present and apply mitigation measures to the derived cyber risk areas (DCSA, 2020; ENISA 2020; IAPH, 2021).

In this study, the "identify threats" and "identity vulnerabilities" steps of the cyber risk management approach of BIMCO et al. (2020) were performed to analyze the cyber threats and vulnerabilities of a smart ship, which is a shipping concept in which smart technologies such as sensor fusion technology or partial-autonomous operation technology are applied to a conventional physical-ship (BIMCO et al., 2020). In addition, migration measures were proposed based on the results of the vulnerability analysis according to smart ship LVs 1 to 3; the smart ship levels were divided into LVs 1-3 by applying the concept followed by the IMO in classifying autonomous ships (IMO, 2018a; Issa et al., 2022). In smart ship LV1, some automation is applied to the ship, and seafarers board and operate it. Regarding smart ship LV2, on-land control is performed by onboard seafarers, and the ship is operated remotely by seafarers onshore in the event of an emergency. Finally, for smart ship LV3, ship operations are controlled on land without any crew members on board. The concepts and classifications of smart ship LVs 1-3 are shown in Figure 2.

Section 2 defines the methodology used for performing the risk assessment of a smart ship and provides a detailed step-by-step description of the risk assessment procedure and associated terms. Then, section 3 presents the existing scope of cyber assets, cyber threats, vulnerability analyses, and mitigation measures. Finally, section 4 summarizes the key findings and discusses the inferences made from this study as well as the limitations and future research.

2. Methodology

Risk assessment for a smart ship is performed using the procedure shown in Figure 3. First, the target systems (cyber asset) that potentially pose a threat to cybersecurity in the smart ship category are identified, and the impact and likelihood indices are identified accordingly. An initial risk assessment (inherent risk) is performed, and the calculated risk index is compared with the

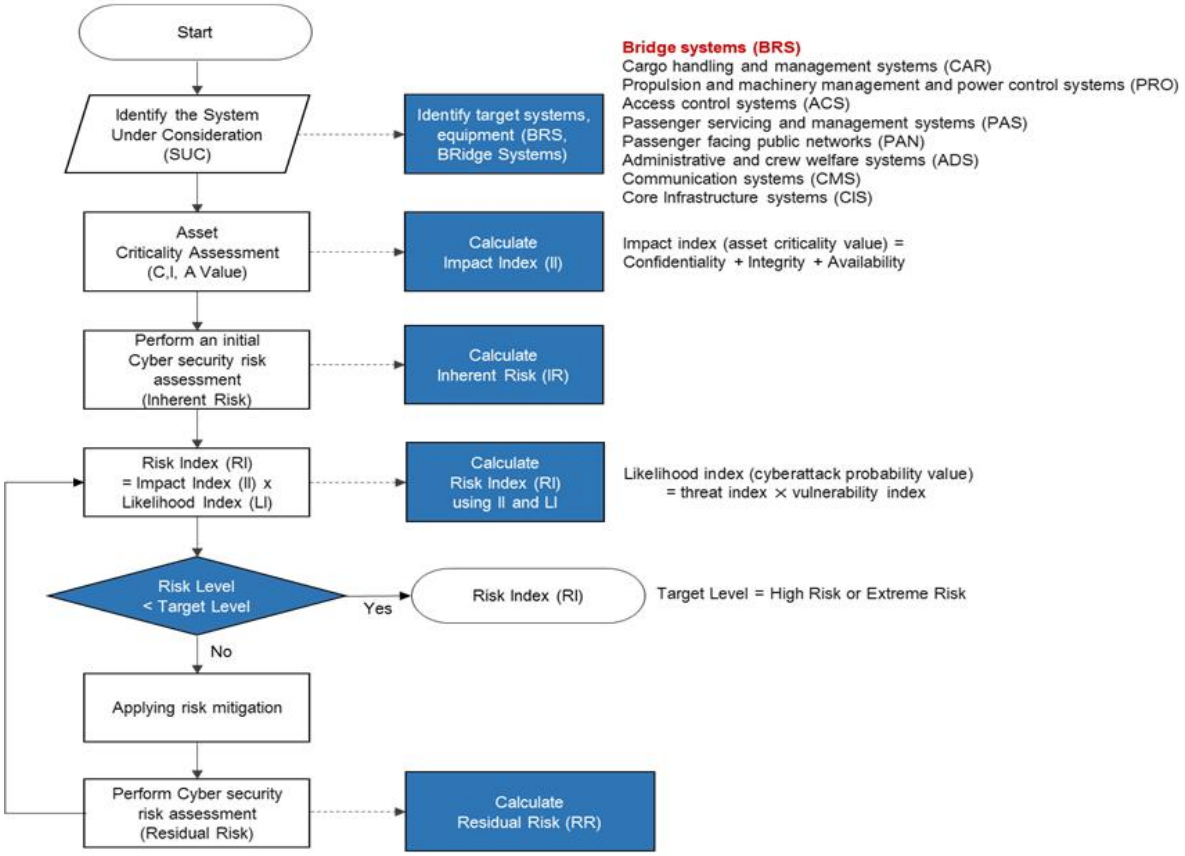

Fig. 3. Methodology for risk assessment.

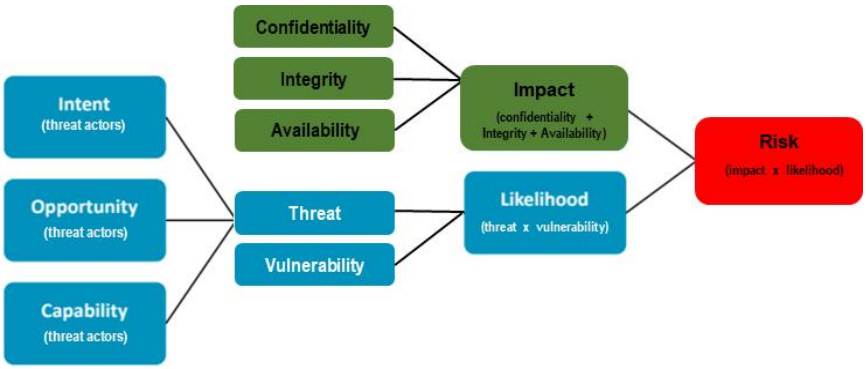

Fig. 4. Relationship between the factors influencing risk, adapted from (BIMCO et al., 2020).

target level. If the risk index exceeds the threshold, the necessary mitigation measures are applied, and risk assessment is re-performed to assess the residual risk.

Cybersecurity threats include the intentions, opportunities, and capabilities of threat actors. These threats and vulnerabilities determine the frequency of cyber risk occurrence (likelihood) in risk assessment. The risk assessment is performed according to the degree to which cyber risk affects confidence, integrity, and availability, which are the three elements of security. Finally, risk assessment is quantitatively analyzed using a risk matrix based on the impact and likelihood of cyber risk (BIMCO et al., 2020; ISO/IEC, 2018; Yoo and Park, 2021). Yoo and Park (2021) categorized risk components into administrative, technical, and physical security areas and identified the risk level with vulnerability improvement priorities. In this study, risk mitigation measures based on smart ship levels (LVs 1-3) were classified into

administrative, technical, and physical security areas, and a network configuration plan for strengthening ship cyber-resilience was presented based on the IACS UR E26, which will be enforced from July 2024 (IACS, 2022). The relationships between the factors influencing cyber risk are shown in Figure 4.

The cyber risk impact of the SMS of a ship is determined by confidence, integrity, and availability; and it is divided into five stages: critical, significant, moderate, minor, and negligible. A detailed description of these stages is presented in Table 1. In addition, cyber risk likelihood is determined by threat and vulnerability indicators. Regarding the threat index, it is divided into five stages: definite, probable, occasional, remote, and improbable, while the vulnerability index is divided into five stages: very high, high, medium, low, and very low; these indices are detailed in Table 2.

Finally, the risk matrix for performing cyber risk analysis is quantitatively analyzed by scoring the detailed steps of frequency and influence, normalizing the score according to the risk from 1 to 5, as shown in Figure 5. The risk level, according to the risk score, is divided into low risk for 1-5, medium risk for 6-10, high risk for 11-19, and extreme risk for 20 points. The risk levels and descriptions according to the risk values are listed in Table 3.

The risk matrix is divided into three risk regions as defined below.

- Intolerable risk level (red area in Figure 5): It contains risk indices $\geq$ 20.0. This level of risk exposes the system to intolerable losses in terms of human lives, assets, and the environment. No hazard in this region is acceptable; thus, any hazard located here should be eliminated, or its level of risk should be reduced immediately through appropriate security

Table 1. Impact level and description from SMS, adapted from (BIMCO et al., 2020; DCSA, 2020)

*Impact index		Descriptor	Definition
Confidentiality	5	critical	Unauthorized disclosure could result in critical risks to human lives, assets, and the environment Critical financial losses, very long-term business interruptions/expenses, possibility of fatalities
	4	significant	Significant financial losses, long-term business interruptions/expenses, permanent physical injuries
	3	moderate	Unauthorized disclosure could result in moderate risk to human lives, assets, and the environment Moderate financial losses, medium-term business interruptions/expenses, short-term injuries
	2	minor	Minor financial losses, short-term business interruptions/expenses, first-aid type injuries
	1	negligible	Unauthorized disclosure would not pose a risk to human lives, assets, or the environment Negligible financial losses, very short-term business interruptions/expenses
Integrity	5	critical	Unauthorized disclosure could result in critical risks to human lives, assets, and the environment Critical financial losses, very long-term business interruptions/expenses, possibility of fatalities
	4	significant	Significant financial losses, long-term business interruptions/expenses, permanent physical injuries
	3	moderate	Unauthorized disclosure could result in moderate risks to human lives, assets, and the environment Moderate financial losses, medium-term business interruptions/expenses, short-term injuries
	2	minor	Minor financial losses, short-term business interruptions/expenses, first-aid type injuries
	1	negligible	Unauthorized disclosure would not pose a risk to human lives, assets, and the environment Negligible financial losses, very short-term business interruptions/expenses
Availability	5	critical	Unavailability (15 min) could result in critical risks to human lives, assets, and the environment Critical financial losses, very long-term business interruptions/expenses, possibility of fatalities
	4	significant	Unavailability (1 h) could result in significant risks to human lives, assets, and the environment Significant financial losses, long-term business interruptions/expenses, permanent physical injuries
	3	moderate	Unavailability (6 h) could result in moderate risks to human lives, assets, and the environment Moderate financial losses, medium-term business interruptions/expenses, short-term injuries
	2	minor	Unavailability (1 day) could result in minor risks to human lives, assets, and the environment Minor financial losses, short-term business interruptions/expenses, first-aid type injuries
	1	negligible	Unavailability (1 week) would not pose a risk to human lives, assets, and the environment Negligible financial losses, very short-term business interruptions/expenses
	1	definite	3 impact index 4
	2	probable	5 impact index 6
	3	occasional	7 impact index 9
	4	remote	10 impact index 12
	5	improbable	13 impact index 15

*Impact index (asset criticality value) = confidentiality + integrity + availability

Table 2. Likelihood scale and description from the SMS of a ship, adapted from (NIST, 2012)

*Likelihood index		Descriptor	Definition
Threat index	5	definite	The subject asset or similar assets are targeted or attacked on a frequently recurring basis (e.g., 1 event per week)
	4	probable	A credible threat exists against the asset (e.g., 1 event per month)
	3	occasional	There is a possible threat to the asset (e.g., 1 event per year)
	2	remote	There is a low threat against the asset (e.g., 1 event in 10 years of operation)
	1	improbable	There is no history of actual or planned threats (e.g., no expected attack in the life of the vessel operation)
Vulnerability index	5	very high	There are ineffective security measures currently in place; so, the adversary would easily be able to succeed
	4	high	There are some security measures, but there is no complete and effective application; so, an attack could succeed relatively easily
	3	medium	Although there are some effective security measures in place, they could still be compromised
	2	low	There are effective security measures in place; however, there is potentially at least one weakness
	1	very low	Multiple layers of effective security measures exist
	1	definite	1 likelihood index 5
	2	probable	6 likelihood index 10
	3	occasional	11 likelihood index 15
	4	remote	16 likelihood index 19
	5	improbable	20 likelihood index 25

*likelihood index (cyberattack probability value) = threat index × vulnerability index.

Table 3. Normalized risk value and risk level, adapted from (ISO, 2022)

Risk value	Risk level	Definition
1-5	Low risk	Once the risk materializes, there is almost no impact on the system onboard the ship; it can be overcome by simple measures. E.g., an onboard office computer error.
6-10	Medium risk	Once the risk materializes, there is a slight impact, not on the system onboard the ship but on the economy or production and business. E.g., a ship equipment error.
11-19	High risk	Once the risk materializes, there is a severe impact, not on the system onboard the ship but on the economy or society.
20-25	Extreme risk	Once the risk materializes, there is a very severe impact, not on the system onboard the ship but on the economy or society. E.g., a major ship accident, which causes serious damage to the reputation of the associated company and creates a terrible influence on society.

actions.

- Manageable (or as low as reasonably practicable (ALARP)) risk level (yellow and orange areas in Figure 5). It contains risk indices ranging from 6.0 to 19.0. In principle, all hazards in this region have acceptable risk levels, but this level of risk should be mitigated by administrative, physical, and technical security controls that can be practically applied. When the level of risk cannot be further reduced without additional expenditure, the person responsible for the project should make a decision on its implementation based on the ALARP principle.
- Negligible risk level (green area in Figure 5). It contains risk indices ≤ 5.0. This level of risk is low enough to be ignored. Any hazard in this region is widely acceptable, and further security actions for risk reduction are not necessary.

A risk is defined as a combination of the frequency of a hazard (or hazardous event) and the severity of its consequences. For risk prioritization or ranking, a risk index can be determined as the product of the impact and likelihood indices.

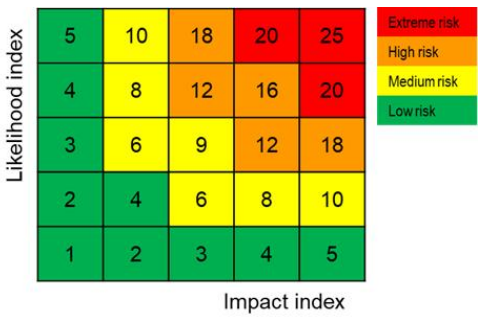

Fig. 5. Example risk matrix of a ship company for risk assets, adapted from (BIMCO et al., 2020).

Risk index (RI) = impact index (II) × likelihood index (LI)

Relevant risk indices are assigned to all the identified hazards or hazardous events, and the risk levels of each hazard or hazardous event can be prioritized. The risk level can be classified into four stages according to the risk matrix shown in Figure 5; the normalized risk values and risk levels are listed in Table 3.

3. Results of Risk Assessment

This section discusses the HAZard IDentification (HAZID)-based risk assessment that was performed according to the smart ship LVs (1,2,3) (IMO, 2018b; ISO/IEC, 2018), based on the methodology described in section 2. The vulnerability factor and inheritance risk were calculated with respect to the cyber assets (section 3.1) and cyber threats (section 3.2), and the mitigation measures and categories were determined as well. It was confirmed that the risk value and mitigation category varied depending on the LVs of a ship (1, 2, 3).

3.1 Cyber Assets

The International Association of Classification Societies (IACS) Unified Requirement (UR) E26 defines cyber assets as computer-based systems (CBSs), which are programmable or interoperable sets of electronic devices configured to achieve one or more specified purposes, such as collecting, processing, maintaining, using, sharing, disseminating, or disposing information. Onboard CBSs include IT and OT systems(IACS, 2022). Table 4 lists the various categories of cyber assets associated with ships(IMO, 2017): bridge systems (BRS), cargo handling and management systems (CAR), propulsion and machinery management and power control systems (PRO), access control

Table 4. Target systems and equipment for risk assessment, adapted from (IMO, 2017; BIMCO et al., 2020)

Category	Systems and equipment
Bridge systems (BRS)	Integrated navigation system (INS)
	Position reference system (e.g., GPS)
	Electronic Chart Display Information System (ECDIS)
	Systems that interface with electronic navigation systems and propulsion/maneuvering systems
	Automatic identification system (AIS)
	Heading and gyro system
	Radar equipment (X- and S-band radars)
	Auto pilot
	Bridge navigation and watch alarm system (BNWAS)
	Voyage data recorder (VDR)
Cargo handling and management systems (CAR)	Cargo Control Room (CCR) and its equipment
	Cargo level, pressure, and temperature monitoring and alarm system
	Cargo tank and other cargo-related safety systems
	Inert gas control and monitoring system
	Loading and offloading control and monitoring system
	Local and remote control, monitoring, and alarm systems for cargo pumps, valves
	Remote cargo and container tracking and sensing systems
Propulsion and machinery management and power control systems (PRO)	Power management system
	Integrated control system
	Power source safety system
	Electrical circuit protection system
	Emissions monitoring
	Heating, ventilation, and air-conditioning monitoring
Access control systems (ACS)	Surveillance systems such as closed-circuit television (CCTV) networks
	Electronic “personnel-on-board” systems
Passenger servicing and management systems (PAS)	Property management system (PMS)
	Ventilation and climate control system
	Emergency safety/response system
	Flooding detection system
	Ship-management systems (often including electronic health records)
	Ship passenger/visitor/seafarer boarding access systems
	Infrastructure support systems like domain naming system (DNS) and user authentication/authorization systems
Passenger facing public networks (PAN)	Passenger Wi-Fi or local area network (LAN) internet access (e.g., onboard personnel can connect their own devices
Administrative and crew welfare systems (ADS)	Administrative systems
	Wi-Fi or LAN internet access for the crew (e.g., onboard personnel can connect their own devices).
Communication systems (CMS)	Integrated communication systems (ICS)
	Satellite communication equipment
	Voice Over Internet Protocols (VOIP) equipment
	Wireless networks (WLANs)
	Public address and general alarm systems
	Global Maritime Distress and Safety System (GMDSS)
Core Infrastructure systems (CIS)	Firewalls
	Routers/switches
	Intrusion detection systems (IDS)
	Intrusion prevention systems (IPS)
	Security event logging systems

systems (ACS), passenger servicing and management systems (PAS), passenger facing public networks (PAN), administrative and crew welfare systems (ADS), communication systems (CMS), and core infrastructure systems (CIS). Notably, BIMCO et al. (2020) defined a detailed system that constituted a cyber asset. Bridge systems comprise integrated navigation and positioning systems such as Global Positioning System (GPS)(BIMCO et al., 2020).

3.2 Cyber Threats

Cyber threats are situations or events that may adversely affect the operation of an organization and its assets, individuals, other organizations, or countries through unauthorized access, destruction, disclosure, or modification of information(NIST, 2012). In this study, the target system for performing the risk assessment was a ship; the corresponding cyber threat categories are listed in Table 5 (BSI, 2022; IACS, 2021). Threat categories can be divided into nefarious activities/abuse, physical attacks, unintentional damage or errors leading to the loss of information or IT assets, and malfunctions/failures.

Table 5. Cyber threats of target systems (BSI, 2022; IACS, 2021)

Threat categories	Cyber threat, attack, or technique	Threat ID
Nefarious activities/ abuse	Brute force	THR-N-001
	Distributed denial-of-service (DDoS) attacks	THR-N-002
	Infiltration of malware via removal of media and mobile systems	THR-N-003
	Unauthorized access	THR-N-004
	Manipulation of data	THR-N-005
	Social engineering and phishing	THR-N-006
	Spoofing	THR-N-007
	Targeted attacks	THR-N-008
	Intrusion via remote access	THR-N-009
	Network manipulation and information gathering	THR-N-010
	Compromising extranet and cloud components	THR-N-011
Physical attacks	Sabotage	THR-P-001
	Unauthorized physical access/ unauthorized entry to premises	THR-P-002
Unintentional damage or errors leading to loss of information or IT assets	Erroneous use or administration of devices and systems	THR-U-001
	Erroneous penetration testing	THR-U-002
	Use of unreliable source	THR-U-003
	Deletion/change of data in an information system	THR-U-004
	Inadequate design and planning or improper adaptation	THR-U-005
	Third party security failure	THR-U-006
	Information leakage	THR-U-007
Malfunctions /failures	Technical failure and force majeure	THR-M-001
	Vulnerabilities of systems or devices	THR-M-002

3.3 Vulnerability Analysis and Mitigation Measures

Vulnerability refers to a weakness in the function of a cyber asset, procedure, internal control, or implementation that can be exploited or triggered by a threat source. This weakness is either been intentionally incorporated into the design of some computer components or accidently inserted at any time during the life cycle of the computer(IEC, 2020). Different threats and vulnerabilities have different impacts on assets, often classified in terms of the loss of confidentiality, integrity, or availability(ISO&IEC, 2013). Cyber risk is determined by the vulnerabilities of cyber assets (section 3.1) and cyber threats (section 3.2). Specifically, if the vulnerabilities within cyber assets are removed, the cyber risk will be low, and vice versa. In this study, high-risk and extreme-risk results according to smart ship LVs (1,2,3) were derived, as shown in Table 6(Antonopoulos et al., 2022; Charitos et al., 2022). The vulnerability factor and inheritance risk score were calculated according to cyber assets and cyber threats, and mitigation measures and categories were derived. The mitigation categories of administrative security, physical security, and technical security are discussed below.

Administrative security comprises procedures, policies, and personnel controls, including security policies, audits, training, technical training, performance evaluations, user access control, supervision, recruiting and termination procedures, contingency, disaster recovery, and emergency plans. These actions ensure that authorized users know and understand how to use a system correctly to maintain data security. Physical security refers to the measures and practices implemented to protect physical assets, facilities, and resources from unauthorized access, damage, theft, or harm. This encompasses the design, implementation, and management of physical security controls and safeguards to ensure the safety and security of both physical assets and people. Technical security refers to the set of measures and practices implemented to protect the confidentiality, integrity, and availability of information and technological assets within an organization. It encompasses the use of technical controls and safeguards to secure information systems, networks, devices, and software from unauthorized access, unauthorized use, and other security risks. These measures include access controls, encryption, firewalls, intrusion detection and prevention systems (IDPS), antiviral

Table 6. Results of risk assessment (high risk and extreme risk) and mitigation measures.

Ship CAT. (LV.)	System CAT.	Shore remote access	Vulnerability factor	Threat ID	Risk score	Mitigation measures	Mitigation category
Conventional ship (LV1)	BRS	No	Crew	THR-N-003	20	Create awareness and perform training	(A)
	BRS	No	3rd Party	THR-U-006	16	Establish a CSMS	(A)
	ADS	Yes	Crew	THR-N-006	12	Establish a CSMS	(A)
	BRS	No	Crew	THR-P-002	12	Use a port/LAN blocker	(P)
	BRS	No	3rd Party	THR-P-002	12	Use a port/LAN blocker	(P)
	ADS	Yes	Crew	THR-P-002	10	Perform firewall management	(T)
Smart ship-(I) (LV2)	BRS	Yes (Connected to an IT/OT system)	Network	THR-U-005	20	Improve the OT network architecture (VLAN)	(T)
	BRS		Network	THR-U-005	20	Install an OT firewall	(T)
	BRS		Network	THR-U-005	20	Locate the RAS in the DMZ	(T)
	PRO		System	THR-M-002	18	Perform regular patch updates from outside vendors	(T)
	PRO		System	THR-N-009	16	Use a VPN	(T)
	CIS		Crew	THR-N-003	16	Install a malware protection system	(T)
	BRS		Crew	THR-N-003	20	Create awareness and perform training	(A)
	BRS		3rd Party	THR-U-006	16	Establish a CSMS	(A)
	ADS		Crew	THR-N-006	12	Establish a CSMS	(A)
	BRS		Crew	THR-P-002	12	Use a port/LAN blocker	(P)
	BRS		3rd Party	THR-P-002	12	Use a port/LAN blocker	(P)
	ADS		Crew	THR-N-004	10	Perform firewall management	(T)
Smart ship-(II) (LV3)	CIS	Yes (Connected to an IT/OT system)	Network	THR-M-001	24	Install devices for network redundancy	(T)
	CIS		Network	THR-N-010	24	Implement an SIEM	(T)
	CIS		Network	THR-N-008	24	Honeynet	(T)
	CIS		Network	THR-N-005	24	Implement an (IT/OT) IDS	(T)
	CIS		Network	THR-N-009	24	Implement a remote access solution	(T)
	BRS		Network	THR-U-005	20	Improve the OT network architecture (VLAN)	(T)
	BRS		Network	THR-U-005	20	Install an OT firewall	(T)
	BRS		Network	THR-U-005	20	Locate the RAS in the DMZ	(T)
	PRO		System	THR-M-002	18	Perform Regular patch updates from outside vendors	(T)
	PRO		System	THR-N-009	16	Install a VPN	(T)
	CIS		Crew	THR-N-003	16	Implement a malware protection system	(T)
	ADS		Crew	THR-N-004	10	Perform firewall management	(T)

[1] (A): administrative security, (P): physical security, (T): technical security
[2] CSMS: Cyber Security Management System, [3] VLAN: virtual local area network
[4] VPN: virtual private network, [5] SIEM: security information and event management
[6] IDS: intrusion detection system, [7] RAS: remote access system
[8] VPN: virtual private network

software, security information and event management (SIEM) systems, patch management, network segmentation, and other technical controls. Technical security controls are designed to prevent, detect, respond to, and mitigate security incidents and threats to information and technological assets.

The lower the smart ship LV, the higher the risk index owing to the source. Smart ship LV1 only allows internet access to the business network of the crew, and there is no connection contact with the OT network. Therefore, humans (crew and 3rd party) are the most vulnerable. The mitigation measures for sailors are administrative security (A), such as raising awareness and

Table 7. Results of smart ship LV2 cyber risk areas and cyberattack scenarios

System CAT.	Negligible	ALARP	Intolerable	No. of cyber attack scenarios
BRS	50	14	7	71
CAR	15	5	2	22
PRO	24	8	4	36
ACS	8	3	1	12
PAN	12	2	1	15
ADS	10	2	3	15
CMS	2	1	1	4
CIS	24	15	5	44
Total	145	50	24	219

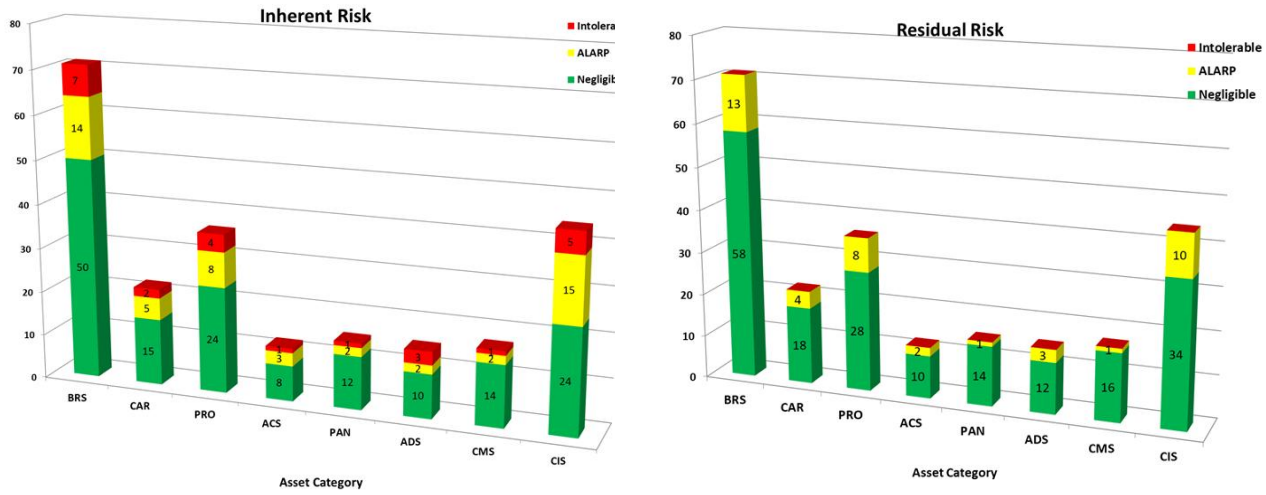

Fig. 6. Results of smart ship LV2 cyber risk levels (inherent and residual risk areas).

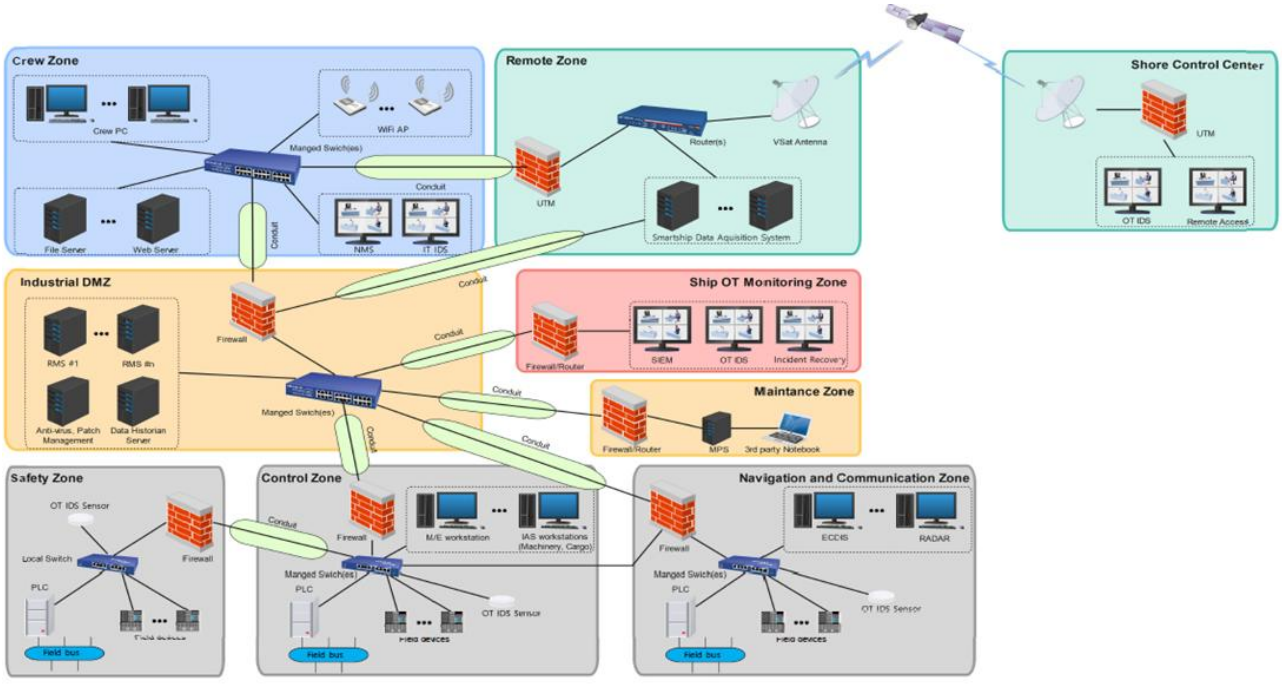

Fig. 7. Ship network configuration.

establishing cybersecurity policies and physical security (P) to prevent Universal Serial Bus (USB) use.

Smart ship LV2 is mounted by a source, and it supports remote access and land control. A solution for gathering OT data to monitor the status of smart ships in the land center is installed, which inevitably leads to a connection with the OT network. Owing to the remote connection with the land, the vulnerability factor (vulnerability) increases compared with that under LV1. Here, the network architecture is the most vulnerable factor, with vulnerable factors arising owing to onboarding humans (sailors and 3rd parties). The mitigation measure requires technical security (T) according to network architecture improvements (network separation, OT firewall installation, and demilitarized zone (DMZ) configuration), and administrative security (A) and physical security (P) are required to be the same as those in LV1(Issa et al., 2022). Vulnerability and related risks in track and field centers are important issues; however, they were excluded from consideration in this study.

Regarding smart ship LV3, it is not mounted by a source, and it is operated completely by remote control; therefore, network redundancy (devices such as switch, router, firewall) is required, and the importance of CIS assets increases. To defend against high-level hacker attacks, such as advanced persistent threat (APT) attacks, it is necessary to establish a control zone on ships (a variety of technical solutions, such as SIEM and Honeynet(Ananbeth et al., 2022; Guidetti et al., 2023), and the mitigation measure focuses on technical security (T). As the smart ship LV increases, the proportion of technical security increases, which entails the introduction and application of technical solutions. Therefore, the application of mitigation measures should consider cost-effectiveness.

Table 7 shows the risk areas according to each system category of smart ship LV2 (excluding PAS only for the passenger ships). In total, 219 risk scenarios were identified. Twenty-four scenarios (10.9%) belonged to the intolerable risk category, and 50 scenarios were identified as ALARP, and 145 scenarios were identified as negligible. Mitigation measures were identified to reduce the risk of ALARP and intolerable risks, and the decision to apply them was dependent on cost effectiveness. Figure 6 shows the inherent and residual risk areas for each system category.

Figure 7 shows a ship network configuration diagram reflecting the mitigation measures listed in Table 6 for a smart ship LV3. The criteria for constructing a zone conduit were obtained from IACS UR E26 (IACS, 2022). The network configuration consisted of a remote zone, crew zone, and safety zone, as well as a control zone and navigation and communication zone corresponding to the IT and OT areas. The industrial DMZ was configured between the IT and OT areas to ensure that remote centers, such as land, would not directly connect to the OT. The ship OT monitoring zone was configured to detect cyberattacks in real time; and SIEM, offset ratio and time interval-based intrusion detection system (OTIDS) (Antonopoulos et al., 2022; Raimondi et al., 2022), and incident recovery systems were installed. In addition, a zero-trust solution was applied to manage remote access more securely (NIST, 2020).

4. Discussion and Conclusions

The IMO has recognized the expansion of the cyberspace owing to the increasing digitalization of ship environments. Accordingly, it has divided the levels of digitalized ships such as autonomous ships into levels 1, 2, 3, and 4, which represent different degrees of automation. In this study, to analyze the cyber threats and vulnerabilities of smart ships, the categories of smart ships were divided into smart-ship LVs 1-3 based on the autonomous levels of autonomous ships according to the IMO, and the cyber risk assessment of smart ships was conducted at each level.

A HAZID-based risk assessment was performed. Risk indices was derived on the target systems (cyber asset) at each smart ship LV. The cyber threats on the target systems were divided into nefarious activity/ abuse, physical attacks, unintentional damage or errors leading to the loss of information or IT assets and malfunctions/ failures. A total of 22 cyber threats (11 for nefarious activity/ abuse, 2 for physical attacks, 7 for unintentional damage or errors, and 2 for malfunctions/ failures) were identified for the cyber assets. Furthermore, high risk (risk value: 11-19) and extreme risk (risk value: 20-25) were identified at each smart ship LV (6 for LV1, 12 for LV2 and LV3).

Cyber risks were calculated according to the smart ship LVs 1-3, and the mitigation measures were classified into three categories: administrative security, physical security, and technical security. In smart ship LV1, the vulnerability factor was the crew; for this, administrative security, which involved enhancing the awareness of the crew and establishing cybersecurity policies, was required. In smart ship LV2, the vulnerability factor was connected to the crew and land, and the higher the connectivity index, the more the technical security was required. Technical security, which involved improving the network architecture and administrative security and physical security, which were applied in LV2, were required as mitigation measures. Smart ship LV3 required a high level of technical security because fully remote control was required. In particular, the application of state-of-the-art security technologies, such as SIEM, Honeynet, IDS, and Zero Trust, was required to respond to APT attacks, and cost-benefit assistance was required to verify the applicability of technical security approaches.

The study had some limitations. For instance, the application of all the steps before formal safety assessment (FSA), including cost-benefit assessment, was excluded from the scope of this study; however, it will be considered in future work(IMO, 2018b). In addition, the HAZID-based risk assessment methodology applied in this research had a limitation in that the risk likelihood and impact potentially differed depending on the operation condition or environment, even if it was applied to smart ships with the same levels of automation. In the case of existing ships, cyber risk management is limited because it is difficult to change the OT system network and implement new cybersecurity functions;

however, by applying this methodology in the construction stage of new ships, it is possible to implement cyber-resilient networks and functions on ships considering security by design. Vulnerability diagnosis and penetration tests can be used to validate cyber resilience in cyber design security using this methodology. There is a practical limit to applying vulnerability diagnosis and penetration tests to actual ships. Therefore, verification through a ship simulation network testbed is underway; this will be considered in future work.

Acknowledgements

This work was supported by the Korea Maritime and Ocean University Research Fund in 2022.

References

[1] ABS(2016), Cybersecurity implementation for the marine and offshore industries. Vol. 2, American Bureau of Shipping, Houston, USA.

[2] Ananbeh, O., R. Alomari, and A. Daniell(2022), Improving ICS security through honeynets and machine learning techniques. Res Square 2022:1-5. https://doi.org/10.21203/rs.3.rs-1333285/v1

[3] Antonopoulos, M., G. Drainakis, E. Ouzounoglou, G. Papavassiliou, and A. Amditis(2022), Design and proof of concept of a predic-tion engine for decision support during cyber range attack simulations in the maritime domain, vol 2022 IEEE Interna-tional Conference on Cyber Security and Resilience (CSR):305-310. https://doi.org/10.1109/CSR54599.2022.9850280

[4] BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF, WSC (2020), The guidelines on cyber security onboard ships. Ver. 4, INTERCARGO.

[5] BSI(2022), Industrial control system security – Top 10 threats and countermeasures 2022.Ver. 1.5, Bundesamt für Sicherheit in Der Informationstechnik.

[6] BV(2018), Rules on cybersecurity for the classification of marine units. 2018 ed., Bureau Veritas.

[7] Charitos, E. D., N. A. Kounalakis, and I. Kantzavelou(2022), Cybersecurity at merchant shipping. 2022 IEEE International Confer-ence on Cyber Security and Resilience (CSR), IEEE:394-399. https://doi.org/10.1109/CSR54599.2022.9850294

[8] DCSA(2020), Implementation guide for cyber security on vessels. Ver. 1, Digital Container Shipping Association.

[9] DNV-GL(2018), Rules for classification: Ships - Sec. 21. Cyber security. 2018 ed., Det Norske Veritas-Germanischer Lloyd.

[10] ENISA(2020), Cyber risk management for ports. European Union Agency for Cybersecurity.

[11] ENISA(2023), Identifying emerging cyber security threats and challenges for 2030. European Union Agency for Cybersecurity.

[12] Guidetti, O. A., C. Speelman, and P. Bouhlas(2023), A review of cyber vigilance tasks for network defense. Front Neuroergonomics 2023(4):1104873. https://doi.org/10.3389/fnrgo.2023.1104873

[13] IACS(2021), Recommendation on incorporating cyber risk management into safety management systems. Rec. No. 171, International Association of Classification Societies.

[14] IACS(2022), Cyber resilience of ships. UR E26, International Association of Classification Societies.

[15] IAPH(2021), Cybersecurity guidelines for ports and port facilities. Ver. 1, International Association of Ports and Harbors.

[16] IEC(2020), Security risk assessment for system design. IEC 62443-3-2 edn. 1, International Electrotechnical Commission.

[17] IMO(2017), Guidelines on maritime cyber risk management. MSC-FAL.1/Circ.3 Annex. International Maritime Organization.

[18] IMO(2018a), Outcome of the regulatory scoping exercise (RSE) for the use of Maritime Autonomous Surface Ships (MASS) - Report of the correspondence group on MASS. MSC 100/5. International Maritime Organization.

[19] IMO(2018b), Revised guidelines for formal safety assessment (FSA) for use in the IMO rule-making process. MSC-MEPC.2/Circ.12/Rev.2, International Maritime Organization.

[20] ISO&IEC(2013), Information technology - Security techniques - Information security management systems - Requirements. ISO/IEC 27001 2nd edn, International Organization for Standardization & International Elec-trotechnical Commission.

[21] ISO(2022), Assessment of onboard cyber safety risk. ISO/TC8/WG4, vol N45; ISO 23799.

[22] ISO/IEC(2018), Information technology - Security techniques - Information security risk management. ISO/IEC 27005:2018.

[23] Issa, M., A. Ilinca, H. Ibrahim, and P. Rizk(2022), Maritime autonomous surface ships: Problems and challenges facing the regula-tory process. Sustainability 14(23):15630. https://doi.org/10.3390/su142315630

[24] KASS(2023), Korea autonomous surface ship (KASS) project. Availble via http://kassproject.org/en/info/projectdetail.php Accessed

10 Mar 2023.

[25] KR(2017), Guidelines of maritime cybersecurity. Ver. 1.0, Korean Register.

[26] NK(2019), Guidelines for designing cyber security onboard ships. Ver. 1, Nippon Kaiji Kyokai.

[27] NIST(2012), Guide for conducting risk assessments, 1st revision. National Institute of Standards and Technology: SP800-830.

[28] NIST(2020), Zero trust architecture. S.P.800-207, National Institute of Standards and Technology.

[29] OCIMF(2022), The Tanker management and self-assessment (TMSA). SIRE 2.0 Question Library Part 1, 7.5. Cyber security. Oil Companies International Marine Forum.

[30] Raimondi, M., G. Longo, A. Merlo, A. Armando, and E. Russo(2022), Training the maritime security operations centre teams. 2022 IEEE International Conference on Cyber Security and Resilience (CSR); IEEE 2022:388-393. https://doi.org/ 10.1109/ CSR54599.2022.9850324.

[31] Yoo, Y. and H. S. Park(2021), Qualitative risk assessment of cybersecurity and development of vulnerability enhancement plans in consideration of digitalized ship. J Mar Sci Eng 9(6):565. https://doi.org/10.3390/jmse9060565.

Received : 2024. 05. 07.
Revised : 2024. 05. 24.
Accepted : 2024. 05. 29.