한국항해항만학회지 제47권 제2호
J. Navig. Port Res. Vol. 47, No. 2 : 57-65, April 2023 (ISSN:1598-5725(Print)/ISSN:2093-8470(Online))
DOI:http://dx.doi.org/10.5394/KINPR.2023.47.2.57

Cybersecurity Development Status and AI-Based Ship Network Security Device Configuration for MASS

Yunja Yoo·Kyoung-Kuk Yoon**·David Kwak***·Jong-Woo Ahn****·†Sangwon Park*

**Associate Professor, Division of Navigation Convergence Studies, Korea Maritime and Ocean University, Busan 49112, Korea*
***Assistant Professor, Division of Maritime AI & Cyber Security, Korea Maritime and Ocean University, Busan 49112, Korea*
****General Manager, 5G Business Division, Penta Security Systems Inc., Seoul 07241, Korea*
*****Principal Surveyor, Cyber Certification Team, Korean Register, Busan 46762, Korea*
† Senior Researcher, Logistics and Maritime Industry Research Department, Korea Maritime Institute, Busan 49111, Korea

Abstract : *In 2017, the International Maritime Organization (IMO) adopted MSC.428 (98), which recommends establishing a cyber-risk management system in Ship Safety Management Systems (SMSs) from January 2021. The 27th International Association of Marine Aids to Navigation and Lighthouse Authorities (IALA) also discussed prioritizing cyber-security (cyber-risk management) in developing systems to support Maritime Autonomous Surface Ship (MASS) operations (IALA guideline on developments in maritime autonomous surface ships). In response to these international discussions, Korea initiated the Korea Autonomous Surface Ship technology development project (KASS project) in 2020. Korea has been carrying out detailed tasks for cybersecurity technology development since 2021. This paper outlines the basic concept of ship network security equipment for supporting MASS ship operation in detailed task of cybersecurity technology development and defines ship network security equipment interface for MASS ship applications.*

Key words : *Maritime Autonomous Surface Ship (MASS), cyber risk management, cybersecurity, cybersecurity gateway, AI-based Network Security Device (AI-SNSD)*

1. Introduction

In June 2017, the IT system of a port terminal operated by Maersk Line was attacked by ransomware. Consequently, the container loading operation was performed manually for three weeks. It not only had a direct impact on the shipping industry, but also damaged related industries, and the total amount of damage was approximately $300 million. This incident triggered awareness of the importance of cybersecurity in the shipping industry. The IMO is also aware of the cyber threats posed by ship digitization and has been developing guidelines to address these concerns.

The IMO approved "Guidelines on maritime cyber risk management" in 2017, and recommends that each company's Safety Management System(SMS) manage cyber risks for ship systems(IMO, 2017a). In addition, the Baltic and International Maritime Council(BIMCO) has published "The guidelines on cyber security onboard ships" to introduce practical countermeasures against cyber-attacks(BIMCO et al., 2018). The international community has recognized that cyber threats in the shipping sector are a reality and has announced guidelines for the prevention and minimization of damage(Kang, 2018).

Meanwhile, the development of technology has resulted in the digitalization of ships and related equipment(Jung et al., 2019). Autonomous navigation, a technology that relies on AI to operate ships without crew members, has become an important issue in the shipping industry. However, network connections in digital devices are exposed to cyber threats, and as a result, technology to prevent cyber threats is considered essential(Yoo et al., 2022; Jo and Cha, 2019). To address these concerns, the IMO has initiated discussions on the acceptance of Maritime Autonomous Surface Ship(MASS), and plans to develop a special agreement for MASS(IMO, 2021). Additionally, the IALA is developing guidelines to support

†Corresponding author, psw6745@kmi.re.kr 051)797-4919
* yjyoo@kmou.ac.kr 051)410-4286
Note) This paper was presented on the subject of "Introduction of Korea Autonomous Surface Ship Project and Ship Network Security Equipment Development" in 2022 Asia Navigation Conference proceedings(Online meeting, 5th-6th of November, 2022, A4-2).

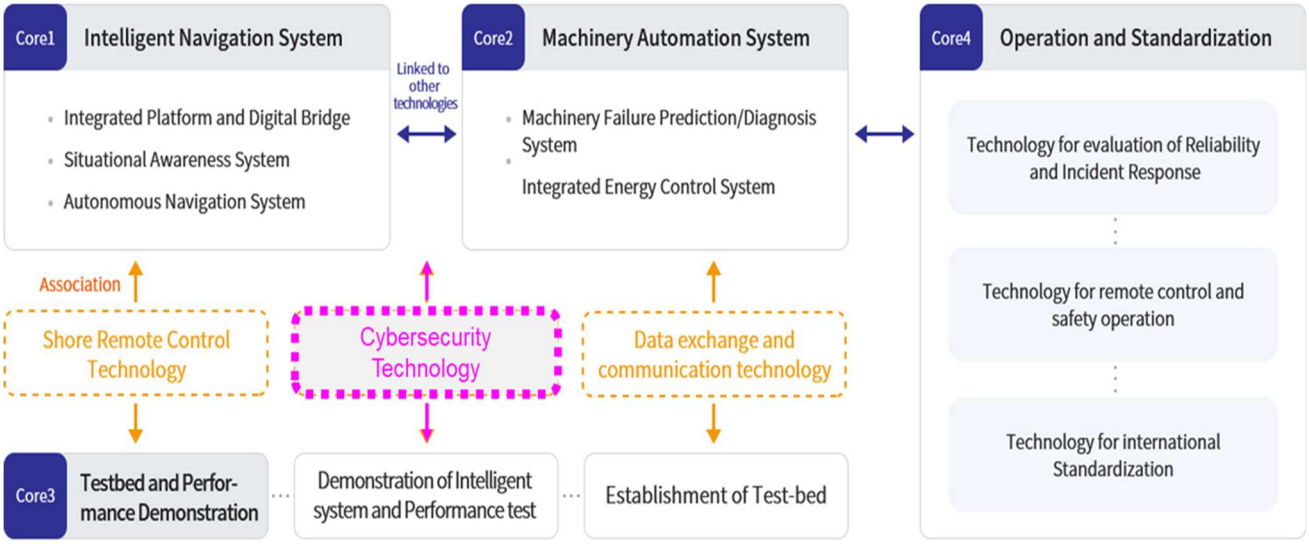

Fig. 1 Main research contents of Korean MASS project and association between core technologies, adapted from KASS project homepage(KASS, 2022)

the operation of MASS in terms of infrastructure, including cybersecurity and cyber risk management (IALA, 2021a).

The Republic of Korea started a six-year project in 2020 to develop autonomous ship technology. The goal of the project is to demonstrate this technology at IMO autonomous level 3 for ocean voyages and IMO autonomous level 2 for coastal voyages by installing a development system of project tasks in a medium-sized vessel. The project can be divided into four core technologies: intelligent navigation system, machinery automation system, testbed and performance demonstration, operation and standardization. Cybersecurity technology will be an essential component associated with the core technologies that will be developed for performance demonstrations.

This study introduces the cybersecurity technology development of the Korean Autonomous Surface Ship(KASS) project for MASS operation. To this end, the details of the cybersecurity development of the KASS project are introduced, along with the configuration of the ship network security device development.

2. Cybersecurity development for MASS

2.1 Concept of Korean MASS project

The Republic of Korea started the autonomous ship technology development project in 2020 to respond to a paradigm shift in the shipbuilding industry and to reduce the maritime accidents caused by human error. The project will be carried out for six years, and its goal is to develop core technologies for autonomous ships and lay the foundation for commercialization through phased demonstrations. In particular, it is planned to develop a medium-sized MASS capable of international navigation.

The target was to operate the vessel at IMO Level 3 in the ocean and IMO Level 2 on the coast. The overall development concept of the Korean MASS project involves shipboard and shore systems, in which ships and shores are connected through a digital bridge onboard.

2.2 Cybersecurity technology for MASS

The main research contents of the Korean MASS project can be divided into four categories: intelligent navigation system, engine automation system, demonstration and operation(KASS, 2022). Fig. 1 shows an association diagram of the development technology according to the main research contents.

The cybersecurity technology for MASS is scheduled for development from 2021 to 2024 and includes the following development items in detail:

- Development of a cybersecurity gateway(AI-SNSD, AI-based ship network security device) product for MASS;
- Development of an integrated security management system for a shore control center(SCC) for MASS;
- Development of cybersecurity type approval guidelines for MASS;
- Development of agenda for international organizations on cybersecurity.

Fig. 2 shows the development phases of the cybersecurity gateway for MASS by year.

An outline of the cybersecurity technology development of the Korean MASS project and details of

the technology development are described in Chapter 3.

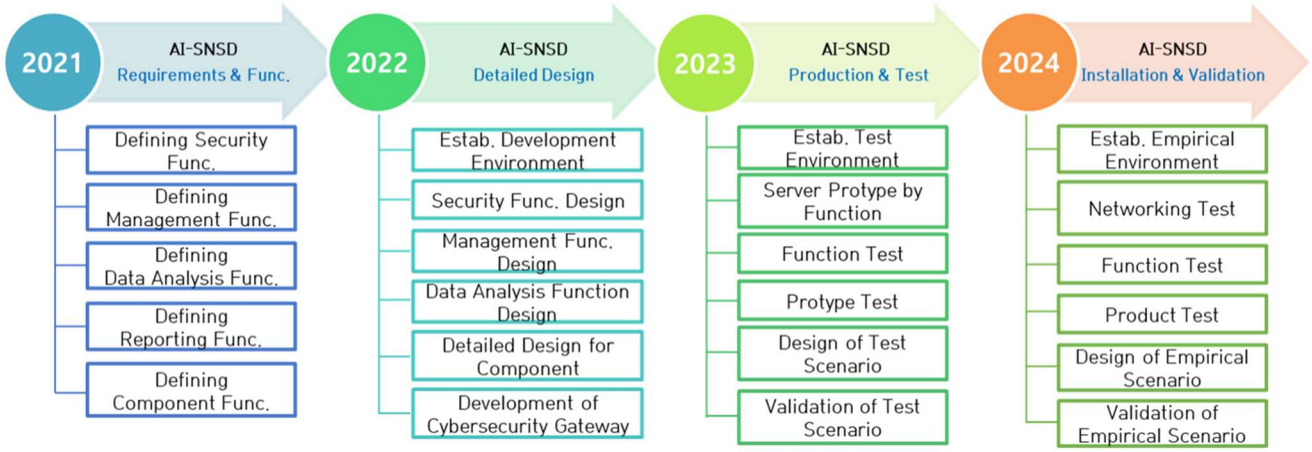

Fig. 2 Development phase of cybersecurity gateway(AI-SNSD) for MASS

technology development, is to develop systems and related technology standards that utilize the latest cybersecurity technologies to detect, defend, and respond to cyber threats inside and outside autonomous ships.

Fig. 3 shows the overall configuration of the cybersecurity technology development for MASS, which consists of four steps: 1) cybersecurity gateway development, 2) integrated cybersecurity management system development, 3) cybersecurity technology

3. AI-based ship network security device(AI-SNSD) development

3.1 Overview of cybersecurity technical development

Application of the avoidance sector threshold to the actual avoidance action is as follows: one of the detailed tasks of the Korean MASS project, cybersecurity

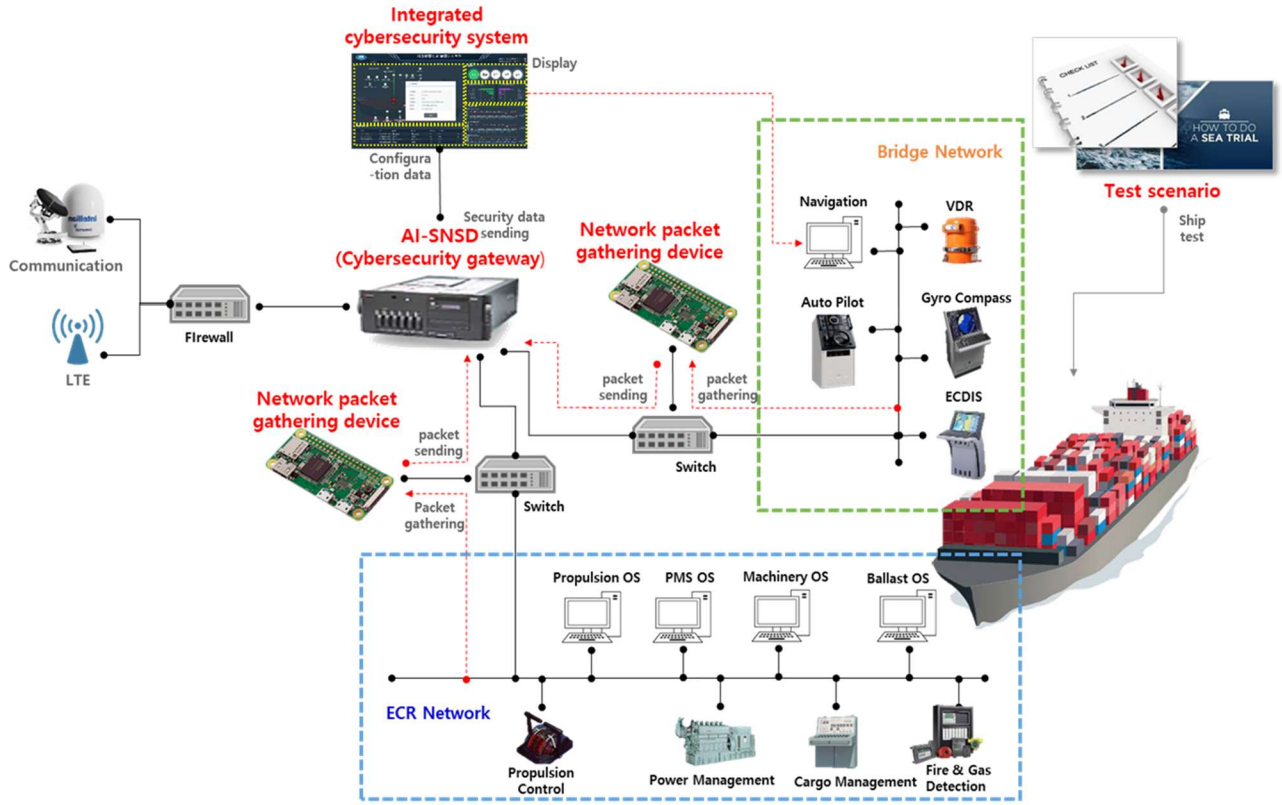

Fig. 3 Overall configuration of the cybersecurity technology development for MASS

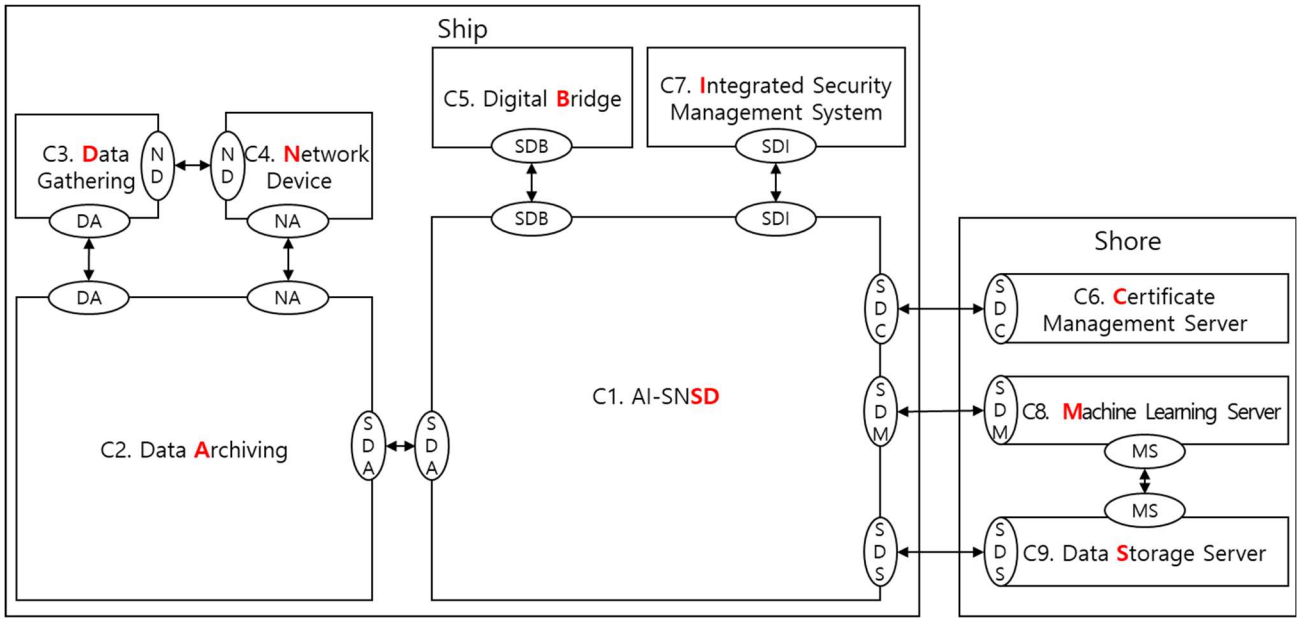

Fig. 4 Cybersecurity gateway(AI-SNSD) interface based on function requirements

standard development, and 4) cybersecurity system operation test and test scenario development.

First, the cybersecurity gateway which is a critical aspect of the MASS is developed. It is an AI-based ship network security device(AI-SNSD) that includes various features such as authentication and encryption technology for ship-to-external communication, detection and blocking of attacks based on a deep packet inspection(DPI) analysis of external incoming traffic.

The second aspect of the MASS's cybersecurity development is the development of an integrated cybersecurity management system. This system will include various features, such as data processing technology, cybersecurity data collection and analysis technology, dashboard development, in-ship ICT asset management, and public-information-based cyber asset vulnerability analysis technology.

Third, the development of cybersecurity technology standards includes the development of guidelines for the cybersecurity-type approval of autonomous ships, the development of cybersecurity gateway technology standards for autonomous ships, and the development of guidelines for test procedures for autonomous ship cybersecurity systems.

Fourth, the development of actual cybersecurity system operation tests and test scenarios includes the collection and analysis of current cybersecurity status data of existing ships, the development of cybersecurity test plan scenarios based on the analyzed data, the application of autonomous ships, and testing and verification.

This study focuses on the 'Development of cybersecurity gateway products for MASS' as a key component of the cybersecurity technology development tasks.

3.2 Configuration of AI-based ship network security device(AI-SNSD)

Functional requirements for MASS operations were identified in 2021 to develop a security gateway for MASS ships. In the case of AI-SNSD, functions such as firewall, intrusion detection and protection(IDPS), anomaly detection, and deep packet inspection are required. In the case of Data-Archiving, functions such as collection of data(packet), analysis of network status, decompression and re-compression of collection data(packets) files, failover of collection data(packet)

Table 1 Cybersecurity gateway(AI-SNSD) components and interface definition

No.	Component	Interface
C1	AI-SNSD(SD)	SDA/ SDB/ SDC/ SDI/ SDM/ SDS
C2	Data Archiving(A)	DA/ NA/ SDA
C3	Data Gathering(D)	DA/ ND
C4	Network Device(N)	ND/ NA
C5	Digital Bridge(B)	SDB
C6	Certificate Management Server(C)	SDC
C7	Integrated Security Management System(I)	SDI
C8	Machine Learning Server(M)	SDM/ MS
C9	Data Storage Server(S)	SDS/ MS

Table 2 Cybersecurity gateway(AI-SNSD) components and interface description

No.	Interface	Description
C1	SDA	Linkage interface associated with Data Archiving devices
	SDB	Linkage interface associated with Digital Bridge
	SDC	Linkage interface associated with the Certificate Management Server
	SDI	Linkage interface associated with Integrated Security Management System
	SDM	Linkage interface associated with Machine Learning Server
	SDS	Linkage interface associated with Data Storage Server
C2	DA	Linkage interface associated with Data Gathering
	NA	Link interface associated with Network Device
	SDA	Linkage interface associated with AI-SNSD
C3	DA	Linkage interface associated with Data Archiving
	ND	Link interface associated with Network Device
C4	ND	Linkage interface associated with Data Gathering
	NA	Linkage interface associated with Data Archiving
C5	SDB	Linkage interface associated with AI-SNSD
C6	SDC	Linkage interface associated with the Certificate Management Server
C7	SDI	Linkage interface associated with Integrated Security Management System
C8	SDM	Linkage interface associated with AI-SNSD
	MS	Linkage interface associated with Data Storage Server
C9	SDS	Linkage interface associated with AI-SNSD
	MS	Linkage interface associated with Machine Learning Server

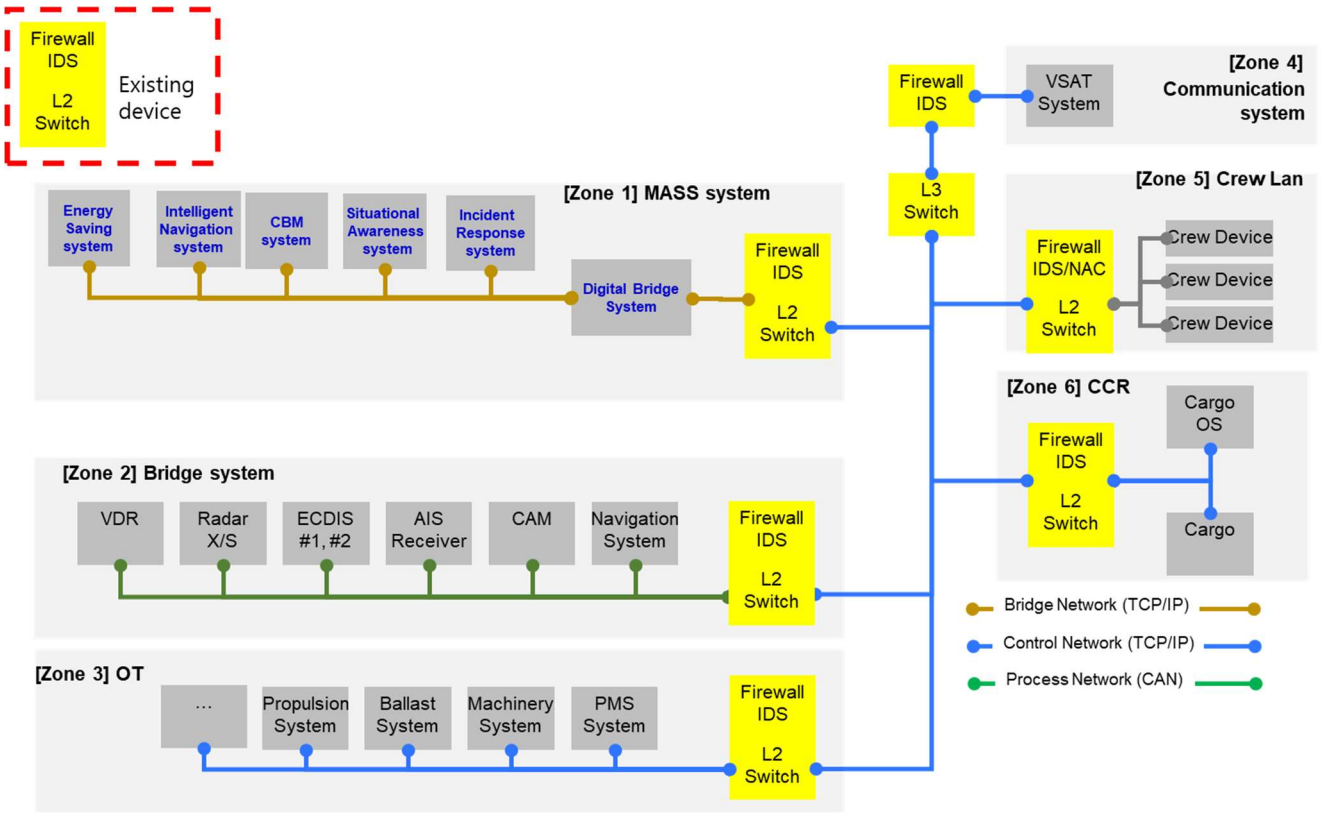

Fig. 5 Cybersecurity topology applied existing equipment by zone

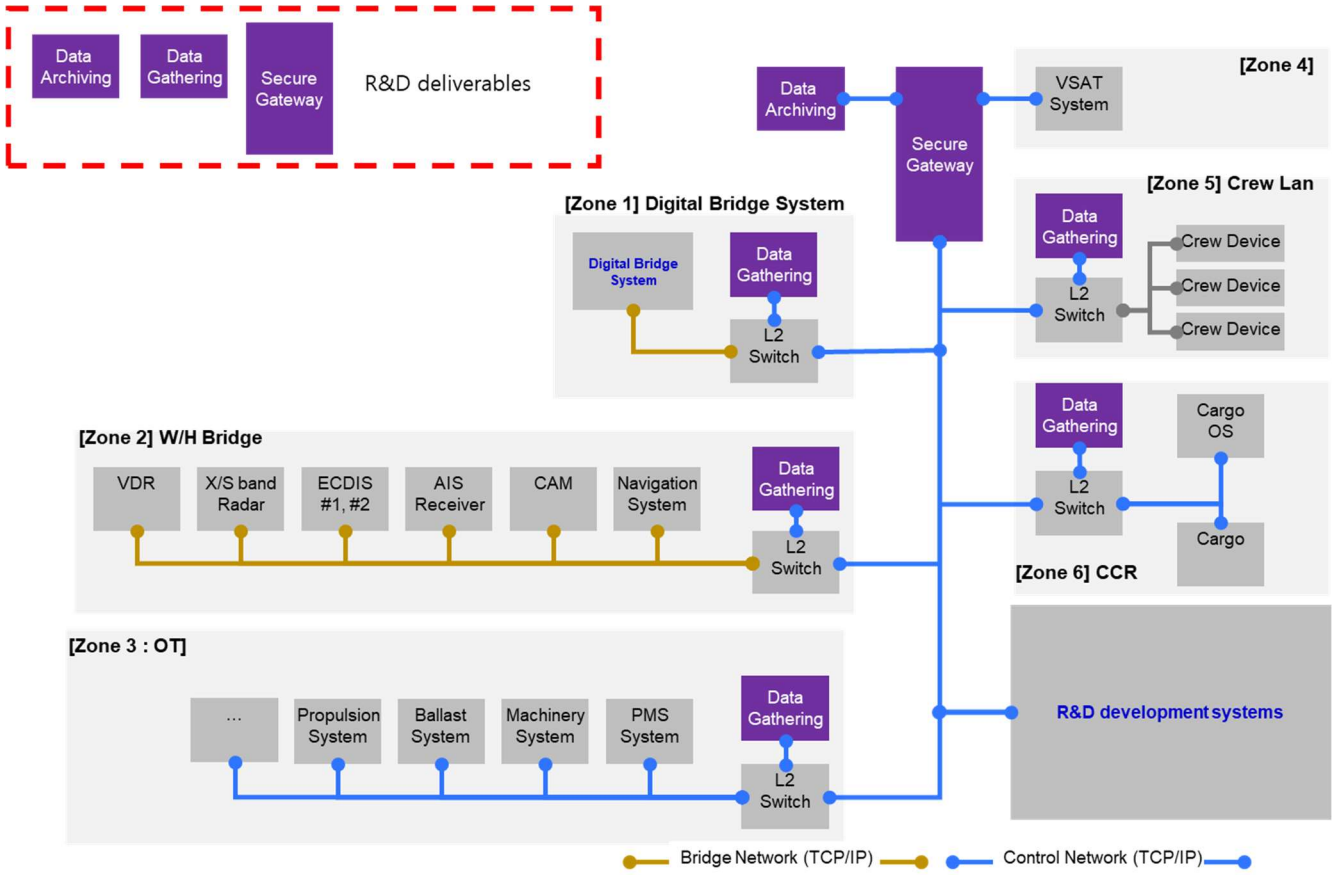

Fig. 6 Cybersecurity topology applied AI-SNSD of MASS by zone

Table 3 Main functions comparison between existing firewall equipment and cybersecurity gateway(AI-SNSD) of MASS

Main function	Existing firewall & IDS/IPS product	AI-SNSD(R&D deliverables)
Firewall	Rule-based and signature-based firewall policy	Existing firewall + IP/port dynamic control
IPS	Rule-based and signature-based intrusion prevention	Rule-based and signature-based intrusion prevention + Machine learning-based intrusion prevention
IDS	Rule-based and signature-based intrusion detection	Rule-based and signature-based intrusion detection + Machine learning-based intrusion detection
Anti-virus/spam	Requires software installation	DPI-based malware detection
IPSec VPN	Possible	Possible
SSL VPN	Possible	Possible
Log/monitoring	Do not support logging/ monitoring for the entire ship network	Support logging/monitoring of the entire ship network by collecting internal and external network traffic
BYOD device management	Requires NAC solution	Support for BYOD access management and authentication based on PKI certificates
Network anomaly detection	External network traffic detection	Internal/external traffic anomaly detection

External communication authentication	Requires PKI and SW installation	Support PKI-based authentication
Data flow control	Inability to control internal communication	Control data flow without product installation
Routing function	Impossible	Possible

forwarding, prevention of disk overflow, and data transmission are required. In the case of Data-Gathering, functions such as data(packet) collection, filtering, forwarding, file compression, forwarding failover, and collection interruption are required. In the case of Management-System, functions such as policy management, certificate management, certificate issuance, log management, monitoring, and notice are required. In the case of Certificate-Management-System, functions such as self-protection, authentication, and encrypted communication are required.

Based on the identified functional requirements, the ship consisted of six components(C1: AI-SNSD, C2: Data Archiving, C3: Data Gathering, C4: Network Device, C5: Digital Bridge, and C7: Integrated Security Management System), and the shore consisted of three components(C6: Certificate Management Server, C8: Machine Learning Server, C9: Data Storage Server).

C1's SDA and SDB transmit data stored from data-gathering and network devices to AI-SNSD. SDC and SDI allow AI-SNSD to receive upper/lower certificates through a certificate management server and transmit policies and data defined by AI-SNSD to an integrated security management system on land. SDM and SDS receive the results of AI-SNSD learning based on data from the machine learning server and transmit the data to be learned from the machine learning server to the data storage server. The DA of C2 stores the data collected from the data-gathering device present in each zone, and the NA stores the data collected from the network device. In addition, SDA transmits data stored in data-gathering and network devices to AI-SNSD. The DA and ND of C3 transmit data stored by the data-gathering device installed in each zone to the data-archiving device. ND and NA of C4 transmit the generated data to the data-gathering device. The SDB of C5 receives associated data from AI-SNSD. The SDC of C6 serves as a certificate management server for issuing AI-SNSD certificates. The SDI of C7 receives data such as those of policies defined by AI-SNSD and provide necessary data for management/operation to AI-SNSD through the integrated security management system. The SDM of C8 transmits the results learned from the machine learning server to the AI-SNSD, and the MS receives data from the data storage server to be learned by the machine learning server. The SDS of C9 receives and stores data to be used for learning from the machine learning server from AI-SNSD, and MS transmits the data stored in the storage server to the machine learning server.

The interface connections for each component are shown in Fig. 4. The interface definitions and function descriptions for each component are listed in Tables 1 and 2.

In general, the network of ships to which the concept of cybersecurity is applied is divided into zones, such as bridge systems related to ship operations such as navigation and communication, engine, propulsion systems related to ship propulsion, crew area, cargo management, and handling. As part of the plan to reduce cyber risk in the event of a cyberattack, a cybersecurity composition diagram of autonomous ships, expressed by separating, classifying, and stratifying networks by region, is shown in Fig. 5.

Considering the current firewalls of commercial equipment, the network topology applicable to MASS ships can be shown in Fig. 5 by applying Open Systems Interconnection model(OSI) 7 layers(L1: Physical Layer, L2: Data Link Layer, L3: Network Layer, L4: Transport Layer, L5: Session Layer, L6: Presentation Layer, and L7: Application Layer)(ISO/IEC, 1994; Microsoft, 2022). Zone-1 consists of the autonomous operating equipment necessary for the operation of MASS ships, Zone-2 consists of a bridge navigation and communication system, Zone-3 is a propulsion and engine system, Zone-4 is a communication system, Zone-5 is a crew area network system, and Zone-6 consists of a cargo handling system divided into L2 layers. The L2 layer configures the L2 switch and firewall in each zone. In addition, the L3 layer installs the L3 switch for internal or external communication using IP addresses, and the firewall between the L3 switch and satellite communication aims to defend against cyber threats entering ships from the outside(on land).

However, when the cybersecurity gateway under development is applied, the network topology of the autonomous ships can be expressed as shown in Fig. 6. Here, the AI-SNSD, which integrates the functions of the L3 switches and firewalls, was installed without setting the firewall function of the existing L2 layer. Data-gathering equipment is installed to monitor potential cyber risks, and AI-SNSD is deployed to detect and block external attacks. As communication between zones is limited, the system is designed to operate effectively for extended periods without maintenance. Additionally,

protocols commonly used on ships are incorporated to enhance the system's ability to respond to cyber threats. Table 3 compares the main functions of existing firewall equipment and the cybersecurity gateway(AI-SNSD) under development for MASS.

In the case of firewall functions, existing equipment is subject to rule-based and signature-based firewall policies, and AI-ANSD of MASS includes dynamic control over IP and ports in addition to existing firewall functions. In the case of intrusion prevention systems, existing equipment is rule-based and signature-based, whereas AI-SNSD adds a machine-learning-based intrusion prevention function to the intrusion prevention systems(IPS) of existing equipment. In the case of intrusion prevention systems, the existing equipment is the same as in intrusion detection systems(IDS); however, AI-SNSD adds machine-learning-based intrusion prevention functions similar to IPS. For antiviruses and spam detection, the existing equipment requires separate software installation, and for AI-SNSD, DPI-based malware detection is added. There is no significant difference in VPN functions, and existing equipment does not support log/monitoring functions for the entire ship network. However, AI-SNSD collects internal and external network traffic to support log/monitoring functions for the entire ship network. In the case of bringing your own device(BYOD) management, existing equipment requires a separate network access control(NAC) solution, whereas AI-SNSD includes public key infrastructure(PKI) certificate-based BYOD device access management and authentication support. In the case of the network abnormality detection function, the existing equipment supports the detection function for external network traffic, and AI-SNSD also supports the abnormality detection function for internal and external traffic. For the authentication function of external communication, separate PKI infrastructure and software installation are required for existing equipment, and PKI-based ship-to-ship/ship-to-shore/shore-to-shore authentication is supported for AI-SNSD. In the case of the data flow control function, internal communication of the existing equipment is impossible because of the network structure, whereas in the case of AI-SNSD, data flow control is possible without installing a separate product. In addition, existing equipment does not provide routing functions, but AI-SNSD provides routing functions that include security functions suitable for MASS ships.

4. Conclusion

Along with the 4th Industrial Revolution, ships, seas, and port infrastructure are also becoming digital, and accordingly, the international community is preparing for the introduction of autonomous ships earnestly. The International Maritime Organization(IMO) adopted MSC.428(98) in 2017(IMO, 2017b), and recommended that the Ship Management System(SMS) manage matters related to cyber risk management during annual ship inspections from January 2022. The International Association of Marine Aids to Navigation and Lighthouse Authorities(IALA) also requires consideration of matters related to cybersecurity when developing an autonomous ship support system(IALA, 2021b).

Accordingly, this study introduced an outline of the autonomous ship project(KASS project, Korea Autonomous Surface Ship project) developed in Korea, and explained the concept and core functions of cybersecurity technology development among the detailed technologies for MASS operation. In addition, the main functions of existing commercial security equipment and AI-SNSD security equipment developed for MASS are compared and described.

In the future, we plan to verify AI-SNSD security equipment and element technology through scenario development and applications for ship testing of security equipment under development for MASS cybersecurity technology.

Acknowledgements

This study was supported by the 'Development of Autonomous Ship Technology(20200615)' funded by the Ministry of Oceans and Fisheries(MOF, Korea).

References

[1] BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF and WSC(2018), The guidelines on cyber security onboard ships, Version 3.

[2] IALA(2021a), Report of the 27th session of the IALA e-navigation information services and communication, International Association of Marine Aids to Navigation and Lighthouse Authorities.

[3] IALA(2021b), IALA guideline on developments in maritime autonomous surface ships, ENAV27 working paper, International Association of Marine Aids to Navigation and Lighthouse Authorities.

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

[5] IMO(2017b), Maritime cyber risk management in safety management systems, Resolution MSC.428(98), Annex 10, International Maritime Organization.

[6] IMO(2021), Report of the maritime safety committee on its 104th session, MSC 104/24, International Maritime Organization.

[7] ISO/IEC(1994), Information technology - Open Systems Interconnection - Basic Reference Model:

The Basic Model, ISO/IEC 7498-1, International Organization for Standardization/ International Electrotechnical Commission.

[8] Jo, Y. H. and Cha, Y. K.(2019), "A study on cyber security requirements of ship using threat modeling", Journal of The Korea Institute of Information Security & Cryptology, Vol. 29, No. 3, pp. 657-673.

[9] Jung, H. R., Chang, H. J. and Song, Y. E.(2019), "Trend of autonomous navigation technology for unmanned ship", Journal of Institute Control, Robotics and Systems, Vol. 25, No. 1, pp. 76-87.

[10] Kang, N. S.(2018), "Analysis of onboard ship cybersecurity", Journal of Korean Society of Marine Engineering, Vol. 42, No. 6, pp. 463-471.

[11] KASS(2022), Introduction of KASS(Korea Autonomous Surface Ship) project, https://kassproject.org/en/main.php, accessed in 30th Aug. 2022.

[12] Microsoft(2022), Windows Network Architecture and the OSI Model, https://docs.microsoft.com /en-US/windows-hardware/drivers/network/windows-network-architecture-and-the-osi-model, accessed in 30th Aug. 2022.

[13] Yoo, J. W., Jo, Y. H. and Cha, Y. K.(2022), "Artificial intelligence for autonomous ship: Potential cyber treats and security", Journal of The Korea Institute of Information Security & Cryptology, Vol. 32, No. 2, pp. 447-463.

Received 09 March 2023
Revised 24 March 2023
Accepted 19 April 2023