Introduction of Korea autonomous surface ship project and ship network security equipment development

Yunja YOO, Kyoung-Kuk YOON*, David KWAK**, Myongcheol LIM** and Sangwon PARK****

*Korea Maritime and Ocean University, 727 Taejong-ro, Yeongdo-gu, Busan, 49112 Korea
**Penta Security Systems Inc., 115 Yeouigongwon-ro, Yeongdeungpo-gu, Seoul, 07241 Korea
***Korea Maritime Institute, 26 Haeyang-ro 301 beon-gil, Yeongdo-gu, Busan, 49111 Korea
psw6745@kmi.re.kr

Key words: maritime autonomous surface ship, Korea autonomous surface ship (KASS) project, ship network security equipment, autonomous level

ABSTRACT

The International Maritime Organization (IMO) recommends establishing a cyber-risk management system in the ship safety management system (SMS) from January 2021 based on the resolution MSC.428(98) (Maritime cyber risk management in safety management systems). And the 27th International Association of Marine Aids to Navigation and Lighthouse Authorities (IALA) 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). Following these discussions by the international community, Korea has started the Korea autonomous surface ship (KASS) technology development project (KASS project) from 2020 and has been carrying out detailed tasks for cyber security technology development since 2021. This study introduces the four core technologies of the KASS project which are the intelligent navigation system, engine automation system, performance demonstration center and demonstration technology, and operational technology and standardization. In addition, the basic concept of ship network security equipment for supporting KASS ship operation in the detailed task of cybersecurity technology development was introduced, and the ship network security equipment interface for KASS ship application was defined.

1. Introduction

In June 2017, the IT system of a port terminal in Maerskline was attacked by ransomware. As a result, the container loading operation was operated 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 about $300 million. The 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 is discussing guidelines.

In 2017, the IMO approved 'Guidelines on maritime cyber risk management', and recommends that the company's SMS (Safety, Management System) manage cyber risks for ship systems (IMO, 2017). Also, BIMCO published 'The guidelines on Cyber Security Onboard ship' to introduce practical countermeasures against cyber attacks. The international community has recognized that cyber threats in the shipping sector have become a reality, and is announcing guidelines for prevention and minimization of damage. In 2017, the IMO approved 'Guidelines on maritime cyber risk management', and recommends that the company's SMS (Safety, Management System) manage cyber risks for ship systems (IMO, 2017). Also, BIMCO published 'The guidelines on Cyber Security Onboard ship' to introduce practical countermeasures against cyber attacks (Bimco et al., 2018). The international community has recognized that cyber threats in the shipping sector have become a reality, and is announcing guidelines for prevention and minimization of damage.

Meanwhile, the development of technology causes the digitalization of ships and related equipment. In particular, autonomous navigation, which has recently become an issue, is a technology that relies on AI to operate ships without crew members depending on the stage. Network connections of digital devices are exposed to cyber threats, and technology to prevent cyber threats is judged to be essential. The IMO has begun discussions on the acceptance of MASS (Maritime Autonomous Surface Ship), focusing on related agreements, and plans to develop a special agreement for MASS (IMO, 2021). IALA is developing guidelines to support the operation of MASS in terms of infrastructure, including cybersecurity and cyber risk management (IALA, 2021a).

The Republic of Korea started the project for six years from 2020 to develop autonomous ship technology. The goal of the project is to operate a medium-sized vessel at IMO autonomous level 3 for ocean voyages and IMO autonomous level 2 for coastal voyages. The project can be divided into navigation system, machinery system and performance demonstration, and cyber security technology will be developed in the performance demonstration.

The purpose of this paper is to introduce the Korean autonomous surface ship (KASS) project in Republic of Korea and to develop cybersecurity technology for ship networks for MASS operation. To this end, we would like to introduce the details of the KASS project and introduce the ship network concept development and equipment for cybersecurity.

2. Korea Autonomous Surface Ship Project

2.1 Concept of KASS Project

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

The target is to operate the vessel at IMO level 3 in the ocean and at IMO level 2 in the coast. **Fig.1** shows the overall development task of the KASS project. It can be broadly divided into the shipboard system and the shore system, and the ship and shore are connected through a digital twin bridge.

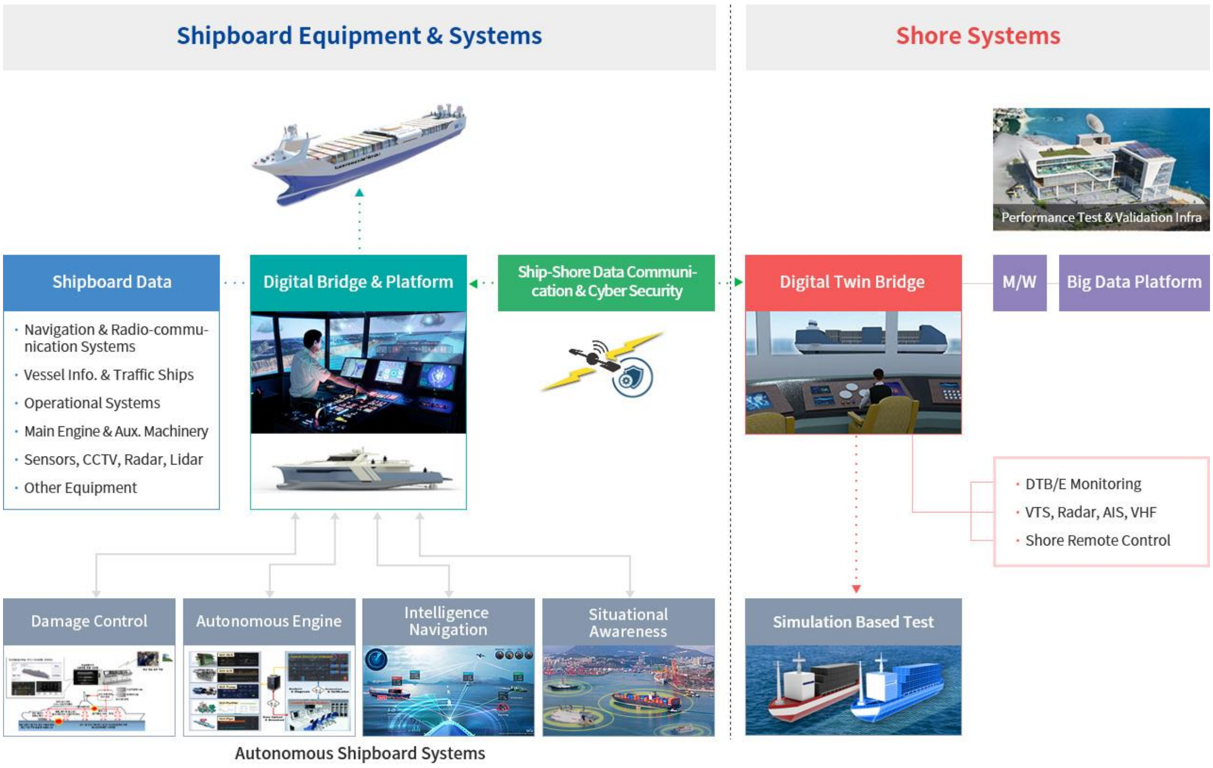

Shipboard Equipment & Systems
Shore Systems
Performance Test & Validation Infra
Shipboard Data
Navigation & Radio-communication Systems
Vessel Info. & Traffic Ships
Operational Systems
Main Engine & Aux. Machinery
Sensors, CCTV, Radar, Lidar
Other Equipment
Digital Bridge & Platform
Ship-Shore Data Communication & Cyber Security
Digital Twin Bridge
M/W
Big Data Platform
DTB/E Monitoring
VTS, Radar, AIS, VHF
Shore Remote Control
Damage Control
Autonomous Engine
Intelligence Navigation
Situational Awareness
Simulation Based Test
Autonomous Shipboard Systems

Fig. 1 Overview of development task of the KASS project (Source: KASS project homepage (KASS, 2022)).

2.2 Development Target of KASS Project

The main research contents of the KASS project can be divided into four categories: intelligent navigation system, engine automation system, and demonstration and operation (KASS, 2022). **Fig. 2** is the association diagram showing the development technology according to the main research contents. The KASS project has a total of 4 large systems, and there are 13 major technologies under the system. Among them, the intelligent navigation system and the engine automation system are to develop the main technologies of the navigation system and the engine system of MASS. The technology developed here is connected to remote control technology, communication technology, and cyber security technology, and the technology can be tested at the demonstration center. In addition, operating technology will be developed so that the developed MASS can be operated safely and efficiently. **Figs. 2, 3** are showing the relationship between the main tasks.

2.2.1 Intelligent navigation system

The intelligent navigation system sector develops automation systems related to vessel navigation. This includes situational awareness, route decision-making and the development of a digital bridge that can control both navigation and engine room. Situational awareness recognizes and analyzes the maritime situation around the vessel in real time to secure the navigational safety of MASS. For situational awareness, sensors such as AIS, EO/IR, Camera, LiDAR, and Radar are used, and the collected information is integrated through heterogeneous sensor data processing systems. It detects and tracks based on the integrated target data and uses artificial intelligence to suggest the risk of collision.

In the autonomous navigation system, route planning algorithms are developed for operational safety and economic operation. In addition, a route-following control algorithm is also developed to avoid and change the route when a collision object is found on the route. The developed algorithm is applied to the testbed and verified.

Digital Bridge develops a digital control system and navigation system interworking interface that interworks through a ship network. In addition, an integrated system that can monitor, transmit, and control the status of digital control and navigation system devices for autonomous navigation will be developed.

To summarize the intelligent navigation system, it is a system that designs and suggests routes centered on safety and economy, navigates ships, and uses sensors attached to ships to recognize, evaluate, and take an action on objects on the sea. And related data is connected by a digital bridge, and it is a system that can be monitored and controlled even on shore side.

2.2.2 Machinery automation system

The engine automation system sector develops automation systems related to ship engines. This includes the development of engine system performance monitoring and failure prediction technology, and energy control technology.

The engine failure and prediction system is based on CBM (Condition based maintenance) and targets 5 or more engine systems including the main engine and generator. Using the data generated through the failure simulation scenario, it diagnoses failures with methodologies such as statistical analysis and machine learning and predicts the trend of data change. It also develops software that can monitor it. The ship remote maintenance support system is a system that enables onshore experts to check the ship's status and support the field, and is developed based on augmented reality.

The integrated energy control system is a system that can automatically collect and monitor energy data within a ship. Through this, it is possible to diagnose the performance of the ship's energy system and predict and manage the consumption.

To summarize the engine automation system, real-time monitoring of the operating status of the engine system in a ship makes fault diagnosis/prediction with the generated data and develops a system that supports maintenance. The data of the engine system is connected by a digital bridge, and the field can be supported through the digital bridge even on shore side.

2.2.3 Control technology

In the Performance Demonstration Center section, a performance demonstration center can be built to test the developed technology, and demonstration technologies such as communication systems, remote control and cyber security are developed.

To develop MASS technology and secure a certification system, it is necessary to verify performance safety such as major equipment and parts, navigation equipment/devices, and cyber security. Therefore, for this, a test environment infrastructure for testing/evaluation/verification of MASS is established. The infrastructure is built on both shore side and sea, and the built ships are tested.

VDES ship station communication system is developed for smooth data exchange of MASS. Through this, the VDES ship station communication system and gateway and maritime broadband communication integrated gateway are developed and verified. Cybersecurity develops network security equipment that can be applied to ships of level 3 autonomous navigation and develops a system that can monitor and manage them.

The shore based remote control system builds scenarios for each emergency of MASS and develops the remote control system for shore-based centers.

Summarizing the demonstration center and verification system, it will be built onshore/offshore infrastructure and systems that can demonstrate technology for operating MASS, such as navigation and technology and verification technology. Develop communication and remote control technologies that connect shore and MASS and develop technologies that can respond to cyber threats that may occur during data exchange.

Fig. 4 shows the process of demonstration and commissioning of the performance demonstration center.

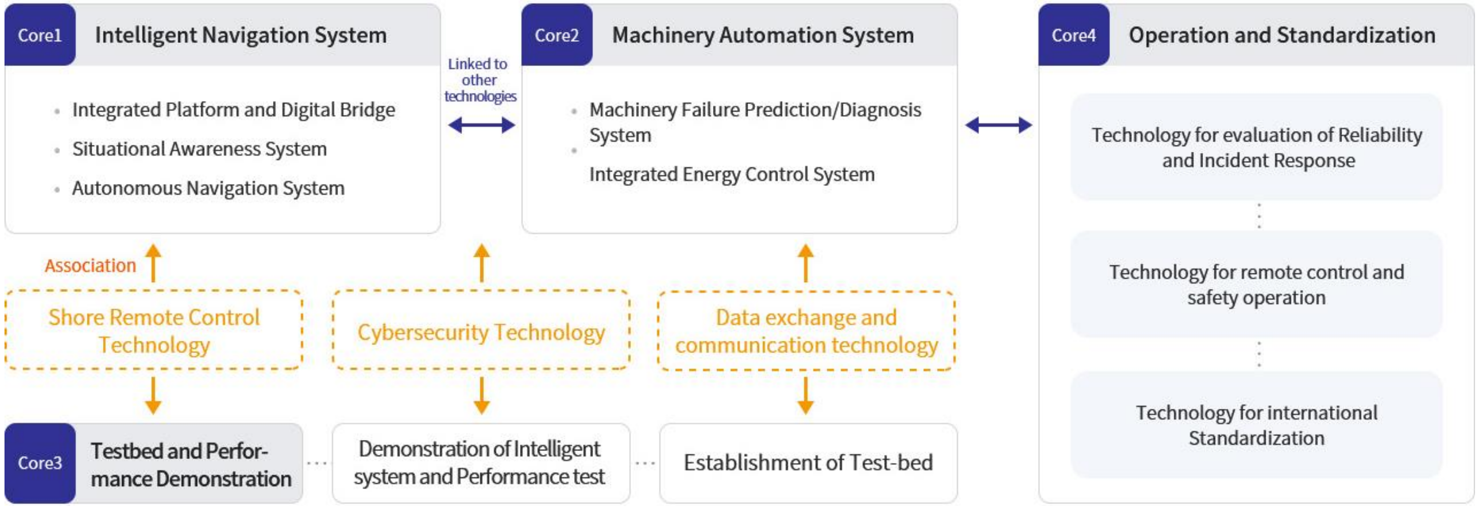
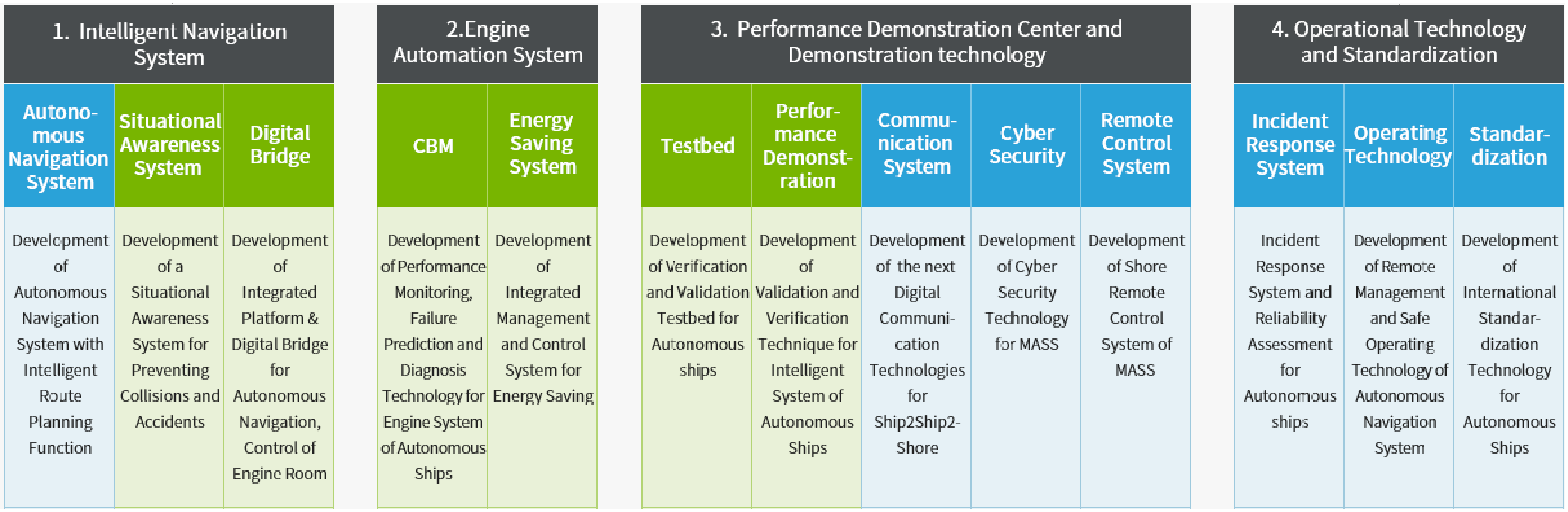

Core1
Intelligent Navigation System
Integrated Platform and Digital Bridge
Situational Awareness System
Autonomous Navigation System
Linked to other technologies
Core2
Machinery Automation System
Machinery Failure Prediction/Diagnosis System
Integrated Energy Control System
Core4
Operation and Standardization
Technology for evaluation of Reliability and Incident Response
Technology for remote control and safety operation
Technology for international Standardization
Association
Shore Remote Control Technology
Cybersecurity Technology
Data exchange and communication technology
Core3
Testbed and Performance Demonstration
Demonstration of Intelligent system and Performance test
Establishment of Test-bed

Fig. 2 Association between core technologies (Source: KASS project homepage (KASS, 2022)).



1. Intelligent Navigation System			2.Engine Automation System		3. Performance Demonstration Center and Demonstration technology					4. Operational Technology and Standardization		
Autonomous Navigation System	Situational Awareness System	Digital Bridge	CBM	Energy Saving System	Testbed	Performance Demonstration	Communication System	Cyber Security	Remote Control System	Incident Response System	Operating Technology	Standardization
Development of Autonomous Navigation System with Intelligent Route Planning Function	Development of a Situational Awareness System for Preventing Collisions and Accidents	Development of Integrated Platform & Digital Bridge for Autonomous Navigation, Control of Engine Room	Development of Performance Monitoring, Failure Prediction and Diagnosis Technology for Engine System of Autonomous Ships	Development of Integrated Management and Control System for Energy Saving	Development of Verification and Validation Testbed for Autonomous ships	Development of Validation and Verification Technique for Intelligent System of Autonomous Ships	Development of the next Digital Communication Technologies for Ship2Ship2-Shore	Development of Cyber Security Technology for MASS	Development of Shore Remote Control System of MASS	Incident Response System and Reliability Assessment for Autonomous ships	Development of Remote Management and Safe Operating Technology of Autonomous Navigation System	Development of International Standardization Technology for Autonomous Ships

Fig. 3 Core technologies of Korea autonomous surface ship (KASS) project (Source: KASS project homepage (KASS, 2022)).

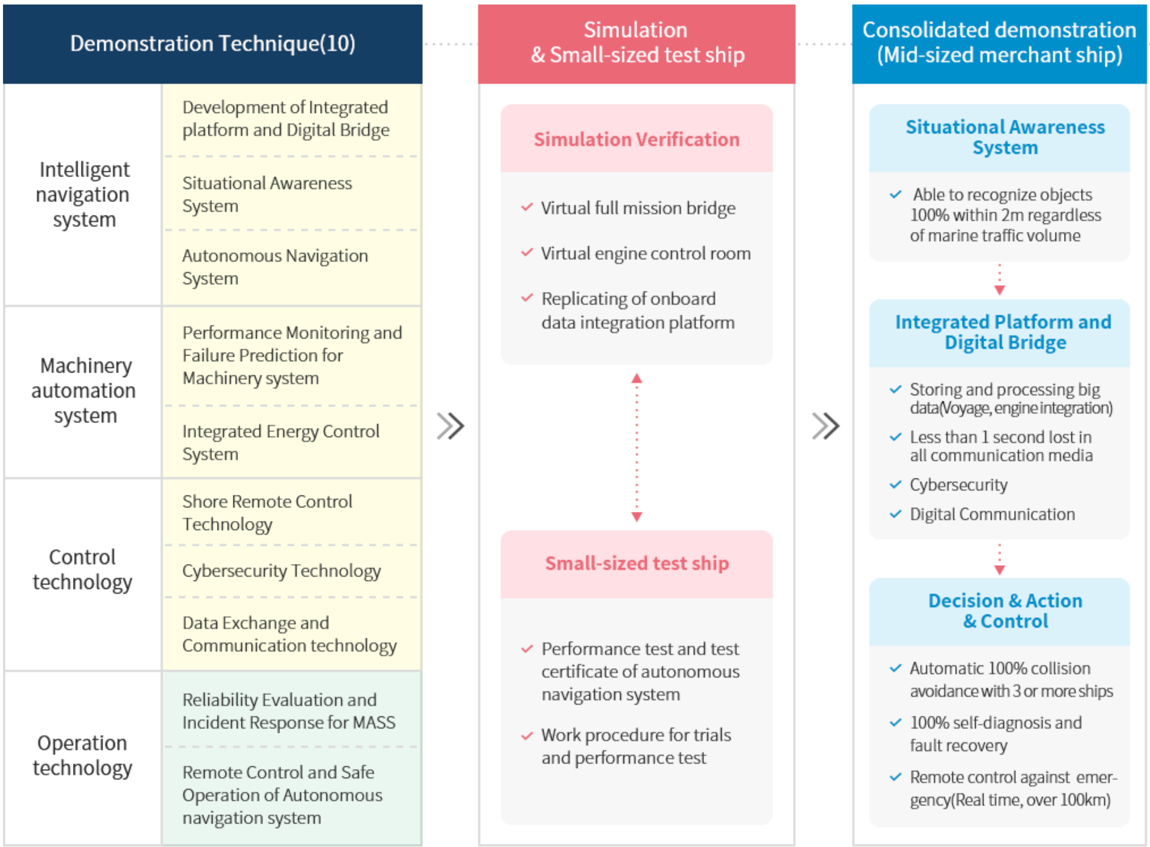

Demonstration Technique(10)
Simulation & Small-sized test ship
Consolidated demonstration (Mid-sized merchant ship)
Intelligent navigation system
Development of Integrated platform and Digital Bridge
Situational Awareness System
Autonomous Navigation System
Machinery automation system
Performance Monitoring and Failure Prediction for Machinery system
Integrated Energy Control System
Control technology
Shore Remote Control Technology
Cybersecurity Technology
Data Exchange and Communication technology
Operation technology
Reliability Evaluation and Incident Response for MASS
Remote Control and Safe Operation of Autonomous navigation system
Simulation Verification
✓ Virtual full mission bridge
✓ Virtual engine control room
✓ Replicating of onboard data integration platform
Small-sized test ship
✓ Performance test and test certificate of autonomous navigation system
✓ Work procedure for trials and performance test
Situational Awareness System
✓ Able to recognize objects 100% within 2m regardless of marine traffic volume
Integrated Platform and Digital Bridge
✓ Storing and processing big data(Voyage, engine integration)
✓ Less than 1 second lost in all communication media
✓ Cybersecurity
✓ Digital Communication
Decision & Action & Control
✓ Automatic 100% collision avoidance with 3 or more ships
✓ 100% self-diagnosis and fault recovery
✓ Remote control against emergency(Real time, over 100km)

Fig. 4 MASS-related demonstration targets and methods (Source: KASS project homepage (KASS, 2022)).

2.2.4 Operation technology

In the operation system sector, MASS reliability evaluation, accident response technology, remote management and safety operation technology are developed. As a system capable of judging the risk of accidents occurring during MASS operation and responding to them, it is developed safety and risk assessment technologies suitable for the characteristics of MASS. And it develops a system that can optimize accident response through prediction of accident situation. Remote management is to develop AI-based hull damage diagnosis technology and fleet asset management platform for efficient operation of MASS. In addition, for stable operation, six safe operation support services will be developed, including cargo loading and unloading, automatic berthing and mooring, condition monitoring support, PSC (Port State Control) inspection support, accident response support, and autonomous navigation support.

To summarize the operating system, it develops the technology to support the safe and efficient operation of MASS from shore to ship.

3. Development of Cybersecurity Technology for KASS

3.1 Overview of Technical Development

One of the detailed tasks of the KASS project, the Cybersecurity Technology Development Task, aims 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. 5** shows the overall configuration of the cybersecurity technology development of the KASS project, and consists of four details: 1) cybersecurity gateway development, 2) integrated cybersecurity management system development, 3) cybersecurity technology standard development, and 4) cybersecurity system operation test and test scenario development.

First, cybersecurity gateway development, which is AI-based ship network security device (AI-SNSD), includes authentication and encryption technology for ship-to-external communication, detection and blocking of attacks based on Deep Packet Inspection (DPI) analysis of external incoming traffic, data flow control between sub-network (IT/OT/crew network), machine learning-based anomaly detection technology, attack detection and security management technology for external communication.

Second, integrated cybersecurity management system development includes 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 approval of cybersecurity type approval for 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 cybersecurity system actual operation test and test scenario includes the collection and analysis of cybersecurity current status data of existing ships, the development of cybersecurity test plan scenarios based on analyzed data, application of autonomous ships, and test and verification.

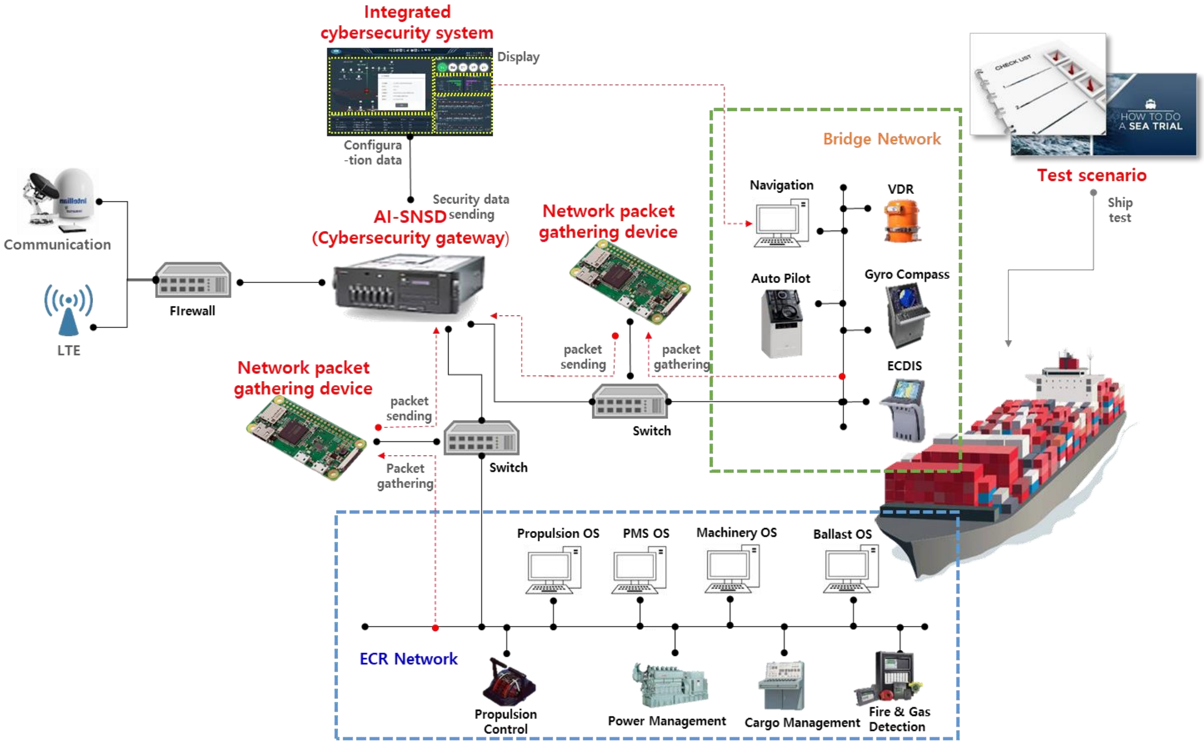


Fig. 5 Overall configuration of the cybersecurity technology development of the KASS project (Source: KASS project workshop (KASS, 2022)).

3.2 Development of Ship Network Security Equipment

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 operation such as navigation and communication, engine and propulsion systems related to ship propulsion, crew area, ship cargo management and handling. As part of a plan to reduce cyber risk in the event of a cyber attack, the cybersecurity composition diagram of autonomous ships expressed by separating, classifying, and stratifying networks by region can be shown in **Fig. 6**. Considering the current firewalls of commercial equipment, the network topology applicable to KASS ships can be shown in **Fig. 6** 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 autonomous operating equipment necessary for the operation of KASS ships, Zone-2 consists of a bridge navigation and communication system, Zone-3 is a propulsion and engine system, Zone-4 is a crew area network system, and Zone-5 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 outside (on land).

On the other hand, when the cybersecurity gateway under development in the KASS project is applied, the network topology of autonomous ships can be expressed as shown in **Fig. 7**. Here, AI-SNSD, which integrates the functions of L3 switches and firewalls, is installed without setting the firewall function of the existing L2 layer. Since there is relatively little data communication between zones, data gathering equipment is installed to check for problems that are expected to cause cyber risks, and AI-SNSD can be supplemented in preparation for long-term non-maintenance situations and protocols frequently used on ships so that it can respond to external cyber threats.

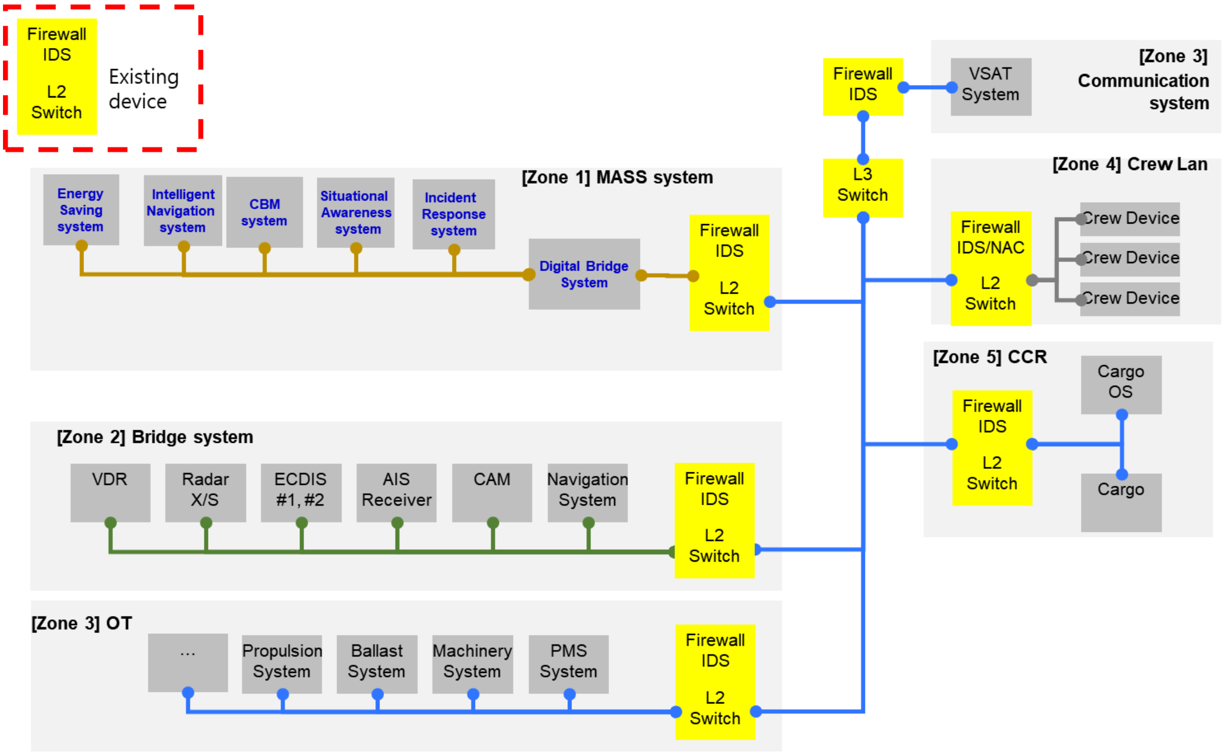


Fig. 6 Cybersecurity topology applied existing equipment by zone (Source: KASS project workshop (KASS, 2022)).

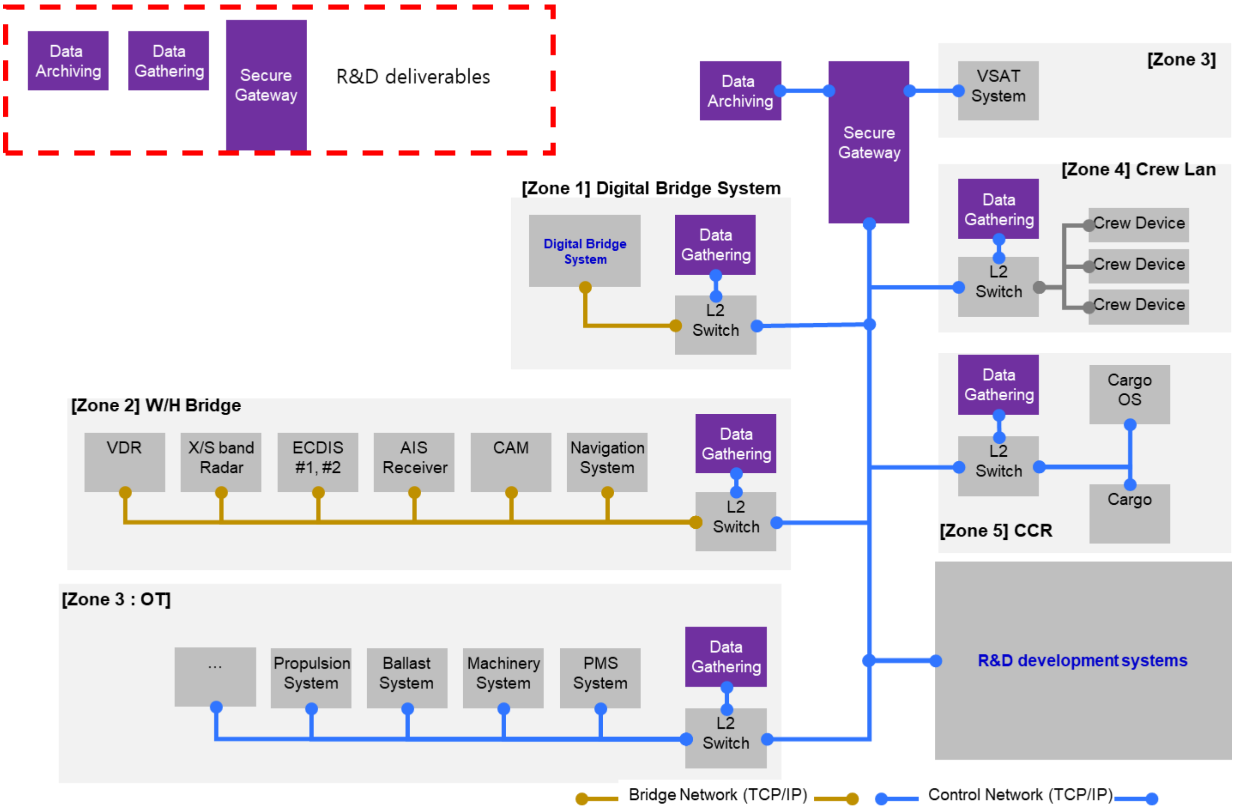


Fig. 7 Cybersecurity topology applied AI-SNSD of KASS project by zone (Source: KASS project workshop (KASS, 2022)).

Table 1 is a table comparing the main functions of existing firewall equipment and cybersecurity gateway (AI-SNSD) under development in the KASS projects. In the case of firewall functions, existing equipment is subject to rule-based & signature-based firewall policies, and KASS AI-ANSD 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 & signature-based intrusion prevention, while AI-SNSD adds machine learning-based intrusion prevention function in addition to intrusion prevention systems (IPS) of existing equipment. In the case of intrusion prevention systems, existing equipment is the same as intrusion detection systems (IDS), but AI-SNSD adds machine learning-based intrusion prevention functions just like IPS. For Anti-virus and spam, existing equipment requires separate software installation, and for AI-SNSD, deep packet inspection (DPI)-based malware detection is added. There is no significant difference in VPN functions, and for log/monitoring functions, existing equipment does not support log/monitoring functions for the entire ship network, but for AI-SNSD, it collects internal and external network traffic to support log/monitoring functions for the entire ship network. In the case of bring your own device (BYOD) management, existing equipment requires a network access control (NAC) solution separately, and in the case of AI-SNSD, it includes public key infrastructure (PKI) certificate-based BYOD device access management and authentication support. In the case of the network abnormality detection function, existing equipment supports detection function for external network traffic, and in the case of AI-SNSD, it also supports abnormality detection function for internal traffic as well as external traffic. In terms of 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 existing equipment is impossible due to the network structure, and in the case of AI-SNSD, data flow control is possible without installing a separate product. In addition, the existing equipment does not provide routing functions, but the AI-SNSD provides routing functions to include security functions suitable for KASS ships.

Table 1 Main functions comparison between existing firewall equipment and cybersecurity gateway (AI-SNSD) of KASS project (Source: KASS project workshop (KASS, 2022)).

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

4. Results and Discussions

Along with the 4th Industrial Revolution, the areas of ship, sea, and port infrastructure are also becoming digital, and accordingly, the international community is preparing for the introduction of autonomous ships in earnest. The International Maritime Organization (IMO) adopted MSC.428 (98) in 2017 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 required to consider matters related to cybersecurity when developing an autonomous ship support system (IALA, 2021b).

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

In the future, it plans to conduct verification of AI-SNSD security equipment and element technology through scenario development and application for ship test of security equipment under development in the KASS project's cybersecurity technology development.

References

(1)BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF and WSC (2018): The guidelines on cyber security onboard ships, Version 3: 4-5, 29-33.

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

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

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

(7)ISO/IEC (1994): KASS project (2022): Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model, ISO/IEC 7498-1, International Organization for Standardization/International Electrotechnical Commission.

(8)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.

Author’s Biography

Yunja YOO

He is working as a professor in the Division of Navigation Convergence Studies at Korea Maritime & Ocean University. She majored in Ocean Engineering. Her main research interests include port engineering, collision risk assessment, GHGs, cybersecurity, MASS, etc.

Kyoung-Kuk YOON

He is working as a professor in the Division of Maritime AI & Cyber Security at Korea Maritime & Ocean University. He majored in Electrical and Electronic Control Engineering. His main research interests include power electronics, motor control, automation, AI, and cyber security.

David KWAK

He is working at Penta Security Systems Inc. as a Head of Blockchain Team. He majored in Business Administration. His main research interests include blockchain, autonomous vehicle security, ship network security, machine learnin.

Myongcheol LIM

He is working at Penta Security Systems Inc. as a Head of Department in the Division of Advance Research Group. He majored in Computer Science. His main research interests include home-network Security, Industrial Control System Security.

Sangwon PARK

He is working as a researcher in the Division of Maritime Industry at Korea Maritime Institute. He majored in Marine Traffic Engineering. His main research interests include marine traffic, MASS, risk assessment, VTS, automation and cyber security.