**Input paper: [[1]](#footnote-1)** ENAV29- 5.1.2.1

**Input paper for the following Committee(s): Purpose of paper:**

(Select as appropriate)

**☐** ARM **☐** ENG **☐** PAP **☒** Input

**☒** ENAV **☐** VTS **☐** Information

**Agenda item** [[2]](#footnote-2) 5.1

**Technical domain/ Task number** 2 ……..…………………………

**Author(s)/ Submitter(s)** Korea Maritime Institute and Penta Security Systems Inc.

considerations for developing NETWORK SECURITY EQUIPMENT in maritime domainS to support MASS OPERAtION[[3]](#footnote-3)

# 1. Summary

This document provides information on cyber security in the maritime domain considering the future systems and requirements for network security equipment to support MASS operation.

## Purpose of the document

The International Maritime Organization (IMO) approved the Interim Guidelines for MASS trials at its 101st session (5 to 14 June 2019) of the Maritime Safety Committee (MSC). Relevant stakeholders, such as shipowners, authorised representatives (including coastal state, flag state, and port state), operators, and other involved parties, should take appropriate steps to ensure sufficient cybersecurity of systems and infrastructure used when conducting MASS trials in consideration of Section 2.10 (cyber risk management) of the Interim Guidelines for MASS trials.

The International Association of Marine Aids to Navigation and Lighthouse Authorities (IALA) discussed the IALA Guideline on Developments on Maritime Autonomous Surface Ships (Edition 1.0) at its 27th session of ENAV Committee and agreed to guide IALA members who may be undertaking testing and trials of MASS system. The guidelines also cover organisations implementing policies, procedures, and technical solutions, including cyber security and cyber risk management, which can be used to support the MASS environment. Section 4.1 (Considerations for provisions of marine AtoN in MASS environment) identifies ship-shore-infra-related considerations, which are MASS service requirements, vessel traffic services (VTS) environment interaction, and adaptation of traditional AtoN services to support MASS.

The Korean government commissioned the Korea autonomous surface ship (KASS) project in 2020 to develop element technologies for the MASS operation by 2025. The MASS ships developed by the KASS project target unmanned ships with an autonomy Level 3 that can be remotely controlled in coastal waters, and cybersecurity technology development is included in the element technologies.

This document aims to introduce detailed tasks for cybersecurity technology development based on the research results of the KASS project. It also proposes the development of guidelines for ‘Requirements for Network Security Equipment in Maritime Domains to support MASS Operation’ in consideration of MASS service requirements as the first step of ship-shore-infra-related considerations in the MASS environment.

## Related documents

IALA ENAV27-x.x.x IALA Guideline on Developments in Maritime Autonomous Surface Ships, Edition 1.0.

# 2. Background

## LEVELS OF AUTONOMY

IMO adopted IMO's [strategic plan](http://www.imo.org/en/About/strategy/Pages/default.aspx) (2018-2023) (IMO Resolution A.1110(30)) in December 2017, and it has a key strategic direction to ‘Integrate new and advancing technologies in the regulatory framework’. In consideration of the IMO’s strategic plan (2018-2023), the MSC [agreed](http://www.imo.org/en/MediaCentre/MeetingSummaries/MSC/Pages/MSC-98th-session.aspx) to include the issue of MASS on its agenda in 2017 and identified four degrees of autonomy for the regulatory scoping exercise (RSE) work.

The degrees of autonomy identified by IMO:

1. Degree one – Ship with automated processes and decision support. Seafarers are onboard to operate and control shipboard systems and functions. Some operations may be automated and at times be unsupervised but with seafarers onboard ready to take control;
2. Degree two – Remotely controlled ship with seafarers onboard. The ship is controlled and operated from another location. Seafarers are available onboard to take control and operate the shipboard systems and functions;
3. Degree three – Remotely controlled ship without seafarers onboard. The ship is controlled and operated from another location. There are no seafarers onboard;
4. Degree four – Fully autonomous ship. The operating system of the ship is able to can make decisions and determine actions.

## IALA GUIDELINE ON DEVELOPMENTS IN MARITIME AUTONOMOUS SURFACE SHIPS

In ENAV 27th session, IALA Guideline on Developments in Maritime Autonomous Surface Ships (Edition 1.0), IALA has agreed to provide guidance on AtoN that can be used to support a MASS environment, including:

1. Fixed shore side AtoN;
2. Floating AtoN;
3. Virtual AtoN;
4. Marking of physical AtoN using Synthetic AtoN;
5. Transmission of local and applicable meteorological and hydrographic data using application-specific messages (ASM) contained in IMO Circular SN.1/ 289;
6. Supporting the safe and efficient operations within a VTS environment
7. Ensuring communication between vessels within a VTS environment, recognising the different degrees or levels of autonomy;
8. Sharing a common operating picture for situational awareness of the waterway within the VTS environment;
9. Scoping and development of guidance on the interaction between VTS and the control centre for MASS shore control centre (SCC);
10. The tracking of both MASS and non-MASS vessels to support the traffic image;
11. Cyber Security – cyber risk management;
12. Augmentation of positioning systems;
13. Promoting standardization of data transfer.

The services delivered using physical, electronic, and virtual AtoN environments for each of the four degrees of autonomy identified by IMO could be different noting that MASS could change its level of autonomy depending on its phase of the voyage. The AtoN to be delivered to support the various degrees of autonomy for MASS operations need to be identified considering:

1. Risk mitigation;
2. Services to be rendered to support safe navigation;
3. Channels for service delivery/ provision;
4. MASS service requirements;
5. AtoN requirements in pilotage waters;
6. Remote berthing and connections to shore services;
7. VTS environment interaction;
8. Rote message transfer;
9. Local situational awareness;
10. Metrological systems and data;
11. Hydrographic systems and data;
12. AtoN availability;
13. Vessel traffic and density;
14. Adaptation of traditional AtoN services to support MASS;
15. Adoption, adaption, or extending of existing technology.

## VULNERABLE SYSTEMS OF EXISTING VESSELS from cyber threats

BIMCO et al. published ‘The Guidelines on Cyber Security Onboard Ships’ (hereafter referred to as BIMCO Guidelines) as guidance to improve the safety and security of the environment, seafarers, cargo, and ships. The guidelines are to assist in the development of a proper management strategy in accordance with relevant regulations and best practices on board a ship.

In the BIMCO Guidelines, Information Technology (IT) systems manage data and support business functions, and Operational Technology (OT) is the hardware and software that directly monitors/ controls physical devices, and processes are an integral part of the ship and must function independently of the IT systems onboard. The OT systems can be connected to the IT network for performance monitoring, remote support, etc.

Annex 1 of the BIMCO Guidelines (Version 4) provides a summary of systems onboard ships that are potentially vulnerable to cyber threats. Vulnerable systems, equipment, and technologies include 1) communication systems, 2) bridge systems, 3) propulsion, machinery management, and power control systems, 4) access control systems, 5) cargo management systems, 6) passenger or visitor servicing and management systems, 7) passenger-facing networks, 8) core infrastructure systems, and 9) administrative and crew welfare systems.

Communication systems may include eg:

1. Integrated communication systems;
2. Satellite communication equipment;
3. Voice over internet protocols (VOIP) equipment;
4. Wireless networks (WLANs);
5. Public address and general alarm systems;
6. Systems used for reporting mandatory information to public authorities.

Bridge systems may include eg:

1. Integrated navigation system;
2. Positioning systems (GPS, etc);
3. Electronic chart display information system (ECDIS);
4. Dynamic positioning (DP) systems;
5. Systems that interface with electronic navigation systems and propulsion/manoeuvring systems;
6. Automatic identification system (AIS);
7. Global maritime distress and safety system (GMDSS);
8. Radar equipment;
9. Voyage data recorders (VDRs);
10. Bridge navigational watch alarm system (BNWAS);
11. Shipboard security alarm systems (SSAS).

Propulsion, machinery management, and power control systems may include eg:

1. Engine governor;
2. Power management;
3. Integrated control system;
4. Alarm system;
5. Bilgewater control system;
6. Water treatment system;
7. Emissions monitoring;
8. Heating, ventilation, and air-conditioning monitoring;
9. Damage control systems;
10. Other monitoring and data collection systems, e.g. fire alarms.

Access control systems may include eg:

1. Surveillance systems such as CCTV network;
2. Electronic ‘personnel-on-board’ systems.

Cargo management systems may include eg:

1. Cargo control room (CCR) and its equipment;
2. Onboard loading computers and computers used for the exchange of loading information and load plan updates with the marine terminal and stevedoring company;
3. Remote cargo and container tracking and sensing systems;
4. Level indication system;
5. Valve remote control system;
6. Ballast water systems;
7. Reefer monitoring systems;
8. Water ingress alarm system.

Passenger or visitor servicing and management system may include eg:

1. Property management system (PMS);
2. Ship management systems (often including electronic health records);
3. Financial related systems;
4. Ship passenger/ visitor/ seafarer boarding access systems;
5. Infrastructure support systems like domain naming system (DNS) and user authentication/ authorisation systems;
6. Incident management systems.

Passenger-facing network may include eg:

1. Passenger Wi-Fi or local area network (LAN) internet access, for example where onboard personnel can connect their own devices;
2. Guest entertainment systems.

Core infrastructure systems may include eg:

1. Security gateways;
2. Routers;
3. Switches;
4. Firewalls;
5. Virtual private network(s) (VPN);
6. Virtual LAN(s) (VLAN);
7. Intrusion prevention systems;
8. Security event logging systems.

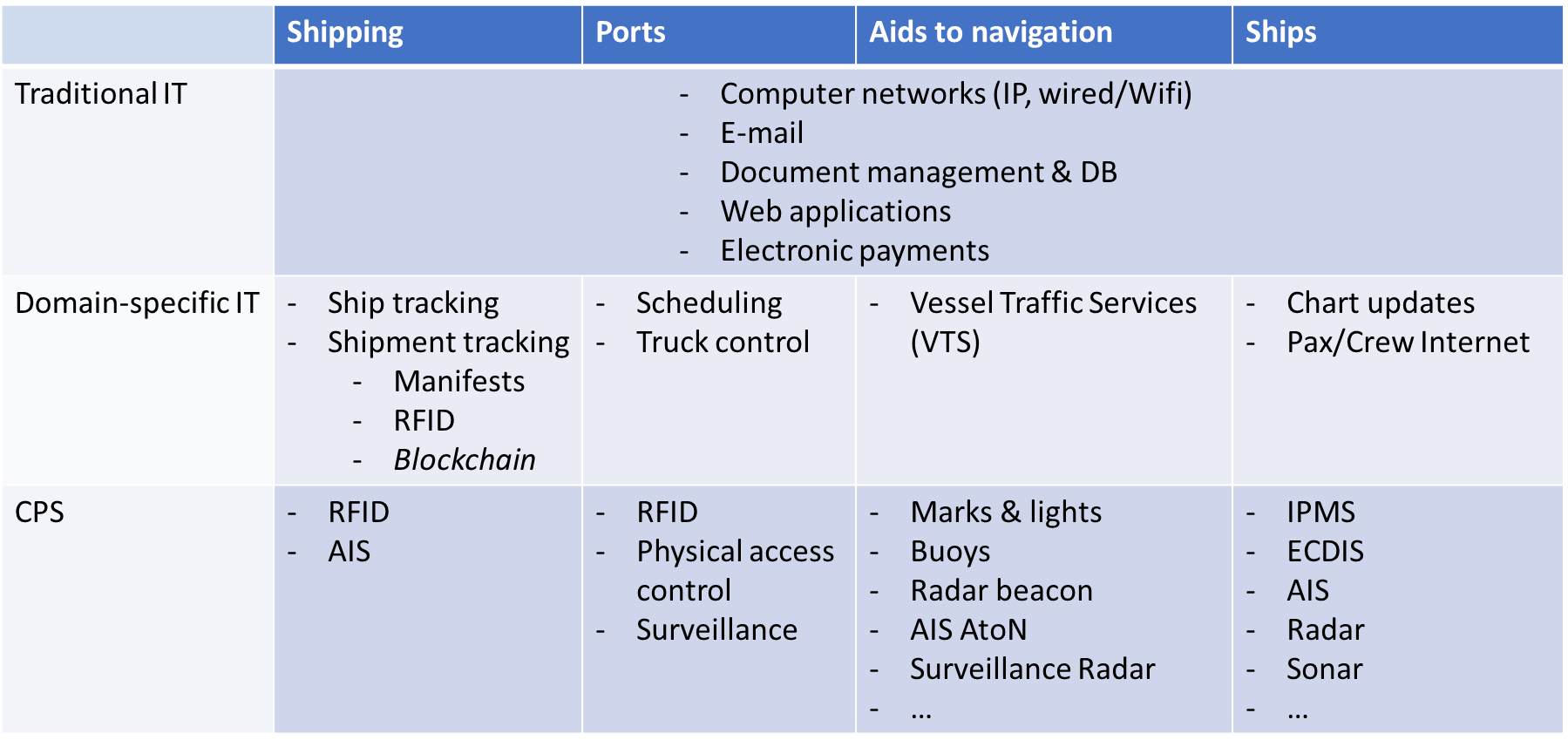
Administrative and crew welfare systems may include eg:

1. Administrative systems;
2. Crew Wi-Fi or LAN internet access, for example where onboard personnel can connect their own devices.

## CYBER security IN THE MARITIME DOMAIN considering the future systems

The workshop on cyber security was held on 12 November 2021 and from 15 to 19 November 2021 as a virtual IALA workshop. In Session 1 of the workshop, Jose Fernandez provided various cyber threats that could affect the maritime domain. The cyber threat to traditional IT includes the cyber supply chain since the hardware is asymmetrically manufactured worldwide, and software threats in the supply chain also occur. This raises the question of supply chain risk in the maritime domain with the physical cyber domain or cyber-physical system (CPS) and its different elements. The IT and OT applied to the maritime domain are presented in the following table:

Table 1 IT & OT in the maritime domain



Jose concluded that the most important cyber risks are placed on Ransomware (targeting critical infrastructure IT (non-maritime-specific)), AIS/ Radar spoofing (on a State-level or subversive actors causing short to mid-term disruption to shipping), and Hacking of AtoN systems. He also prioritised the following:

1. Rapid adoption and introduction of secure technologies ( AIS);
2. Cybersecurity standards for AtoN and VTS products;
3. Human factors (vector for ransomware; how to handle events and recover);
4. Achieving generic IT cybersecurity maturity in the organization;
5. Domain-specific cybersecurity solutions.

In Session 2, Ernest Batty provided the relationship between the increase in VTS complexity and the attack surface:

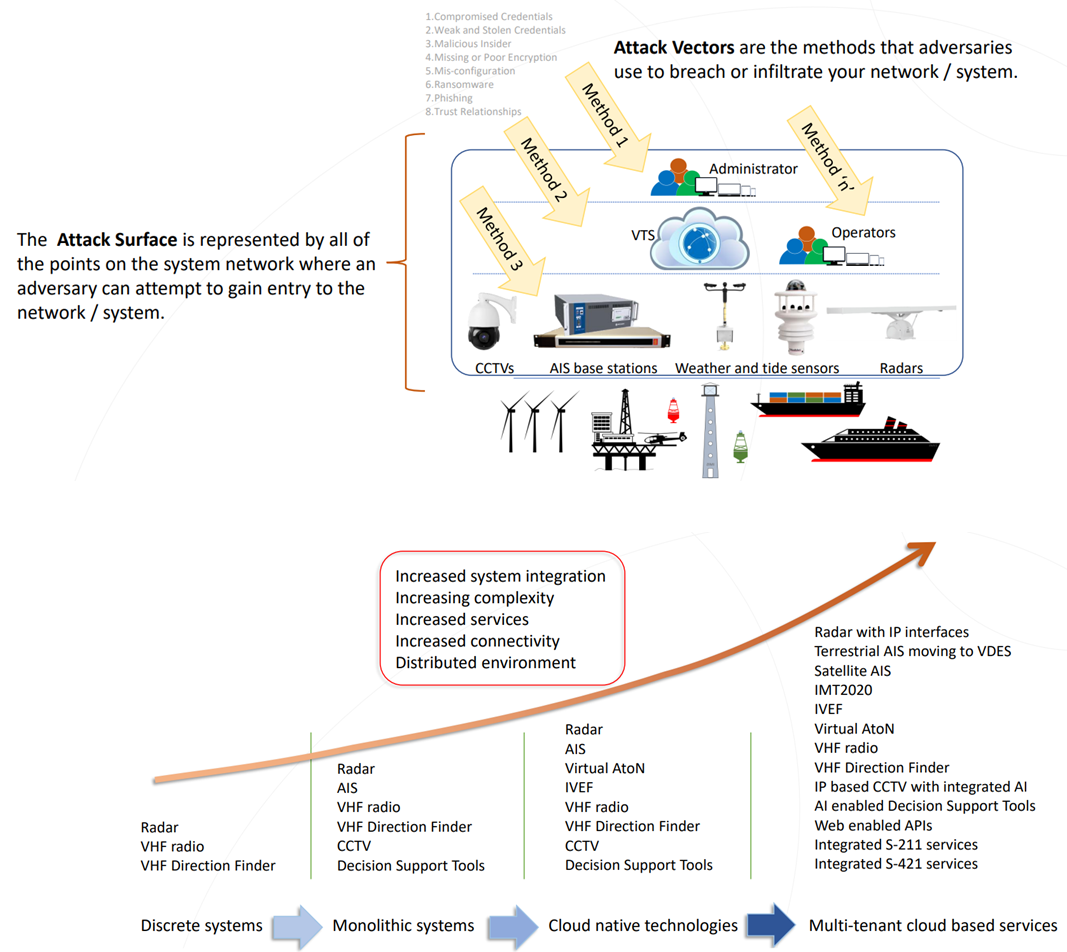


Figure 1 Relation between VTS complexity and attack surface/ vector

Future VTS systems could include an increase in services using AI, a connection with external services, sharing of data with the larger port community (using application programming Interfaces – API); the use of high bandwidth, mobile phone, and even the inclusion of MASS. The internet of things (IoT) is also expected to increase support on VTS services, which implies attack options for hackers. AI has also a role to play on decision support tools, which include external data from a wider data sourceincrease in data surface/data vectors. Ernest finally advised on what could be done in the short term in the VTS to mitigate the cyber security threat:

1. Assume zero trust

2. Create strong VTS user access protocols

3. Use strong authentication policies

4. Protect the VTS backups

5. Segment the VTS network

6. Monitor the VTS network/ system

# 3. MASS project OF Korea

## INTRODUCTION OF KASS project

The Korean government is conducting a research project in cybersecurity technology development as part of the KASS project (2020-2025). The KASS project consists of four core tasks of 1) intelligent navigation system, 2) machinery automation system, 3) testbed and performance demonstration, and 4) operation and standardization. Figure 2 shows the detailed core tasks and the associated technology by task for the technology development research project.

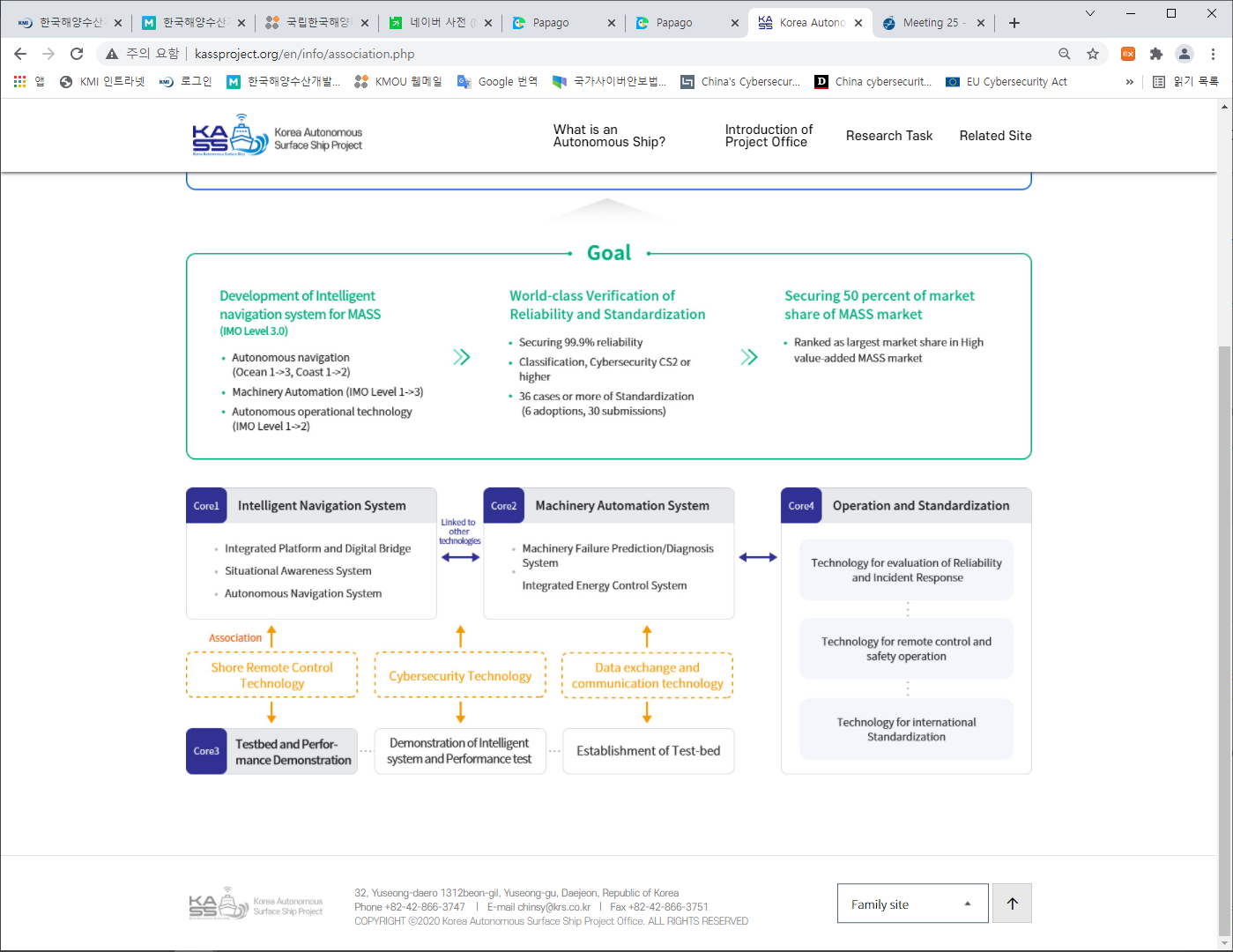


Figure 2 Core tasks with element technologies of KASS project and association between technologies

## Cybersecurity technology development

The cybersecurity technology development project, one of the detailed research tasks of the KASS project, is developing network security equipment applicable to MASS ships with an autonomy Level 3 in the maritime domain in consideration of the operation support of autonomous ships. The main protection targets of the network security equipment to support the MASS environment consist of OT networks, IT networks, and crew networks of ship systems and incoming and outgoing data. Therefore, it is necessary to develop a system that considers the linkage with ship network security equipment and external data to protect the internal and external networks of the MASS system (see Figure 2).

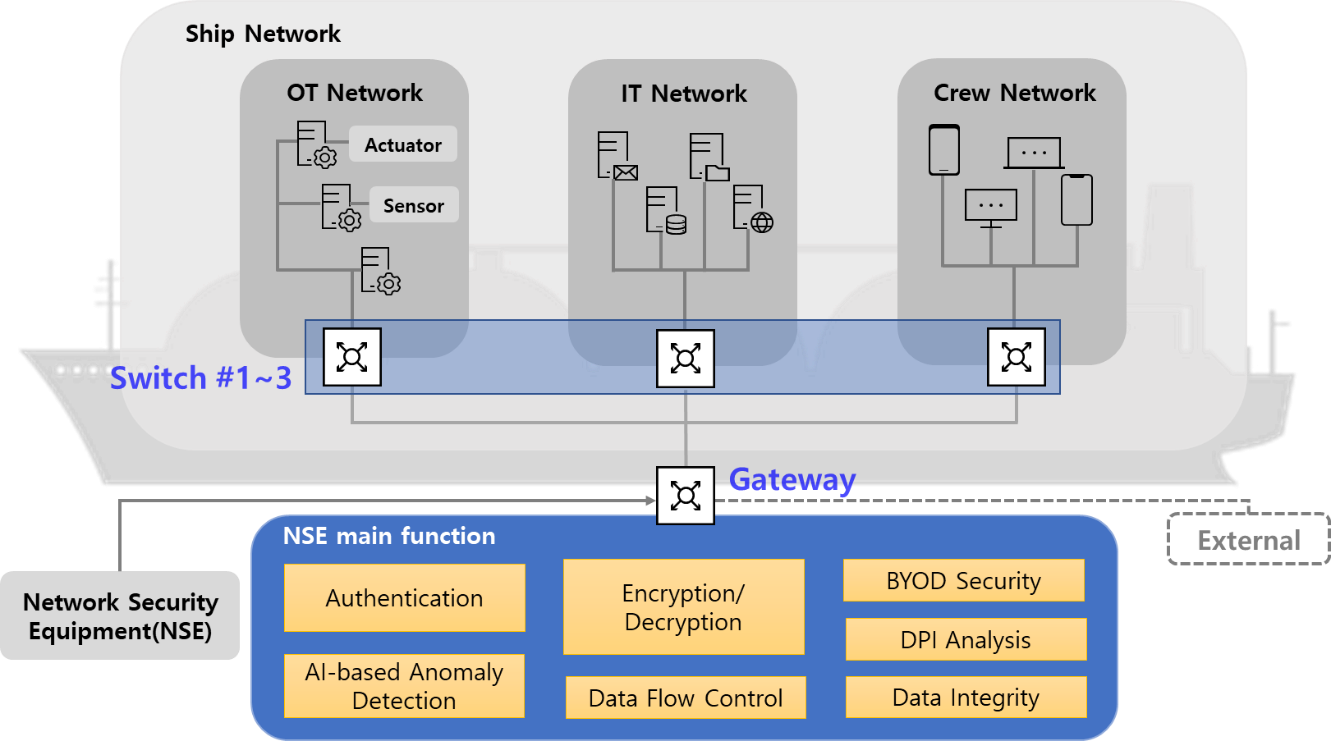


Figure 3 Network Security Equipment (NSE) main function to support MASS

MASS ships, especially unmanned ships with an autonomy Level 3-4, are a system of systems, a collection of huge digital sensors, which means that the MASS environment may be more vulnerable to cyber threats. Therefore, the KASS project aims to develop network security equipment applicable to the maritime domain to secure sufficient cybersecurity in the MASS operation environment and to design structures and develop products to ensure security (confidentiality, encryption, integrity, and availability) in the digital maritime communication environment. The details of network security equipment development are presented in Table 2.

Table 2 Main development contents of network security equipment applicable to maritime domain to support MASS environment

|  |  |
| --- | --- |
| Network security equipment product development | ▪ Provision of authentication and encryption between ship and external communication  ▪ Detection and blocking of attacks based on deep packet inspection (DPI) analysis of external incoming traffic  ▪ Data flow control for external incoming traffic  ▪ AI-based anomaly detection through monitoring of internal networks  ▪ Interworking of an integrated security management system for attack detection and collection-analysis of anomalies detection results  ▪ Provision of security for the user’s bring your own device (BYOD) device (such as malware detection)  ▪ Prevention of forgery and modulation of data on external communication with the ship and internal communication of the ship |

# 4. REQUIREMENTS for network security equipment IN MARITIME DOMAINS TO SUPPORT MASS operation

## Requirements definition

In this section, based on the results of the cybersecurity technology development research developed by the KASS project, high-level requirements to be considered when developing network security equipment to support the MASS environment are derived. The following considerations are necessary for developing network security equipment applicable when operating MASS ships:

1. Security requirements – Describe the requirements for controlling data, functions, and operational access of the target system for confidentiality and integrity of information assets;
2. System functional requirements – Describe the functions (operations) that must be performed by a target system or that must be performed by a user using the target system (however, individual functional requirements are based on the hierarchical structure analysis of the entire system, followed by detailed functional requirements for each unit task);
3. Performance requirements – Describe the performance requirements such as processing speed and time, throughput, dynamic and static capacity, and availability of the target system;
4. System interface requirements – Describe the requirements for the system interface and user interface connecting the target system to the outside, including links with other software, hardware and communication interfaces, and protocols used for information exchange with other systems (user-centred requirements, user experience, etc.);
5. Equipment composition requirements – Describe the equipment details, essential requirements (functional requirements), and components HW/ SW/ NW required for the configuration of the target system;
6. Test requirements – Describe the performance test (benchmarking test) of the equipment being introduced or the test requirements for testing and checking whether the built system is operating properly relative to the planned target.

## requirements

### Security Requirements

Security requirements include:

1. User authentication and control management;
2. Control of access to MASS network security equipment;
3. Crews’ security management;
4. Security management of external personnel;
5. Security management of MASS network security equipment;
6. Mobile media management of MASS network security equipment;
7. Anomaly detection of MASS security equipment system;
8. Self-protection function of MASS network security equipment.

### System Functional Requirements

Functional requirements include:

1. Algorithm specification of MASS network security equipment;
2. Certificate properties specifications;
3. Validity of the certificate;
4. Data collection and storage requirements;
5. Protection of saved data;
6. Measures to protect sensitive information;
7. AI-based cyber threat detection and processing of MASS network;
8. Detection and blocking of DPI analysis-based attacks of incoming traffic;
9. Detection of malware for a BYOD device;
10. Data flow control for external incoming traffic;
11. A communication standard between MASS network security equipment;
12. Communication forgery/modulation detection of MASS network security equipment;
13. MASS network security equipment and external communication function;
14. MASS network security equipment and prevention of forgery/modulation of external communication;
15. Data destruction function;
16. Warning/audit log management;
17. Requirements for data and job logs to be provided to the monitoring server;
18. Policy management of MASS network security equipment;
19. BYOD device management function;
20. Access control between internal networks;
21. Requirements for issuing and managing MASS network security equipment certificates;
22. Firewall requirements;
23. MASS wireless network security equipment requirements.

### Performance Requirements

Performance requirements include:

1. Requirements for MASS network security equipment support.

### System Interface Requirements

System interface requirements include:

1. How to link MASS network security equipment;
2. How to link with the key management system;
3. How to connect with machine learning server;
4. How to link with a data collector;
5. A plan to link with a digital bridge.

### Equipment Composition Requirements

Equipment composition requirements include:

1. Configuration of MASS network security equipment;
2. Transparency of MASS network security equipment;
3. Construction of machine learning server;
4. Deep defence strategy;
5. Data collector specification;
6. Key generation and management;
7. Operation stabilisation of MASS network security equipment;
8. Specification of MASS network security equipment.

### Test Requirements

Test requirements include general information for testing.

# 5. References

[1] BIMCO et al. The Guidelines on Cyber Security Onboard Ships, Version 4.

[2] IMO MSC 99/5, Regulatory scoping exercise for the use of Maritime Autonomous Surface Ship (MASS).

[3] IMO Resolution A.1110(30) Strategic Plan for the Organization for the Six-year Period 2018 to 2023.

[4] KASS homepage, Association between Core Technology, https://kassproject.org/en/info/association.php.

[5] Microsoft homepage, The STRIDE threat model, https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)?redirectedfrom=MSD.

[6] Khan, R. K. et al. STRIDE-based threat modelling for cyber-physical systems, Proceedings IEEE, 2017 Innovative Smart Grid Technologies Conference Europe (ISGT-Europe).

# 6. Action requested of the Committee

The ENAV Committee is requested to consider the development of The Guidelines on Requirements for Network Security Equipment in Maritime Domains in Consideration of MASS Operation.

1. Input document number, to be assigned by the Committee Secretary [↑](#footnote-ref-1)
2. Leave open if uncertain [↑](#footnote-ref-2)
3. Footer will automatically populate [↑](#footnote-ref-3)