Input paper: [[1]](#footnote-1) ENAV25-x.xx.xx

Input paper for the following Committee(s): check as appropriate Purpose of paper:

**□** ARM **□** ENG **□** PAP **□** Input

**X** ENAV **□** VTS **X** Information

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

Technical Domain / Task Number 2 Working Group 2 (Emerging Digital Technology)

Author(s) / Submitter(s) Jeoungkyu Lim (Korean Register)

Jinho Yoo (Korean Register)

Kaemyoung Park (Korean Register)

Introduction of Cyber Security Standards applicable to Maritime Digital Devices

# Summary

This document introduces international cyber security standards for equipment that could be applicable to maritime digital devices.

## Purpose of the document

This document is to inform IALA of cyber security international standards applicable to maritime digital devices. Following the document ENAV24-7.1, committee work programme for 2018-2022, IALA will develop the cyber security for maritime digital devices operations recommendation / guideline.

The Korean Register proposes that the committee refers to international cyber security standards in the development of IALA’s cyber security recommendations / guideline.

## Related documents

None.

# Background

The Cyber Security concepts and solutions have mostly been developed for office IT systems and applications. Cyber security for the maritime domain not only comes with different security priorities, it also comes with different management & operational characteristics and requirements.

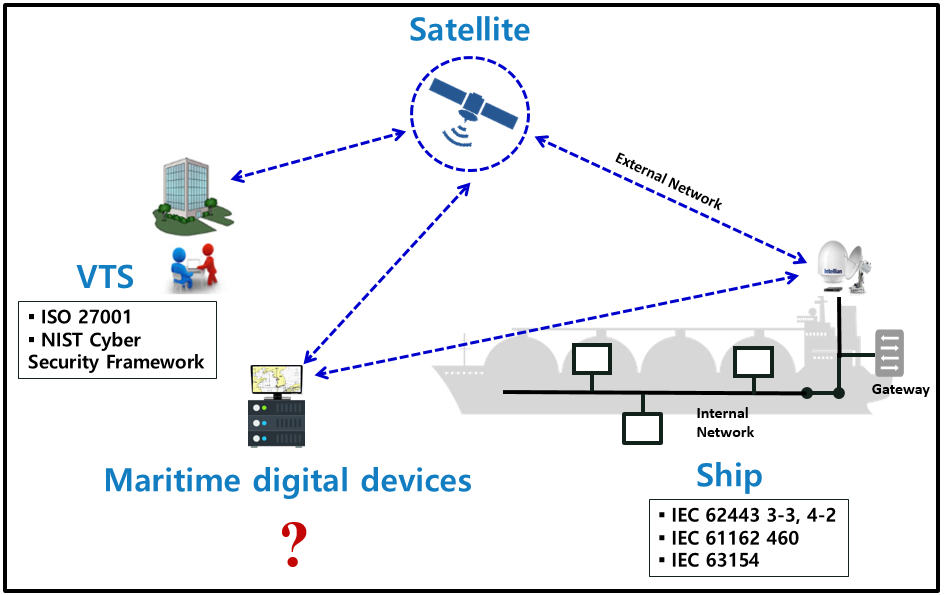
According to the emerging technology needs in the maritime domain, Smart maritime digital devices will be developed which is expected to provide additional information. This new maritime digital devices device necessarily requires cyber security.

# Discussion

Cyber ​​security of VTS, ships and maritime digital devices, etc. is emerging as a critical issue for the maritime environment and safety. Since each characteristic is different, it is not advisable to apply one cyber security standard to all areas. Therefore, the following strategic decisions are needed in applying international standards.

Table 1. Applicable cyber security standard to VTS, Ship and Maritime digital devices

|  |  |  |
| --- | --- | --- |
| Category | Standard | Title |
| **VTS** | ISO 27001 | Information security management |
| NIST | NIST Cybersecurity framework |
| **Ship** | IEC 62443 4-2 | Technical security requirements for IACS components |
| IEC 62443 3-3 | System security requirements and security levels |
| IEC 61162 460 | Maritime navigation and radiocommunication equipment and systems – digital interfaces Part 460: Ethernet interconnection – safety and security |
| IEC 63154 | Maritime navigation and radiocommunication equipment and systems – Cybersecurity – General requirements, methods of testing and required test results |
| **Maritime digital devices** | To be considered above international standards as a reference | |



*Figure 1. Maritime Data Transfer and Cyber Security Standartd Overview*

## VTS(Vessel Traffic Services) Applicable Cyber Security Standard

VTS is a service implemented by a Competent Authority, designed to improve the safety and efficiency of vessel traffic and to protect the environment. The service should have the capability to interact with the traffic and respond to traffic situations developing in the VTS Area.

Cyber ​​security standards that organizations should refer includes **ISO 27001** and the **NIST Cyber ​​Security Framework**.

### ISO 27001 Requirement

It is important that the information security management system is part of and integrated with the organization’s processes and overall management structure and that information security is considered in the design of processes, information systems, and controls. It is expected that an information security management system implementation will be scaled in accordance with the needs of the organization. This International Standard can be used by internal and external parties to assess the organization’s ability to meet the organization’s own information security requirements. [1]

Table 2. ISO 27001 : 2013 Requirement

|  |  |  |  |
| --- | --- | --- | --- |
| **Part** | **Code** | **Sub-Category** | **Q’ty** |
| **Management**  **Security** | 5.1 | Information security policies | 2 |
| 6.1 | Organization of information security | 7 |
| 7.1 | Human resource security | 6 |
| 8.1 | Asset management | 10 |
| 12.1 | Operations security | 14 |
| 15.1 | Supplier relationships | 5 |
| 16.1 | Information security incident management | 7 |
| 17.1 | Information security aspects of business continuity management | 4 |
| 18.1 | Compliance | 8 |
| **Technical**  **Security** | 9.1 | Access control | 14 |
| 10.1 | Cryptography | 2 |
| 13.1 | Communications Security | 7 |
| 14.1 | System acquisition, development and maintenance | 13 |
| **Physical**  **Security** | 11.1 | Physical and environmental security | 15 |

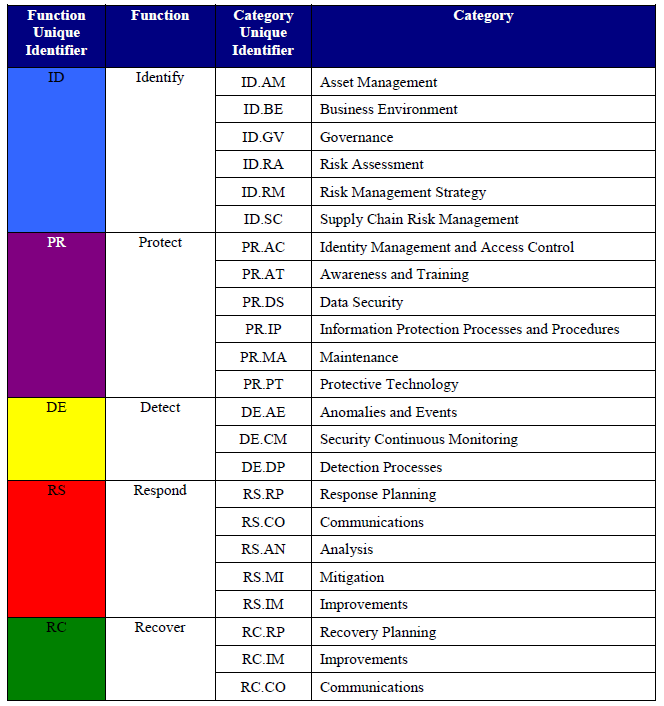
### NIST Cyber Security Framework

The NIST Cyber Security Framework focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization’s risk management processes. The Framework consists of three parts: the Framework Core, the Implementation Tiers, and the Framework Profiles. The Framework Core is a set of cybersecurity activities, outcomes, and informative references that are common across sectors and critical infrastructure. Elements of the Core provide detailed guidance for developing individual organizational Profiles. Through use of Profiles, the Framework will help an organization to align and prioritize its cybersecurity activities with its business/mission requirements, risk tolerances, and resources. The Tiers provide a mechanism for organizations to view and understand the characteristics of their approach to managing cybersecurity risk, which will help in prioritizing and achieving cybersecurity objectives.

An organization can use the Framework as a key part of its systematic process for identifying, assessing, and managing cybersecurity risk. The Framework is not designed to replace existing processes; an organization can use its current process and overlay it onto the Framework to determine gaps in its current cybersecurity risk approach and develop a roadmap to improvement. Using the Framework as a cybersecurity risk management tool, an organization can determine activities that are most important to critical service delivery and prioritize expenditures to maximize the impact of the investment.[2]

Table 3. Framework Core

|  |  |
| --- | --- |
| **Function** | **Description** |
| **Identify** | Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities. |
| **Protect** | Develop and implement appropriate safeguards to ensure delivery of critical services. |
| **Detect** | Develop and implement appropriate activities to identify the occurrence of a cybersecurity event |
| **Respond** | Develop and implement appropriate activities to take action regarding a detected cybersecurity incident. |
| **Recover** | Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. |



*Figure 2. Function and Category Unique Identifiers*

## Maritime digital devices Applicable Cyber Security Standard

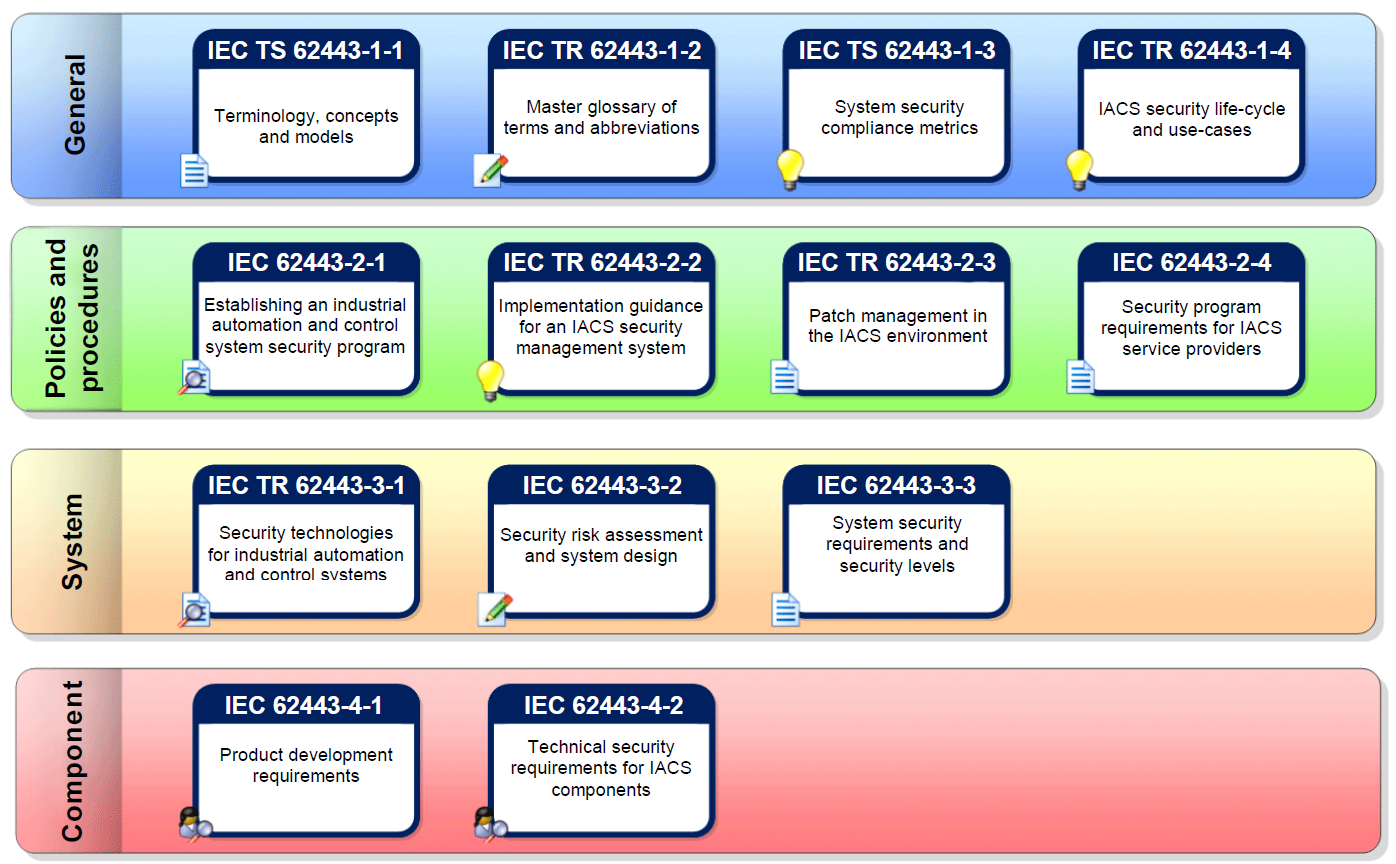
Maritime digital devices can be any kind of sensors, device or system equipped with IoT or 5G terminal communication.

It is recommended that the during the development of Cyber ​​security standards applicable to maritime digital devices, the following standards are taken into consideration: **IEC 62443 4-2, IEC 61162-460 and IEC 63154**. This section provides an overview of these standards.

### IEC 62443 series overview

The international industrial security standard IEC 62443 is a security framework defined by the International Electrotechnical Commission (IEC). It covers both organisational and technical aspects of security, without being prescriptive regarding the technical solution. In the set of corresponding documents, security requirements are defined, which target the solution operator and the integrator, but also the product vendor.

The primary goal of the IEC 62443 series is to provide a flexible framework that facilitates addressing current and future vulnerabilities in IACS(industrial automation and control system) and applying necessary mitigations in a systematic, defensible manner. It is important to understand that the intention of the IEC 62443 series is to build extensions to enterprise security that adapt the requirements for business IT systems and combines them with the unique requirements for strong integrity and availability needed by IACS [4].



*Figure 3. IEC 62443 series overview*

### IEC 62443 3-3 : system security requirements and security level

This standard expands the seven foundational requirements (FRs) defined in IEC 62443 1-1 into a series of system requirements (SRs). Each SR has a baseline requirement and more requirement enhancements (REs) to strengthen security. All seven FRs have a defined set of four SLs.

Table 4. Foundational Requirements (FRs) and Purpose

|  |  |
| --- | --- |
| **FR(Foundational Requirement)** | **Purpose** |
| FR1.Identification and authentication control (IAC) | Identify and authenticate all users (humans, software processes and devices), prior to allowing them access to the system or assets. |
| FR2. User Control (UC) | Enforce the assigned privileges of an authenticated user (human, software process or device) to perform the requested action on the component and monitor the use of these privileges. |
| FR3. System Integrity (SI) | Ensure the integrity of the component to protect against unauthorized manipulation or modification. |
| FR4. Data confidentiality (DC) | Ensure the confidentiality of information on communication channels and in data stored in repositories to protect against unauthorized disclosure. |
| FR5. Restricted data flow (RDF) | Segment the control system via zones and conduits to limit the unnecessary flow of data. |
| FR6. Timely response to events(TRE) | Respond to security violations by notifying the proper authorities, reporting needed evidence of the violation and taking timely corrective action when incidents are discovered. |
| FR7. Resource availability (RA) | Ensure the availability of components against the degradation or denial of essential services. |

Table 5. Security Levels (SLs) definition

|  |  |
| --- | --- |
| **Security Level(SL)** | **Purpose** |
| SL 1 | Prevent the unauthorized disclosure of information via eavesdropping or casual exposure |
| SL 2 | Prevent the unauthorized disclosure of information to an entity actively searching for it using simple means with low resources, generic skills and low motivation. |
| SL 3 | Prevent the unauthorized disclosure of information to an entity actively searching for it using sophisticated means with moderate resources, IACS specific skills and moderate motivation. |
| SL 4 | Prevent the unauthorized disclosure of information to an entity actively searching for it using sophisticated means with extended resources, IACS specific skills and high motivation. |

### IEC 62443 4-2 standard : Technical security requirements for IACS components

This standard provides detailed technical control system component requirements (CRs) associated with the seven foundational requirements (FRs) described in IEC 62443 1‑1 [[3]](#_bookmark139) including defining the requirements for control system capability security levels and their components, SL-C(component). Component requirements for four types of components: software application, embedded device, host device and network device. Thus the CRs for each type of component will be designated as follows: [[5]](#_bookmark139)

* Software application requirements (SAR); one or more software programs and their dependencies that are used to interface with the process or the control system itself (for example, configuration software and historian)
* Embedded device requirements (EDR) : special purpose device designed to directly monitor or control an industrial process
* PLC (Programmable Logic Controller), IED (Intelligent Electronic Device)
* Host device requirements (HDR) : general purpose device running an operating system (for example Microsoft Windows OS or Linux) capable of hosting one or more software applications, data stores or functions from one or more suppliers
* Operator workstation, Data historian
* Network device requirements (NDR) : device that facilitates data flow between devices, or restricts the flow of data, but may not directly interact with a control process
* Switch, VPN (Virtual Private Network)

## Overview of IEC 61162 standards

### IEC 61162 series : Maritime navigation and radiocommunication equipment and systems – digital interfaces

Table 6. IEC 61162 series overview

|  |  |
| --- | --- |
| **Part** | **Title** |
| IEC 61162-1(NMEA 0183) | Part 1: Single talker and multiple listener |
| IEC 61162-2(NMEA 0183) | Part 2: Single talker and multiple listener, high speed transmission |
| IEC 61162-3(NMEA 2000) | Part 3: Serial data instrument network |
| IEC 61162-450 | Part 450: Ethernet interconnection |
| IEC 61162-460 | Part 460: Ethernet interconnection – safety and security |

### IEC 61162-460 : Ethernet interconnection – safety and security

This standard is an add-on to the IEC 61162-450 standard where higher safety and security standard are needed due to higher exposure to external threats or to improve network integrity. This standard provides requirements and test method for equipment to be used in an IEC 61162-460 compliant network as well as requirements for the network itself and requirements for interconnection from the network to other networks.

*Figure 4. Functional overview of IEC 61162-460 requirement applications*

Table 7. IEC 61162-460 component definition

|  |  |
| --- | --- |
| **Name** | [**Definition**](http://www.3gpp.org/ftp/Specs/html-info/21-series.htm) |
| 460-Network | Network which consists of only 460-Nodes, 460-Switches, 460 Forwarder, 460-Gateway and 460- Wireless gateway as well as 450-Nodes |
| 460-Node | Device complaint with the requirements of a 450-Node and which satisfies the safety and security requirements as specified in this standard |
| 460-Switch | Network infrastructure device used to interconnect nodes on a 460-Network and which satisfies the safety and security requirements as specified in this standard |
| 460-Forwarder | Network infrastructure device that can safely exchange data stream between a 460- Network and other controlled networks including other 460-Networks |
| 460-Gateway | Network infra structure device that connects 460-Netowrk and uncontrolled networks and which satisfies the safety and security requirements as specified in this standard |
| 460-Wireless gateway | Network infrastructure device that connects a 460-Netowrk and wireless networks and which satisfies the safety and security requirements as specified in this standard |

## Overview of IEC 63154 standard : Maritime Navigation and Radiocommunication equipment and systems – cyber security – General requirements, methods of testing and required test results

### Publication

This standard is still in development, and is expected to be published in April 2021.

### Scope

This document specifies requirements, methods of testing and required test results for shipborne navigation and radiocommunication equipment where standards are needed to provide a basic level of protection against cyber incidents:

a) shipborne radio equipment forming part of the global maritime distress and safety system (GMDSS) mentioned in the International Convention for Safety of Life at Sea(SOLAS) as amended, and by the Torremolinos International Convention for the Safety of Fishing Vessels as amended and to other shipborne radio equipment, where appropriate;

b) shipborne navigational equipment mentioned in the International Convention for Safety of Life at Sea (SOLAS) as amended, and by the Torremolinos International Convention for the Safety of Fishing Vessels as amended,

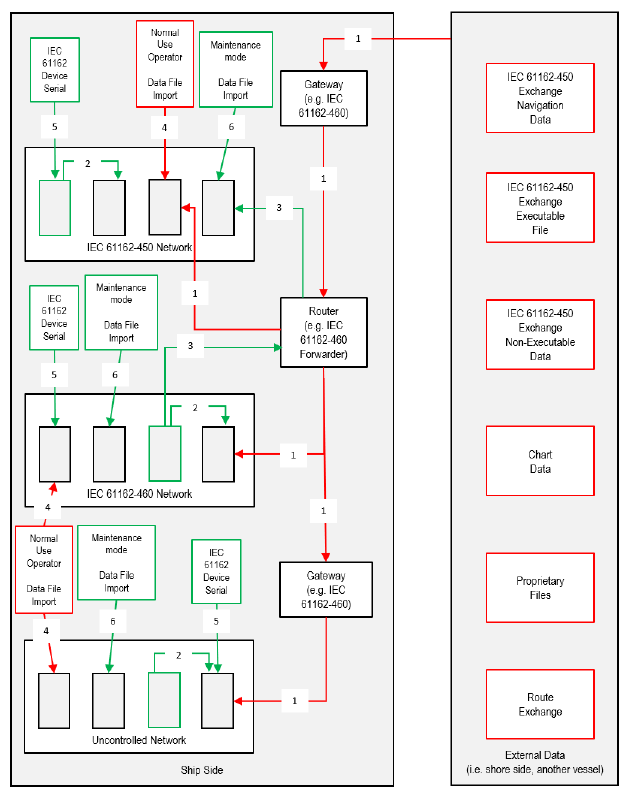
c) other shipborne navigational aids, and Aids to Navigation (AtoN), where appropriate.

Table 8. IEC 63154 overview

|  |  |
| --- | --- |
| **Part** | **Title** |
| Module A | Data files |
| Module B | Execution of executables |
| Module C | User authentication |
| Module D | System defence |
| Module E | Network access |
| Module F | Access to operating system |
| Module G | Booting environment |
| Module H | Maintenacne mode |
| Module I | Protection against unintentional crash caused by user input |
| Module J | Intefaces for removable devices including USB |
| Module K | IEC 61162-1 or IEC 61162-2 as interfacce |
| Module L | IEC 61162-450 as interface |
| Module M | IEC other interfaces |
| Module N | Software maintenance |
| Module O | Remote maintenance |
| Annex A | [Guidance on implementing virus and malware protection ontype approved equipment for IMO SOLAS regime and practical limitations](#_bookmark86) |
| Annex B | File authentication |
| Annex C | [Methods of authentication of data files and executables – some](#_bookmark93) examples |
| Annex D | USB class codes |
| Annex E | Cyber security configuration document for equipment |
| Annex F | Guidance on interconnection between networks |

### Applications

Shipborne navigation and radiocommunication equipment are generally installed in restricted areas, e.g. at the bridge where access is defined by the IMO International Ship and Port Facility Security (ISPS) Code or in an electronic locker room or in a closed cabinet. These restricted areas are referred to as secure areas in this document. This is based on the importance of navigation and radiocommunication equipment for the safety of navigation. These restricted areas are in the following considered as areas with implemented security and access measures. These measures are defined in the ship security plan of the individual vessel derived from ISPS code, they are not part of this standard and not specified or tested in the context of this standard. Accordingly, equipment installed in these physically restricted access areas are understood to benefit from these security measures. This standard provides mitigation against the remaining cyber vulnerabilities for equipment installed in such areas. Following the above this standard includes consideration of cyber threats from unauthorized users, from removable external data sources (REDS) like USB sticks, from network segments installed outside of the restricted areas including interfaces to external networks e.g. ship to shore, ship to ship. The risk of an incident is different between equipment/system boundaries and the mitigating security measures required should be appropriate to the identified risk of incidents and proportional to the identified adverse consequences. Boundaries take the form of both physical, such as direct access to the equipment via its ports (e.g. network, USB, import of digital files, software installation) and logical (e.g. connections over a network, transfer of data, operator use). A key tenet of cyber security is authentication of who has provided the data and verification that what is being provided has not been tampered with. To reflect the difference in cyber security risk the needs for authentication and verification between secure and non-secure areas are illustrated in the Figure 1. The methods for achieving authentication and verification are described in each Module of this standard. [[7]](#_bookmark139)



*Figure 5. Some Examples of Data transfer*

# Conclusion

Cyber security will be essential for the operation of ships with highly integrated and connected systems installed such as MASS (Maritime Autonomous Surface Ships). In this context, KR propose IEC 62443 4-2, IEC 61162-460, IEC 63154 standard to be considered as a direction of cyber security applied to maritime digital devices.

# References

1. ISO 27001 : 2013 *Information security management system requirements*
2. *NIST Cybersecurity Framework*
3. IEC 62443 1-1 *Security for industrial automation and control system, Concepts and models*
4. IEC 62443 3-3 *Security for industrial automation and control system, System security requirements and security levels*
5. IEC 62443 4-2 *Security for industrial automation and control system, Technical security requirement for IACS components*
6. IEC 61162 460 *Maritime navigation and radiocommunication equipment and systems – digital interfaces, Ethernet interconnection – safety and security*
7. IEC 63154 *Maritime navigation and radiocommunication equipment and systems – cyber security – General requirements, methods of testing and required test results.*

# Action requested of the Committee

The Committee is requested to:

1. Note the this information paper provided by Korean Register, and take action as appropriate

2. Review the IEC 62443 4-2, IEC 61162-460, IEC 63154 standards while developing IALA cyber security recommendation / guideline for maritime digital devices operations or other maritime ICT equipment

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