Input paper: [1] ENAV24-6.1.14

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]	6
Technical Domain / Task Number [2]	Working Group 3 (Emerging Digital Technology)
Author(s) / Submitter(s)	Jeoungkyu Lim (Korean Register of shipping)
	Jinho Yoo (Korean Register of shipping)
	Kaemyoung Park (Korean Register of shipping)

Introduction of cyber security type approval applicable case based on IEC 62443 and IEC 61162-460 standards

1 SUMMARY

This document introduces cyber security type approval applicable case for maritime ICT equipment based on IEC 62443 and IEC 61162-460 standards and examples of applied cases.

1.1 Purpose of the document

This document is to inform IALA of cyber security type approval applicable case based on IEC 62443 standard, Technical security requirements for IACS (Industrial Automation and Control System) components, and examples of applied cases.

Following the document ENAV24-7.1, committee work programme for 2018-2022, IALA will develop the cyber security for AtoN operations recommendation / guideline.

The Korean Register proposes to committee refer to international standard of cyber security in other domain to be developed IALA's cyber security recommendations

1.2 Related documents

None.

2 BACKGROUND

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

The risk of maritime cyber-attacks in the maritime domain is also increasing globally, the importance of maritime cyber security has emerged in the international community such as International Maritime

1 Input document number, to be assigned by the Committee Secretary
2 Leave open if uncertain

Organization (IMO), International Association of Classification Societies (IACS), Baltic and International Maritime Council (BIMCO), Oil Companies International Marine Forum (OCIMF).

3 DISCUSSION

This clause describes IEC 62443 and IEC 61162-460 standards.

3.1 Overview of IEC 62443 standards

3.1.1 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 [3].

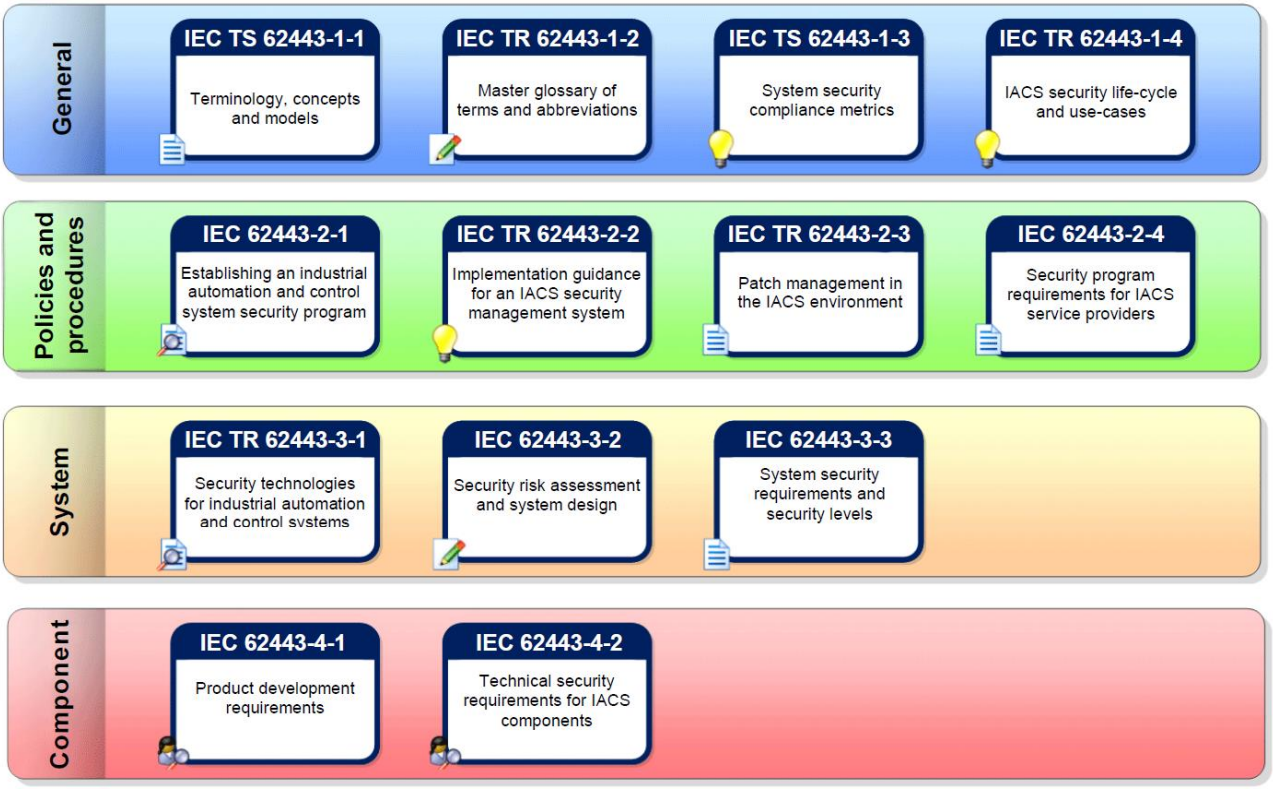


Figure 1. IEC 62443 series overview

3.1.2 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 2. 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. Use 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 2. 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.

3.1.3 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 [1] 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:

- 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)

3.2 Overview of IEC 61162 standards

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

Table 3. 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

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

This standard add-on 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.

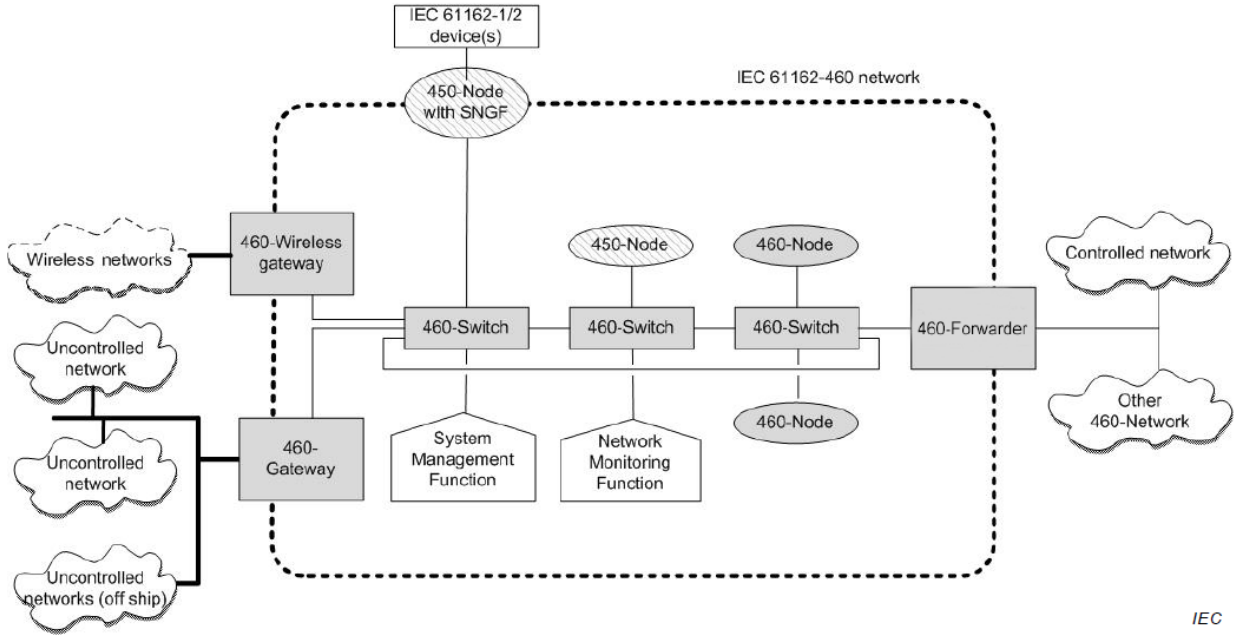


Figure 2. Functional overview of IEC 61162-460 requirement applications

Table 3. IEC 61162-460 component definition

Name	Definition
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

3.3 Development of KR guidance based on IEC 62443 and IEC 61162-460

3.3.1 Guidance for Type Approval of Maritime Cyber Security

As a classification society, KR conducts type approval of cyber security system and devices in accordance with KR Rules based on IEC 62443 4-2 and IEC 61162-460, granting to systems that meet class requirements and therefore can be installed on smart or autonomous ships.

- IEC 62443 4-2 : Security Level, Component requirements
- IEC 61162 460 : Terminology of devices (node, network, forwarder, gateway)

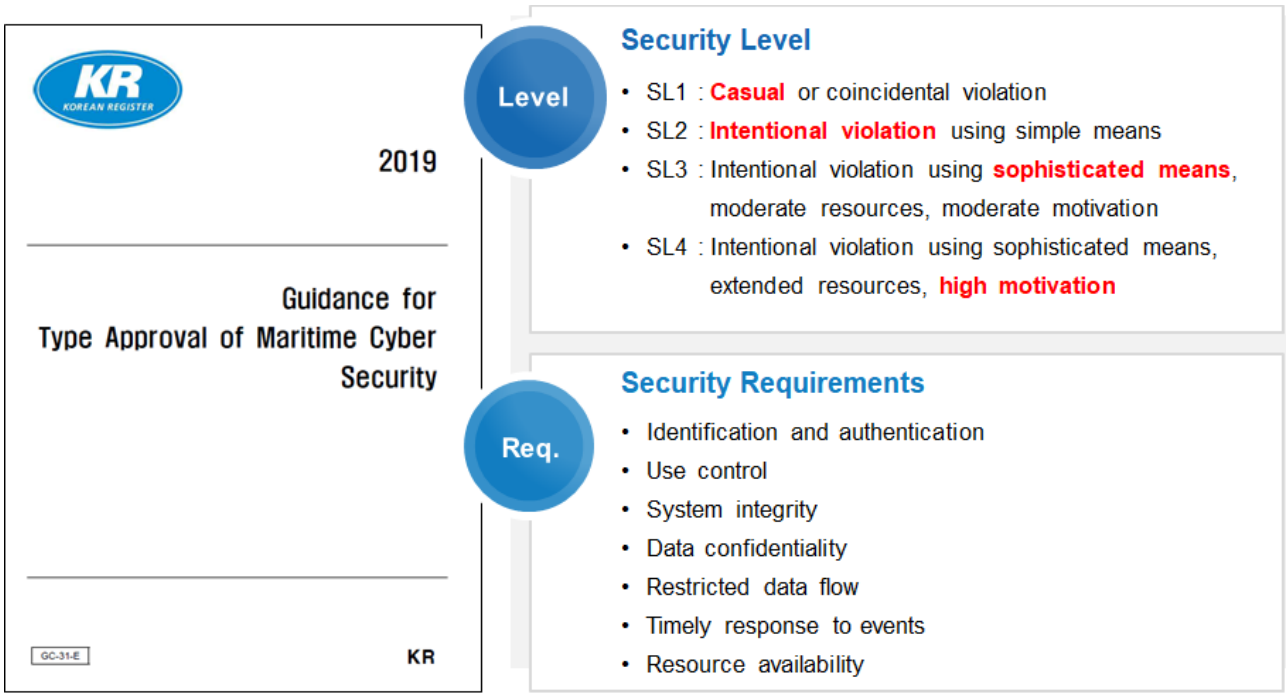


Figure 3 Guidance for Type Approval of Maritime Cyber Security

Table 3. Composition of KR Guidance

Section	Title
Section 1	General
Section 2	Identification and Authentication
Section 3	Use Control
Section 4	System Integrity
Section 5	Data Confidentiality
Section 6	Restricted Data Flow
Section 7	Timely Response to Events
Section 8	Resource Availability
Section 9	Software Application Requirements
Section 10	Embedded Device Requirements

Section 11	Host Device Requirements
Section 12	Network Device Requirements

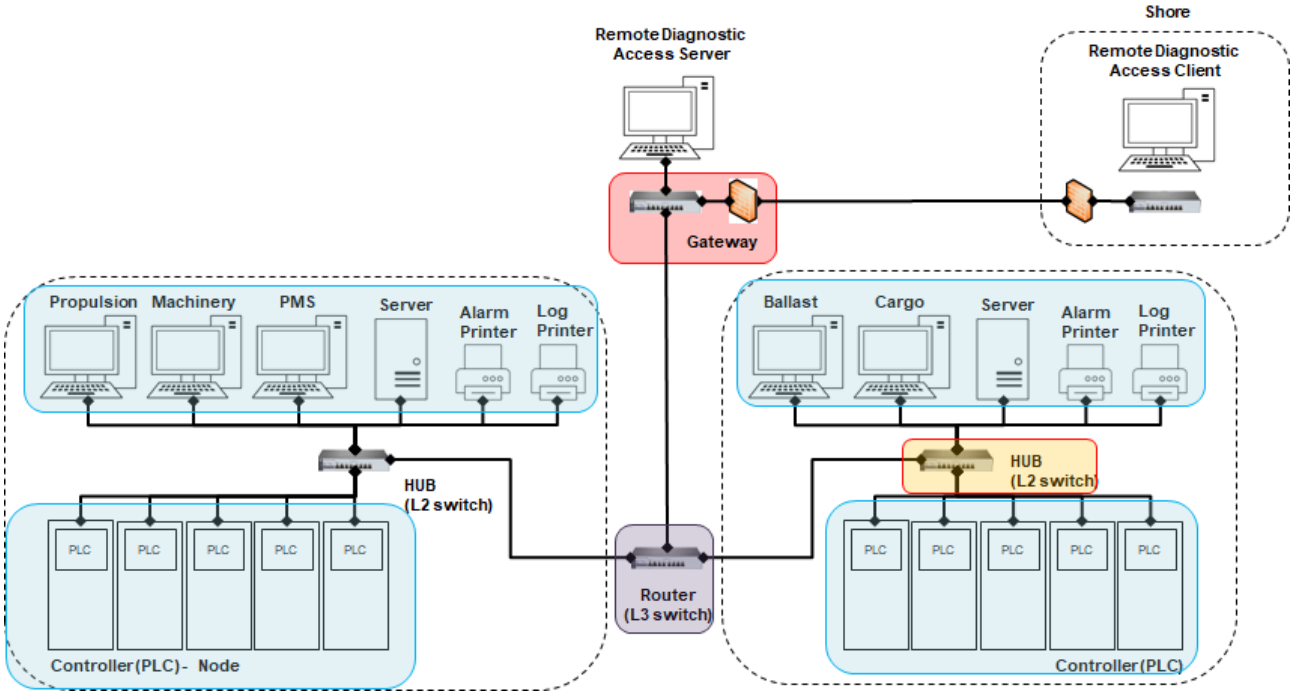


Figure 4 Scope of Component: Node, Switch, Router, Gateway

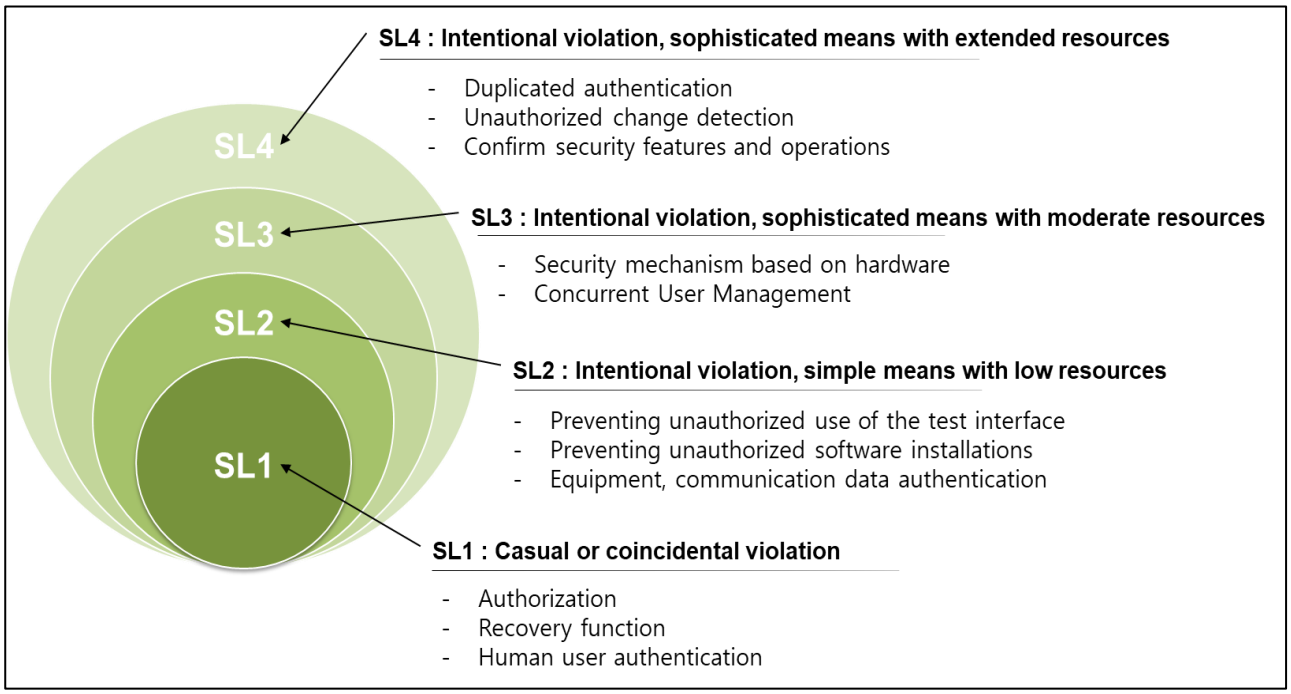


Figure 5 Concept of Security Level and requirements

3.3.2 Procedures for cyber security type approval

The Society examines below document where deemed appropriate, those are to be approved and returned to the manufactures.

- Functional specification
- System topology

- System drawing
- List of assets
- Test program related to cyber security
- Manual for user and/or operator
- Risk assessment report

After completion of the document reviews, the type test are to be carried out for the test products in the presence of the surveyors in accordance with the approved type test program and test method described in each section of the Guidance or equivalent method thereof.

3.3.3 Explanation of requirments : Section 2 Identification and Authentication - Human user identification and authentication(code : 201)

Identifier means a symbolic pattern unique within the security domain that identifies, displays, or names the entity claiming identity, and authentication means proof of identification request. Human user identification and authentication requires the ability to verify that the user is an appropriate user.

SL	Title
1	▪ Components should provide the capability to identify and authenticate all human users on all interfaces capable of human user access ▪ User identification and authentication shouldn't hamper fast, local emergency actions
2	▪ Components should provide the capability to employ multifactor authentication for all human user access to the component
3,4	▪ Components should provide the capability to uniquely identify and authenticate all human users

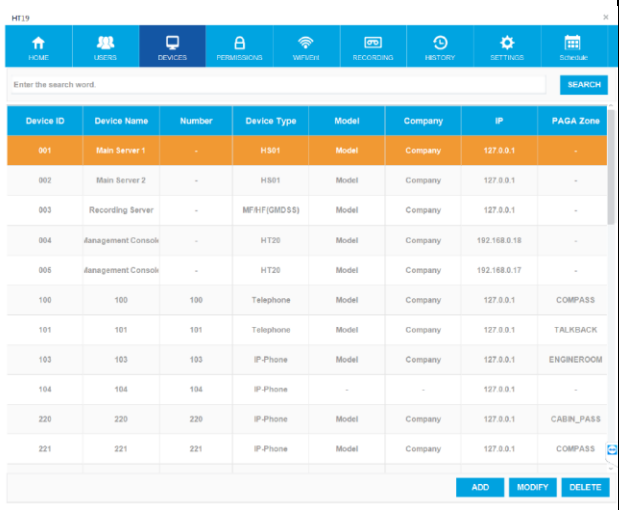
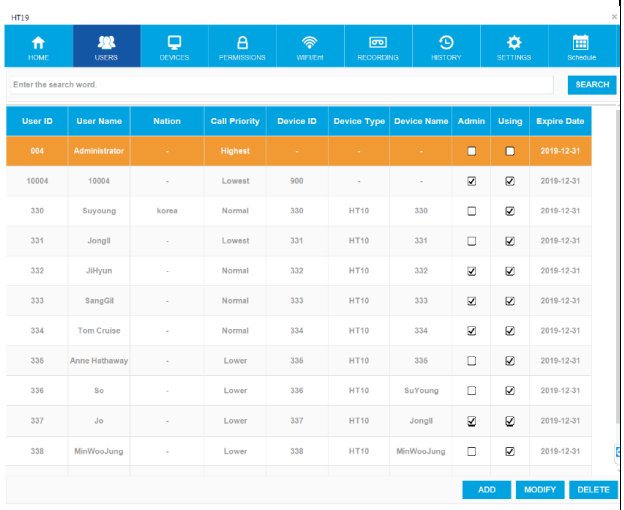
- **SL1** first requires identification and authentication on all interfaces that allow human user access. An example of this may be a human machine interface (HMI).
- **SL2** requires that in addition to SL1, every human user is uniquely identified. User identification and authentication can be role based or group based. In order to meet the SL2 requirements, it is necessary to create and manage individual identifiers for individual users, even if they are role-based or group-based identifier configurations.
- **SL3, SL4** require multi-factor authentication in addition to SL1 and SL2. The authentication factor is divided into three factors. **Knowledge-based factors (passwords, PIN codes, etc.**) using what you know, **ownership-based factors (security cards, OTP, etc.)** using what you have. There is an **attribute-based factor (fingerprint recognition, etc.)** that uses its own unique attribute. Multifactor authentication refers to a method of authenticating using two or more factors.

Knowledge based factor	Ownership based factor	Attribute based factor
		

3.3.4 Example of approval and verification of requirement : Section 2 Identification and Authentication - Human user identification and authentication(code : 201)

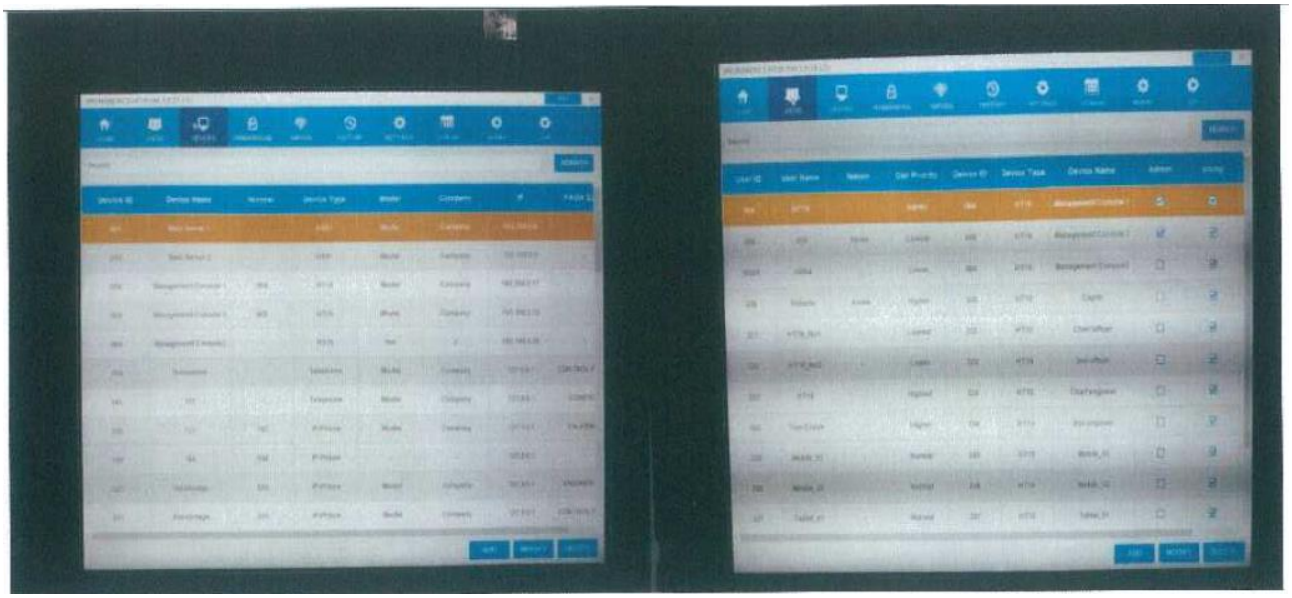
The Society examines document review for approval and type test for verification according to components type and security level.

<Document Review>

Device List	User List
	

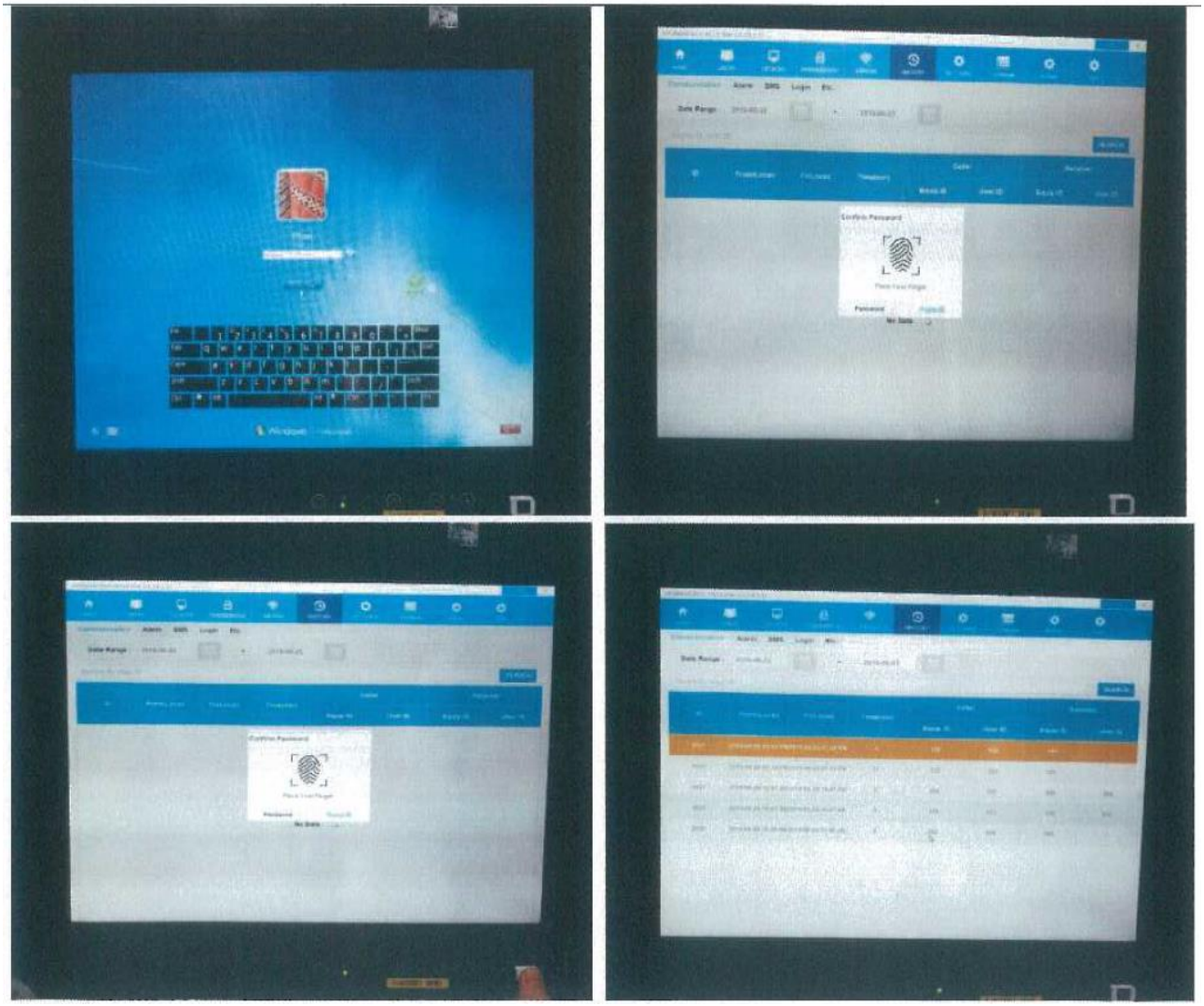
<Test Procedure and results for SL1 : *identify and authenticate all human users*>

procedure	Check point	Result
1) *Connect to administration display* 2) *Check device list and user list in the screen*	*Identify device and user*	*Pass*



<Test Procedure and results for SL2 : *Multifactor authentication for all interfaces*>

procedure	Check point	Result
1) *Boot the terminal and log in to Windows* 2) *Check the fingerprint recognition when connecting to the administrator*	*Multifactor authenticator*	*Pass*



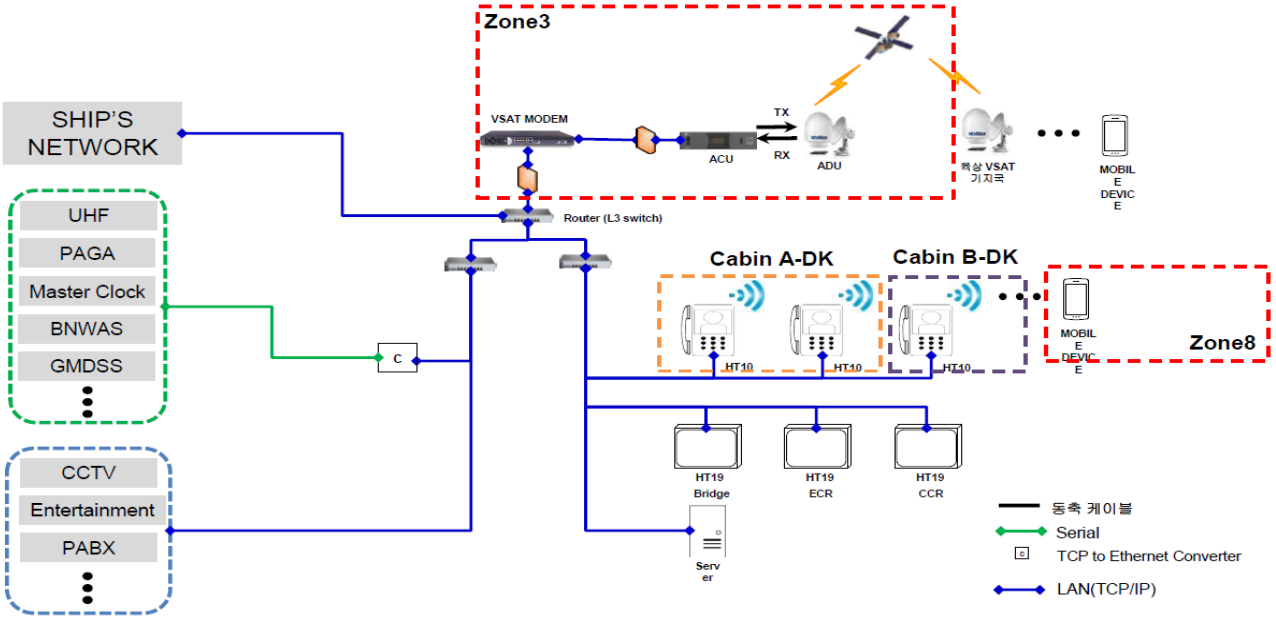
3.3.5 Example of Hyundai ISCS (Integrated Smart Communication System)

Hyundai ISCS is smart integrated communication system for ships and it interfaces and manages all different communication systems. ISCS 10" terminal manages integrated operations in a monitor with interfacing Telephone, PAGA, VHF, UHF, BNWAS, CCTV, etc. systems for ships. To assure cyber security for ISCS, Hyundai ISCS received cyber security type approval certificate from KR according to KR cyber security type approval procedures. Through cyber security risk assessment report cyber threat, vulunerbility countermeasures to the ISCS operation server, database, network device, wireless network device were verified.

1) Equipment List

Component type	SL	Components	Operating System	Remark
Node	*3*	*ISCS Main Server*	*Windows server series*	*Hyundai ISCS*
Node	*3*	*ISCS 10" Terminal*	*Android*	
Node	*3*	*ISCS 19" Terminal*	*Windows 7 Professional*	
Switch	*-*	*Netgear*		*Commercial Products for Network*
Forwarder	*-*	*CISCO Router*	*IOS*	

2) Network Topology



4 CONCLUSION

Cyber security will be essential for the operation of ship with highly integrated and connected systems installed such as MASS (Maritime Autonomous Surface Ship) and autonomous ship. In this context, KR developed a cyber security type approval program that can be applied to components and systems based on IEC 62443 4-2 and IEC 61162-460 standard. In conclusion, this document to be used as a direction of cyber security applied to AtoN related equipment.

5 REFERENCES

[1] IEC 62443 1-1 *Security for industrial automation and control system, Concepts and models*

[2] IEC 62443 3-3 *Security for industrial automation and control system, System security requirements and security levels*

[3] IEC 62443 4-2 *Security for industrial automation and control system, Technical security requirement for IACS components*

[4] IEC 61162 460 *Maritime navigation and radiocommunication equipment and systems – digital interfaces, Ethernet interconnection – safety and security*

[5] Korean Register *Guidance for type approval of maritime cyber security*

6 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 and 61162-460 standards to develop IALA cyber security recommendation / guideline for AtoN operations or other maritime ICT equipment

APPENDIX 1 Mapping of CRs and REs to FR SLs 1-4, Annex B in IEC 62443 4-2

This appendix is intended to provide overall guidance to the reader as to how SL levels 1 to 4 are differentiated on an FR-by-FR basis via the defined CRs and their associated REs.

SRs and Res	SL 1	SL 2	SL 3	SL 4
FR 1 – Identification and authentication control (IAC)				
CR 1.1 – Human user identification and authentication	✓	✓	✓	✓
RE (1) Unique identification and authentication:		✓	✓	✓
RE (2) Multifactor authentication for all interfaces			✓	✓
CR 1.2 – Software process and device identification and authentication		✓	✓	✓
RE (1) Unique identification and authentication			✓	✓
CR 1.3 – Account management	✓	✓	✓	✓
CR 1.4 – Identifier management	✓	✓	✓	✓
CR 1.5 – Authenticator management	✓	✓	✓	✓
RE (1) Hardware security for authenticators			✓	✓
NDR 1.6 – Wireless access management	✓	✓	✓	✓
RE (1) Unique identification and authentication		✓	✓	✓
CR 1.7 – Strength of password-based authentication	✓	✓	✓	✓
RE (1) Password generation and lifetime restrictions for human users			✓	✓
RE (2) Password lifetime restrictions for all users (human, software process, or device)				✓
CR 1.8 – Public key infrastructure certificates		✓	✓	✓
CR 1.9 – Strength of public key-based authentication		✓	✓	✓
RE (1) Hardware security for public key -based authentication			✓	✓
CR 1.10 – Authenticator feedback	✓	✓	✓	✓
CR 1.11 – Unsuccessful login attempts	✓	✓	✓	✓
CR 1.12 – System use notification	✓	✓	✓	✓
NDR 1.13 – Access via untrusted networks	✓	✓	✓	✓
RE (1) Explicit access request approval			✓	✓
CR 1.14 – Strength of symmetric key-based authentication		✓	✓	✓
RE (1) Hardware security for symmetric key-based authentication			✓	✓

SRs and Res	SL 1	SL 2	SL 3	SL 4
FR 2 – Use control (UC)				
CR 2.1 – Authorization enforcement	✓	✓	✓	✓
RE (1) Authorization enforcement for all users (humans, software processes and devices)		✓	✓	✓
RE (2) Permission mapping to roles		✓	✓	✓
RE (3) Supervisor override			✓	✓
RE (4) Dual approval				✓
CR 2.2 – Wireless use control	✓	✓	✓	✓
CR 2.3 – Use control for portable and mobile devices				
SAR 2.4 – Mobile code	✓	✓	✓	✓
RE (1) Mobile code authenticity check		✓	✓	✓
EDR 2.4 – Mobile code	✓	✓	✓	✓
RE (1) Mobile code authenticity check		✓	✓	✓
HDR 2.4 – Mobile code	✓	✓	✓	✓
RE (1) Mobile code authenticity check		✓	✓	✓
NDR 2.4 – Mobile code	✓	✓	✓	✓
RE (1) Mobile code authenticity check		✓	✓	✓
CR 2.5 – Session lock	✓	✓	✓	✓
CR 2.6 – Remote session termination		✓	✓	✓
CR 2.7 – Concurrent session control			✓	✓
CR 2.8 – Auditable events	✓	✓	✓	✓
CR 2.9 – Audit storage capacity	✓	✓	✓	✓
RE (1) Warn when audit record storage capacity threshold reached			✓	✓
CR 2.10 – Response to audit processing failures	✓	✓	✓	✓
CR 2.11 – Timestamps	✓	✓	✓	✓
RE (1) Time synchronization		✓	✓	✓
RE (2) Protection of time source integrity				✓
CR 2.12 – Non-repudiation	✓	✓	✓	✓
RE (1) Non-repudiation for all users				✓

EDR 2.13 – Use of physical diagnostic and test interfaces		✓	✓	✓
RE (1) Active monitoring			✓	✓
HDR 2.13 – Use of physical diagnostic and test interfaces		✓	✓	✓
RE (1) Active monitoring			✓	✓
NDR 2.13 – Use of physical diagnostic and test interfaces		✓	✓	✓
RE (1) Active monitoring			✓	✓

SRs and Res	SL 1	SL 2	SL 3	SL 4
FR 3 – System integrity (SI)				
CR 3.1 – Communication integrity	✓	✓	✓	✓
RE (1) Communication authentication		✓	✓	✓
SAR 3.2 – Protection from malicious code	✓	✓	✓	✓
EDR 3.2 – Protection from malicious code	✓	✓	✓	✓
HDR 3.2 – Protection from malicious code	✓	✓	✓	✓
RE (1) Report version of code protection		✓	✓	✓
NDR 3.2 – Protection from malicious code	✓	✓	✓	✓
CR 3.3 – Security functionality verification	✓	✓	✓	✓
RE (1) Security functionality verification during normal operation				✓
CR 3.4 – Software and information integrity	✓	✓	✓	✓
RE (1) Authenticity of software and information		✓	✓	✓
RE (2) Automated notification of integrity violations			✓	✓
CR 3.5 – Input validation	✓	✓	✓	✓
CR 3.6 – Deterministic output	✓	✓	✓	✓
CR 3.7 – Error handling	✓	✓	✓	✓
CR 3.8 – Session integrity		✓	✓	✓
CR 3.9 – Protection of audit information		✓	✓	✓
RE (1) Audit records on write-once media				✓
EDR 3.10 – Support for updates	✓	✓	✓	✓
RE (1) Update authenticity and integrity		✓	✓	✓
HDR 3.10 – Support for updates	✓	✓	✓	✓

RE (1) Update authenticity and integrity		✓	✓	✓
NDR 3.10 – Support for updates	✓	✓	✓	✓
RE (1) Update authenticity and integrity		✓	✓	✓
EDR 3.11 – Physical tamper resistance and detection		✓	✓	✓
RE (1) Notification of a tampering attempt			✓	✓
HDR 3.11 – Physical tamper resistance and detection		✓	✓	✓
RE (1) Notification of a tampering attempt			✓	✓
NDR 3.11 – Physical tamper resistance and detection		✓	✓	✓
RE (1) Notification of a tampering attempt			✓	✓
EDR 3.12 – Provisioning product supplier roots of trust		✓	✓	✓
HDR 3.12 – Provisioning product supplier roots of trust		✓	✓	✓
NDR 3.12 – Provisioning product supplier roots of trust		✓	✓	✓
EDR 3.13 – Provisioning asset owner roots of trust		✓	✓	✓
HDR 3.13 – Provisioning asset owner roots of trust		✓	✓	✓
NDR 3.13 – Provisioning asset owner roots of trust		✓	✓	✓
EDR 3.14 – Integrity of the boot process	✓	✓	✓	✓
RE (1) Authenticity of the boot process		✓	✓	✓
HDR 3.14 – Integrity of the boot process	✓	✓	✓	✓
RE (1) Authenticity of the boot process		✓	✓	✓
NDR 3.14 – Integrity of the boot process	✓	✓	✓	✓
RE (1) Authenticity of the boot process		✓	✓	✓

SRs and Res	SL 1	SL 2	SL 3	SL 4
FR 4 – Data confidentiality (DC)				
CR 4.1 – Information confidentiality	✓	✓	✓	✓
CR 4.2 – Information persistence		✓	✓	✓
RE (1) Erase of shared memory resources			✓	✓
RE (2) Erase verification			✓	✓
CR 4.3 – Use of cryptography	✓	✓	✓	✓

SRs and Res	SL 1	SL 2	SL 3	SL 4
FR 5 – Restricted data flow (RDF)				
CR 5.1 – Network segmentation	✓	✓	✓	✓
NDR 5.2 – Zone boundary protection	✓	✓	✓	✓
RE (1) Deny all, permit by exception		✓	✓	✓
RE (2) Island mode			✓	✓
RE (3) Fail close			✓	✓
NDR 5.3 – General purpose, person-to-person communication restrictions	✓	✓	✓	✓

SRs and Res	SL 1	SL 2	SL 3	SL 4
FR 6 – Timely response to events (TRE)				
CR 6.1 – Audit log accessibility	✓	✓	✓	✓
RE (1) Programmatic access to audit logs			✓	✓
CR 6.2 – Continuous monitoring		✓	✓	✓

SRs and Res	SL 1	SL 2	SL 3	SL 4
FR 7 – Resource availability (RA)				
CR 7.1 – Denial of service protection	✓	✓	✓	✓
RE (1) Manage communication load from component		✓	✓	✓
CR 7.2 – Resource management	✓	✓	✓	✓
CR 7.3 – Control system backup	✓	✓	✓	✓
RE (1) Backup integrity verification		✓	✓	✓
CR 7.4 – Control system recovery and reconstitution	✓	✓	✓	✓
CR 7.5 - Emergency Power				
CR 7.6 – Network and security configuration settings	✓	✓	✓	✓
RE (1) Machine-readable reporting of current security settings			✓	✓
CR 7.7 – Least functionality	✓	✓	✓	✓
CR 7.8 – Control system component inventory		✓	✓	✓