Input paper: [1] ENAV28-5.1.1.4

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]	
Technical Domain / Task Number [2]	Working Group 1 (Digital Information System)
Author(s) / Submitter(s)	Juntae Kim (Korean Register) Sanghoon Choi (Korean Register) Jinho Yoo (Korean Register) Kaemyoung Park (Korean Register)

The analysis of general cybersecurity requirements applicable to ship's e-Nav service display device based on international standards

1 SUMMARY

This document includes information regarding the high-level review which was conducted to derive general cybersecurity requirements applicable to the ship's e-Navigation service display device based on international standard.

To proceed with the review, all international standards for cybersecurity were analysed in order to identify most applicable standards to ship's e-Nav service display device and cyber risk assessment was conducted for the device. According to this, most appropriate cybersecurity requirements were identified for this device based on international standard such as IEC 62443-4-2 as the result of cybersecurity risk assessements.

1.1 Purpose of the document

This document is to provide information on the analysis of cybersecurity requirements based on the international standards to ensure cyber security for ship's e-Navigation service display devices that provide maritime digital services.

1.2 Related documents

None.

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

1.3 Terms and definitions

1.3.1 **authentication**

provision of assurance that a claimed characteristic of an identity is correct

1.3.2 **authenticator**

means used to confirm the identity of a user (human, software process or device) property of ensuring timely and reliable access to and use of control system information and functionality

1.3.3 e-Navigation service display device

shipboard device to display information of maritime services(refer to MSC.1/Circ.1610) in the context of e-Navigation, which may be ECDIS, INS or a dedicated display unit.

1.3.4 **identifier**

symbol, unique within its security domain, that identifies, indicates or names an entity which makes an assertion or claim of identity

1.3.5 **integrity**

property of protecting the accuracy and completeness of assets

1.3.6 **least privilege**

basic principle that holds that users (humans, software processes or devices) should be assigned the fewest privileges consistent with their assigned duties and functions

1.3.7 **non-repudiation**

ability to prove the occurrence of a claimed event or action and its originating entities

1.3.8 **security level**

level corresponding to the required set of countermeasures and inherent security properties of devices and systems for a zone or conduit based on assessment of risk for the zone or conduit (IEC 62443-4-2 / 3.1.37)

1.3.9 **threat**

circumstance or event with the potential to adversely affect operations (including mission, functions, image or reputation), assets, control systems or individuals via unauthorized access, destruction, disclosure, modification of data and/or denial of service

2 BACKGROUND

The International Maritime Organization (IMO) hase approved the e-Navigation implementation strategy to enhance maritime safety by applying ICT technology to ships, and recently officially approved the new work programme for introducing VDES as international communication means to support e-Navigation service at MSC 104.

As the introduction of e-Navigation service is expected to expand in the future, the cyber attack threats are expected to increase. In addition, the number of cases of introducing digital solutions in ships using ICT technology in the maritime field is increasing recently. Thus, the numbers of cyber attack attempts and damage cases in the maritime domain is continuously on the rise.

The IMO has approved “Cyber Risk Management in Safety Management Systems (MSC.428(98))” in 2017, and recommends the establishment and implementation of a cyber risk management system for international voyage vessels since 2021. To support ship's implementation, IMO issued the guidelines on maritime cyber risk management as per MSC-FAL.1/Circ.3.

In this background, the analysis was conducted to figure out cyber security requirements applicable to e-Navigation service display device based on international standards, and for the sake of this, analysis for applicable international standards and the the qualitative cyber risk assessment was performed.

3 DISCUSSION

3.1 Analysis of applicable international standards

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.

Table 1 cyber security standards applicable to maritime digital devices

Category	Standard	Title
Maritime digital devices	IEC 62443-4-2	Technical security requirements for IACS components
	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

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.

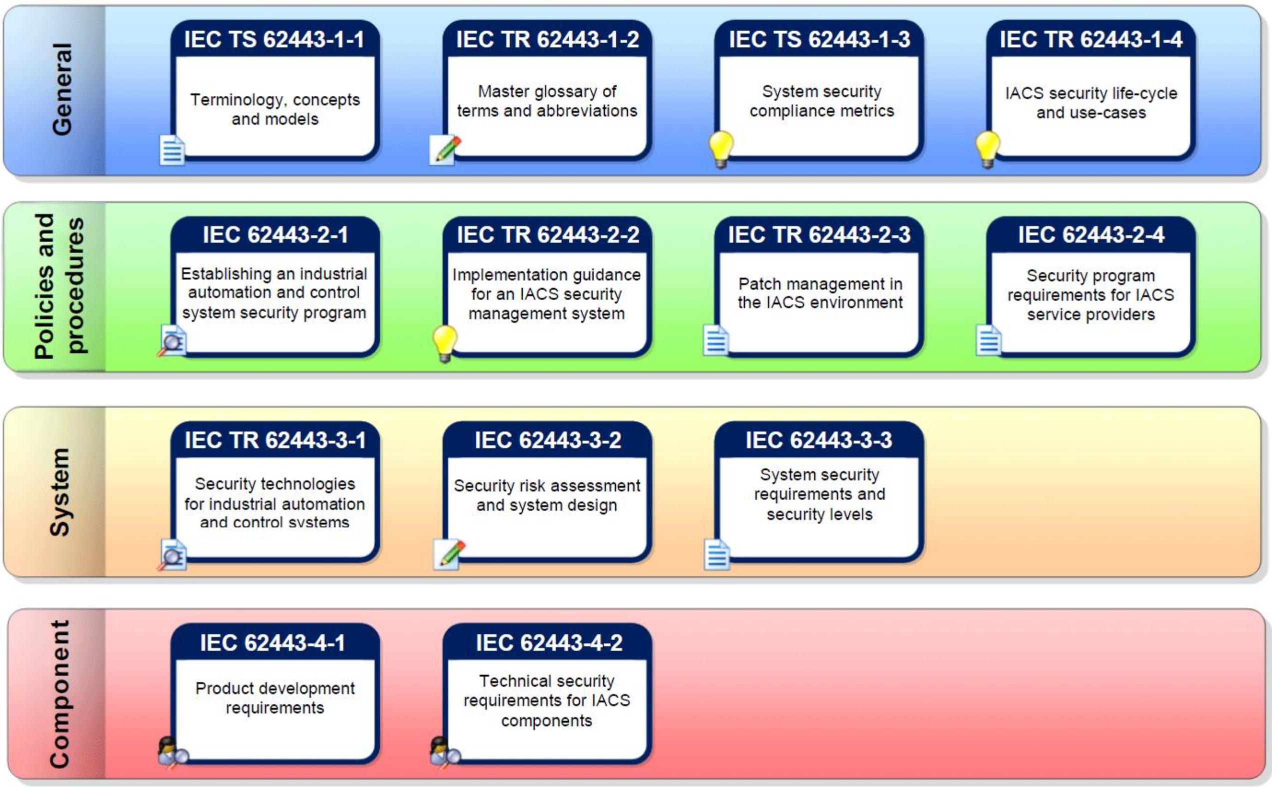

General
IEC TS 62443-1-1
Terminology, concepts and models
IEC TR 62443-1-2
Master glossary of terms and abbreviations
IEC TS 62443-1-3
System security compliance metrics
IEC TR 62443-1-4
IACS security life-cycle and use-cases
Policies and procedures
IEC 62443-2-1
Establishing an industrial automation and control system security program
IEC TR 62443-2-2
Implementation guidance for an IACS security management system
IEC TR 62443-2-3
Patch management in the IACS environment
IEC 62443-2-4
Security program requirements for IACS service providers
System
IEC TR 62443-3-1
Security technologies for industrial automation and control systems
IEC 62443-3-2
Security risk assessment and system design
IEC 62443-3-3
System security requirements and security levels
Component
IEC 62443-4-1
Product development requirements
IEC 62443-4-2
Technical security requirements for IACS components

Figure 1 IEC 62443 series overview

3.1.1.1 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. 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 3 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.

3.1.1.2 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 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)

3.1.2 Overview of IEC 61162 standards

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

Table 4 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

3.1.2.1 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.

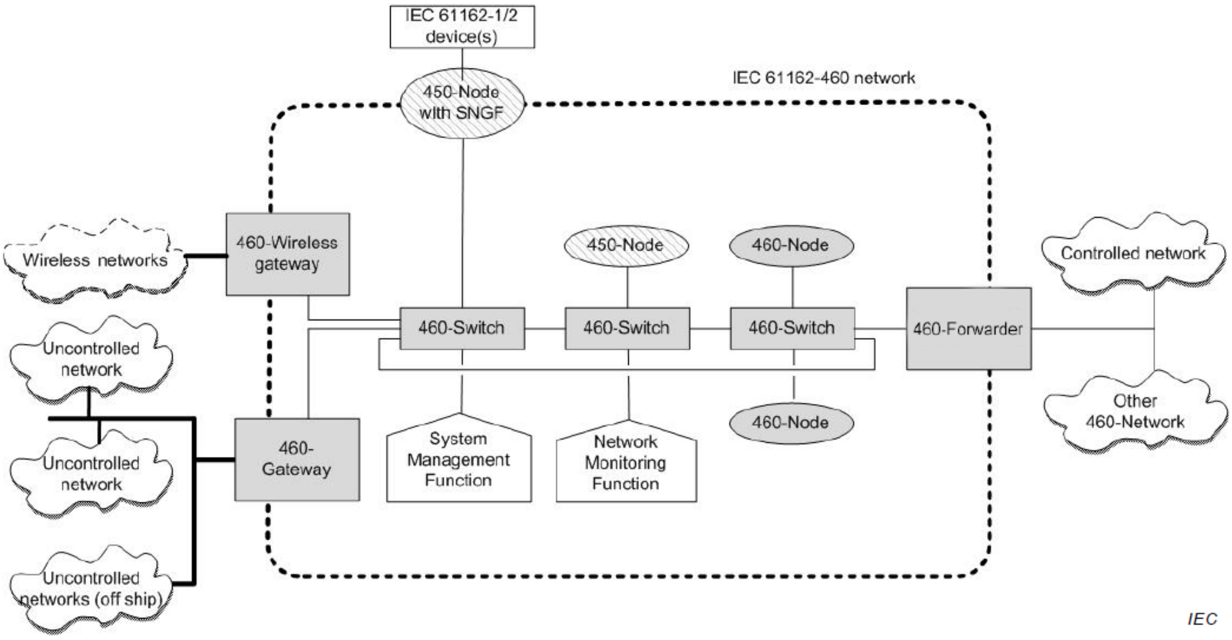


Figure 2 Functional overview of IEC 61162-460 requirement applications

Table 5 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

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

3.1.3.1 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:

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

Table 6 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
Annex B	File authentication
Annex C	Methods of authentication of data files and executables – some examples
Annex D	USB class codes
Annex E	Cyber security configuration document for equipment
Annex F	Guidance on interconnection between networks

3.1.3.2 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 3. The methods for achieving authentication and verification are described in each Module of this standard.

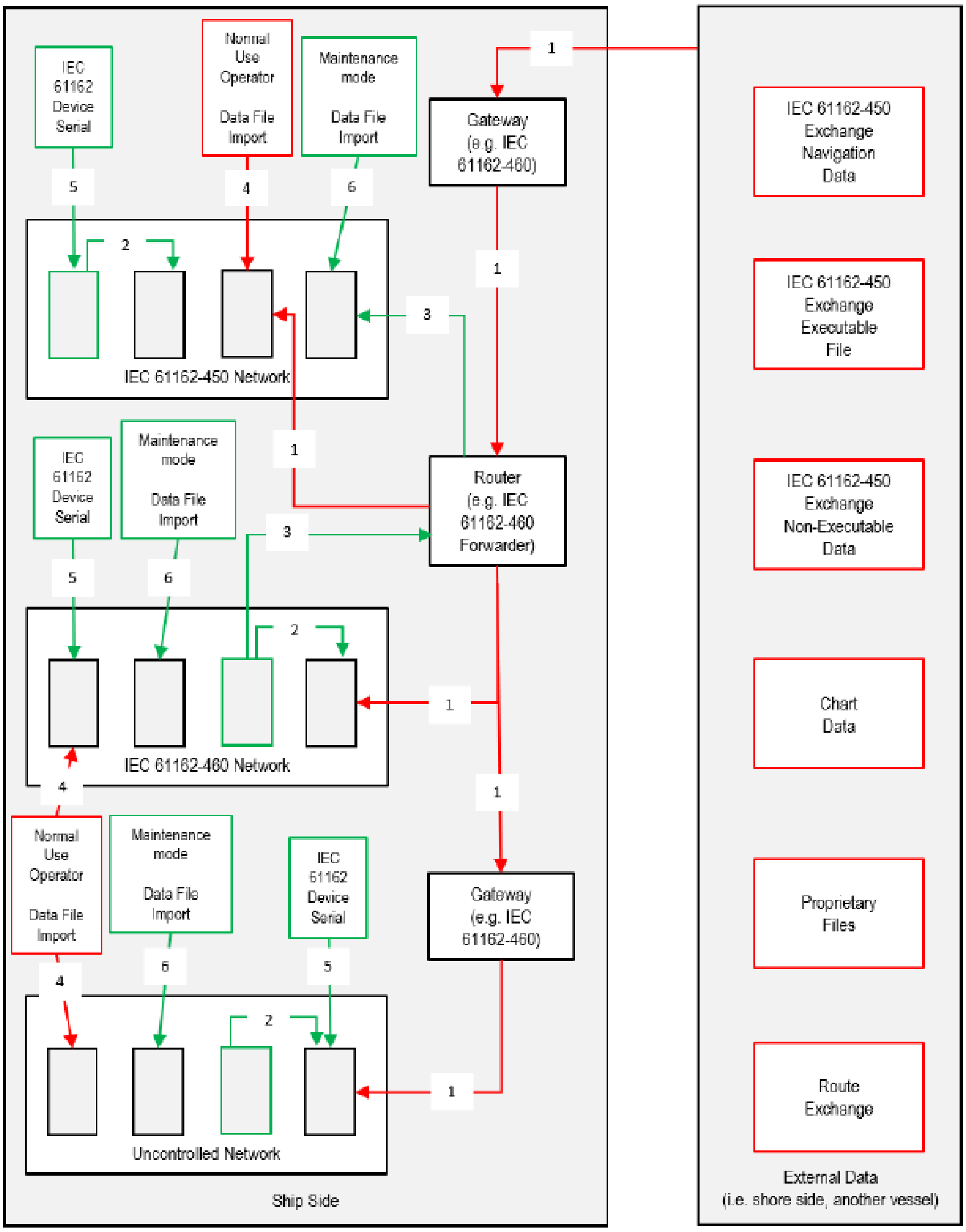

IEC 61162 Device Serial
Normal Use Operator Data File Import
Maintenance mode Data File Import
1
Gateway (e.g. IEC 61162-460)
5
4
6
2
3
IEC 61162-450 Network
1
IEC 61162 Device Serial
Maintenance mode Data File Import
1
Router (e.g. IEC 61162-460 Forwarder)
3
5
6
2
1
IEC 61162-460 Network
4
1
Normal Use Operator Data File Import
Maintenance mode Data File Import
IEC 61162 Device Serial
Gateway (e.g. IEC 61162-460)
4
6
5
2
1
Uncontrolled Network
Ship Side
IEC 61162-450 Exchange Navigation Data
IEC 61162-450 Exchange Executable File
IEC 61162-450 Exchange Non-Executable Data
Chart Data
Proprietary Files
Route Exchange
External Data (i.e. shore side, another vessel)

Figure 3 Some Examples of Data transfer

3.2 Cyber risk assessment methodolgy

Since there are so many cyber security requirements applicable to the e-Navigation service display device and it is impractical that all requirement are ideally applied to a device, qualitative cyber risk assessment is very valuable to understand of vulnerabilities and risk of specific device taking into account cyber attack scenario, and it is enable to figure out most suitable requirements to mitigate overall cyber risk based on the result of cyber risk assessment.

Structured and systematic risk assessment methodologies were used to identify the cyber risk for a device taking into acout the methods mentioned in "The Guidelines on Cyber Security Onboard Ships Version 4" and "ISO 27005: 2018 - Information security risk management".

The general process of cyber security risk assessment is shown in Figure 4 as below. Through systematic cyber security risk assessment, it should be made to check the cyber security risk level for a device, and to analyze the cyber security means to to mitigate high level of risk into acceptable level based on cyber security requirements.

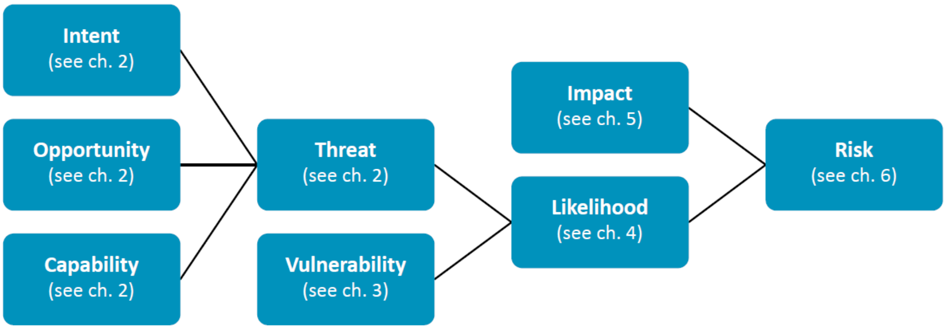


Figure 4 Overall Schematic Diagram of Cyber Security Risk Assessment Procedure

3.2.1 Threat Index(TI) and vulnerability Index(VI)

Threat list is provided in Table 7. The value of threats to assets is calculated considering both the probability that an attack occurs to assets, and is expressed as a Threat Index (TI) shown in the table below.

Table 7 Definition of Threat Index (TI)

TI	Category	description
5	Definite	Happens frequently when undertaking the work in question.
4	Probable	Happens occasionally in own company, typically in the context of faulty equipment or by mistakes by people involved (the kind of mistakes that tend to happen on board from time to time).
3	Occasional	Incident has probably occurred in own company, but in the context of faulty equipment or by surprising mistakes made by people involved.
2	Remote	Heard of in industry, but only extremely rarely and as the result of a chain of many unfortunate events.
1	Improbable	Never heard of in industry. Close to being something unimaginable.

In general, vulnerability is the probability that the attack succeeds given that the cyber-attack occurs. In this study, the value of vulnerability is calculated considering the level of cyber security controls that are already implemented to protect those assets against cyber-attacks. The value of vulnerability is expressed as a Vulnerability Index (VI) shown in the table below.

Table 8 Definition of Vulnerability Index (VI)

VI	Category	Description
5	Very high	There are very ineffective security measures currently in place, and so the adversary would easily be able to succeed
4	High	There are some security measures but there is not a complete and effective application, it would make an attack succeed relatively easily
3	Medium	Although there are some effective security measures in place, the existing countermeasures could still be compromised
2	Low	There are effective security measures in place, however at least one weakness exists
1	Very low	Multiple layers of effective security measures exist

Then, the probability of occurrence of the identified cyber-attack scenarios (i.e., combination of 'Threat Index' and 'Vulnerability Index') is expressed as a numerical index, 'Probability Index'. The Probability Index is determined based on the value of cyber-attack scenario occurrence, as shown in the table below.

3.2.2 Likelyhood Index (LI)

- Likelyhood Index = Threat Index X Vulnerability Index

Table 9 Likelyhood Index (LI)

Likelyhood Index	Calculation
5	21 ≤ TI X VI ≤ 25
4	16 ≤ TI X VI ≤ 20
3	11 ≤ TI X VI ≤ 15
2	6 ≤ TI X VI ≤ 10
1	1 ≤ TI X VI ≤ 5

3.2.3 Quantifying the Impact

The confidentiality, integrity, and availability (CIA) mode provides a framework for assessing the impact of:

- loss of confidentiality of information, eg unauthorised access to and disclosure of information or data about the ship, crew, cargo and passengers
- loss of integrity, which would modify information and data relating to the safe and efficient operation and management of the ship
- loss of availability due to the destruction of the information and data and/or the disruption to services/ operation of ship systems.

Table 10 Table Definition of Impact Index (ImI)

ImI	Category	Description
5	Critical	Fatality or permanent disabilities. Widespread, significant damage to environment, assets, finances, or company's reputation.

4	Significant	Major health effect/relatively serious injuries. Local but major damage to environment, assets, finances, or to company's reputation.
3	Moderate	Some health effect/minor injuries. Minor damage to environment, assets, finances, or to company's reputation.
2	Minor	Very slight health effect/injuries. Very slight damage to environment, assets, finances, or to company's reputation.
1	Negligible	No health effect/injuries. No damage to environment, assets, finances, or company's reputation.

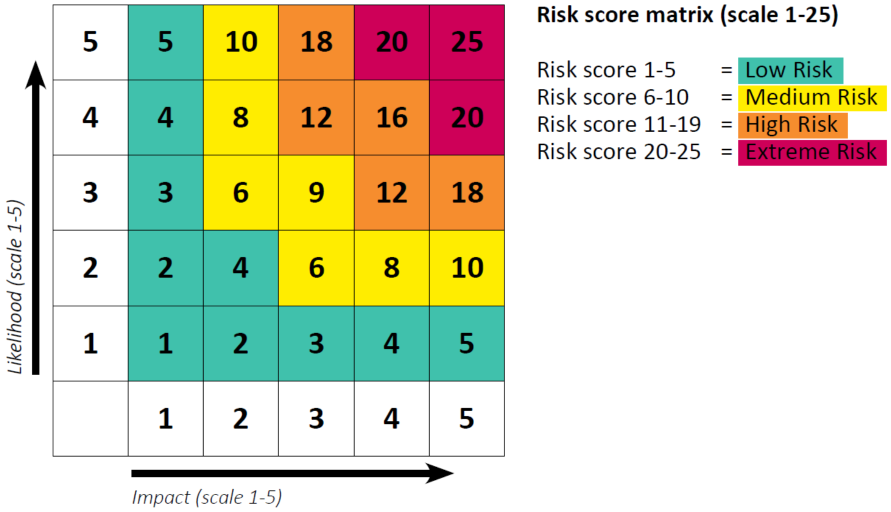
3.2.4 Risk Analysis and Control Identification

Cyber security risk is defined as the combination of Threat (probability that an attack occurs), Vulnerability (probability that the attack succeeds given that it occurs) and Consequence (expected extent of the impacts given that the attack occurs and succeeds). Once the cyber-attack scenarios related to those threats identified for each critical system are identified, the cyber security risk can be calculated by using the following formula:

$$\begin{gathered}\textit{Cyber security Risk Index (RI)}\\ = \textit{TI x VI x ImI}\\ = \textit{Likelyhood Index (TI x VI) x Impact Index (ImI)}\end{gathered}$$

When the cyber threat scenarios and the current mitigation actions for the relevant scenarios are identified, the need for additional mitigation actions should be reviewed to propose additional risk controls. Risk mitigation measures can be divided into measures to reduce the frequency of occurrence of cyber threats and measures to minimize the impact of cyber threats.

When proposing new risk mitigation measures, the costs to mitigate cyber risk and the effects of applying them should be considered. In relation to all proposed risk mitigation measures, the effect and possible side effects to be gained in application should be evaluated and the measures of remaining risks should be reviewed after application.



5	5	10	18	20	25
4	4	8	12	16	20
3	3	6	9	12	18
2	2	4	6	8	10
1	1	2	3	4	5
	1	2	3	4	5

Likelihood (scale 1-5)
Impact (scale 1-5)

Risk score matrix (scale 1-25)

Risk score 1-5	=	Low Risk
Risk score 6-10	=	Medium Risk
Risk score 11-19	=	High Risk
Risk score 20-25	=	Extreme Risk

Figure 5 Risk score matrix

3.3 Cyber Risk Assessment

3.3.1 Scope of the assessment

The scope of the assessment work confines e-Navigation service display devices, which may be ECDIS, INS or dedicated device for this purpose.

We assumed that e-Navigation service display device subject to the cyber risk assessment has the below general specification and functions referring to the information obtained by searching for products regarding ECDIS and INS on sale in the market.

[General specifications]

- Power Supply : 230 VAC, 50/60Hz
- Display Unit : 26 in LCD display
- Main Control Unit
    - OS : Windows 10
    - Interfaces
        - ✓ Multiple Ethernet LAN ports (1GB)
        - ✓ Multiple serial ports (IEC 61162-1 & IEC 61162-2)
        - ✓ Multiple USB ports
        - ✓ CD/DVD-ROM : optional
- Keyboard, trackball mouse

[General functions]

- Display of e-Navigation service information.
- Elctronic chart display
- Display of AIS vessels

3.3.2 Identification of cyber threats

The below examples are not exhaustive. Threats may be intentional, accidental or environmental (natural) and may result, for example, in damage or loss of essential services. Other cyber attack methods are evolving such as impersonating a legitimate shore-based employee in a shipping company to obtain valuable information, which can be used for a further attack. The potential number and sophistication of tools and techniques used in cyber attacks continue to evolve and are limited only by the ingenuity of those organisations and individuals developing them.

Table 11 Identified threats list

No.	Threat	Description
1	Malware	Malware is any software intentionally designed to cause damage to a computer, server, client, or computer network. By contrast, software that causes unintentional harm due to some deficiency is typically described as a software bug. A wide variety of malware types exist, including computer viruses, worms, Trojanhorses, ransomware, spyware, adware, rogue software, wiper and scareware.

No.	Threat	Description
2	Brute force.	An attack trying many passwords with the hope of eventually guessing correctly. The attacker systematically checks all possible passwords until the correct one is found.
3	Denial of Service (DOS)	a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.
4	Social engineering.	A non-technical technique used by potential cyber attackers to manipulate insider individuals into breaking security procedures, normally, but not exclusively, through interaction via social media.
5	Data breach	A data breach is a security violation in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so.
6	Phishing.	Sending emails to a large number of potential targets asking for particular pieces of sensitive or confidential information. The email may also contain a malicious attachment or request that a person visits a fake website using a hyperlink included in the email.
7	Scanning	Searching large portions of the internet at random for vulnerabilities that could be exploited.
8	Network manipulation and information gathering	Illegal collection of information through unauthorized access to the network
9	Man-in-the-middle attack	a cyberattack where the attacker secretly relays and possibly alters the communications between two parties who believe that they are directly communicating with each other. One example of a MITM attack is active eavesdropping, in which the attacker makes independent connections with the victims and relays messages between them to make them believe they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker. The attacker must be able to intercept all relevant messages passing between the two victims and inject new ones.
11	Erroneous use or erroneous administration of devices	During system maintenance(e.g., software update), the introduction of malicious code, system malfunction, setting mistake, integrity test not conducted, etc.
12	Careless use of removable media or device (USB, Laptop, etc)	Careless use of removable media (USB, portable drives, laptops, etc)
13	OS vulnerabilities	Security vulnerabilities that can be caused by failure to patch operating system(Windows, Linux, Android, etc).
14	Application software vulnerabilities	Security vulnerabilities that can be caused by software bugs or failure to patch software

No.	Threat	Description
15	Hardware failure	Hardware failure caused by failure of hardware devices such as CPU, memory, and interfaces
16	Credential stuffing.	Using previously compromised credentials or specific commonly used passwords to attempt unauthorized access to a system or application.
17	Subverting the supply chain	Attacking a company or ship by compromising equipment, software or supporting services being delivered to the company or ship.

3.3.3 Impact index for e-Navigation service display device

The Impact Index of the e-Navigation service display device was considered to be “4: Significant” considering the purpose of use and operating conditions of the device.

3.4 Result of cyber risk assessment for e-Navigation Service Display Device

No	Threats	Potential cause	Potential consequence	VI	TI	ImI	RI	Proposed controls	62443-4-2 reqirements.
1	Malware	1) Installation of unauthorized software 2) Use of email or internet 3) Use of USB	1) Malware infection 2) System malfunction 3) Service interruption 4) Data loss	5	4	4	20	1) Protection from malicious code	IEC 62443-4-2 SAR 3.2
2	Brute force	1) Hacking attampt by attacker	1) Unauthorized access 2) Illegal system manipulation or parameter setting change 3) Confidential data leakage 4) Important data deletion	3	2	4	8	1) Strength of password-based authentication	IEC 62443-4-2 CR 1.7
3	Denial of Service (DOS)	1) DDOS attack by attacker via network	1) Network disruption 2) Service interruption	3	2	4	8	1) Denial of service(DoS) protection 2) Resource management	IEC 62443-4-2 CR 7.1 IEC 62443-4-2 CR 7.2
4	Social engineering	1) Malicious act by attacker via email or internet	1) Malware infection 2) System malfunction 3) Service interruption 4) Data breach	4	2	4	8	1) System backup 2) System recovery and reconstitution	IEC 62443-4-2 CR 7.3 IEC 62443-4-2 CR 7.4
5	Data breach	1) Unauthorized access to data 2) Ransomware infection 3) Sniffing using sniffer 4) Data leakage by spyware infection	1) Confidential data leakage 2) Important data change or deletion	4	3	4	12	1) Information confidentiality 2) Use of cryptography	IEC 62443-4-2 CR 4.1 IEC 62443-4-2 CR 4.3
6	Phishing	1) Malicious act by attacker via email or messenger	1) Confidential information leackage 2) Malware infection	4	2	4	8	1) Protection from malicious code	IEC 62443-4-2 SAR 3.2
7	Spoofing attack	1) IP spoofing 2) ARP spoofing 3) email spoofing	1) System malfunction	3	2	4	8	1) Communication integrity	IEC 62443-4-2 CR 3.1

8	Network manipulation and information gathering	1) Unauthorized access to network access 2) Network sniffing using sniffer	1) Data leakage 2) Network information leakage	3	2	4	8	1) Information confidentiality 2) Use of cryptography	IEC 62443-4-2 CR 4.1 IEC 62443-4-2 CR 4.3
9	Man-in-the-middle attack	1) False service data injection by attacker 2) Eavesdropping by attacker	1) Confidential data leakage 2) Wrong service information	3	2	4	8	1) Public key infrastructure certificates 2) Strength of public key-based authentication 3) Communication integrity	IEC 62443-4-2 CR 1.8 IEC 62443-4-2 CR 1.9 IEC 62443-4-2 CR 3.1
10	Information leakage	1) Unauthorized access to data 2) Eavesdropping by Sniffing or MITM attack 3) Information leakage by spyware infection	1) Confidential information leakage	4	3	4	12	1) Public key infrastructure certificates 2) Strength of public key-based authentication 3) Information confidentiality 4) Use of cryptography	IEC 62443-4-2 CR 1.8 IEC 62443-4-2 CR 1.9 IEC 62443-4-2 CR 4.1 IEC 62443-4-2 CR 4.3
11	Erroneous use or erroneous administration of devices	1) Erroneous parametor settings by administrator 2) Operational mistake in during use by user	1) System malfunction 2) Service interruption	3	5	4	12	1) Auditable events 2) Non-repudiation 3) System backup 4) System recovery and reconstitution	IEC 62443-4-2 CR 2.8 IEC 62443-4-2 CR 2.12 IEC 62443-4-2 CR 7.3 IEC 62443-4-2 CR 7.4
12	Credential stuffing.	1) Unmanaged password 2) Easy password setting(eg. 0000, 1234, password, etc) 3) Unauthorized access atempt	1) Confidential information leakage 2) Data change or deletion 3) System mulfunction 4) Wrong parameter setting	3	3	4	8	1) Human user identification and authentication 2) Strength of password-based authentication	IEC 62443-4-2 CR 1.1 IEC 62443-4-2 CR 1.7

13	Careless use of removable media or device (USB, Laptop, etc)	1) Accidental Malware infection due to use of infected USB device during maintenance 2) Data breach attampt by using external ports.	1) Malware infection 2) System malfunction 3) Service interruption 4) Data breach	5	4	4	20	1) Least functionality 2) Protection from malicious code 3) REDS security	IEC 62443-4-2 CR 7.7 IEC 62443-4-2 SAR 3.2 IEC 61162-460 6.2.3.1
14	OS defects	1) Possible zero-day attacks due to delayed security patch updates	1) System malfunction 2) Service interuption 3) Malware infection	5	3	4	12	1) System backup 2) System recovery and reconstitution 3) Support for updates	IEC 62443-4-2 CR 7.3 IEC 62443-4-2 CR 7.4 IEC 62443-4-2 EDR 3.10
15	Application software defects	1) Possible zero-day attacks due to delayed patch updates	1) System malfunction 2) Service interuption 3) Malware infection	5	3	4	12	1) System backup 2) System recovery and reconstitution 3) Support for updates	IEC 62443-4-2 CR 7.3 IEC 62443-4-2 CR 7.4 IEC 62443-4-2 EDR 3.10
16	Hardware failure	1) Equipment failure due to hardware obsolescence or external influence (EMI, etc.)	1) System failure 2) Service interuption	5	2	4	8	1) System backup 2) System recovery and reconstitution	IEC 62443-4-2 CR 7.3 IEC 62443-4-2 CR 7.4
17	Subverting the supply chain	1) Identification and authentication information leakage in manufacturer side by hacking or malicious employee 2) Leakage of encryption information in manufacture side 3) Malware infection during manufacture's production 4) compromise of update data integrety during transfer	1) System malfunction 2) Service interuption 3) Malware infection 4) Confidential data leakage	5	3	4	12	1) Supply Chain Risk Management	NIST Cybersecurity Framework ID.SC

4 SECURITY REQUIRMENTS FOR E-NAVIGATION DISPLAY UNIT BASED ON IEC 62443-4-2

According to the result of the cyber risk assessment described in Section 3, appropriate protection measures are identified to mitigate the cyber risk level identified for the e-Navigation service display device, and derived cyber security requirement based on the international standard IEC 62443-4-2, which are listed in paragraphs 4.1 to 4.7 as follows. For reference, listed security requirements can be applied differentially from SL1 to SL4 according to the required security level, the detailed information can be founded in paragraphs 3.1.1.1.

During the cyber risk assessment process, important risk items outside the scope of IEC 62443-4-2 were identified, in particular, risks posed by the use of removable storage media and supply chain risks that can be happened by the insufficient security management in manufacturing process. Therefore, additional cybersecurity requirements to cover these risk are additionally included in paragraph 4.8.

4.1 identification and authentication

4.1.1 IEC 62443-4-2 CR 1.1 - Human user identification and authentication

Components shall provide the capability to identify and authenticate all human users according to IEC 62443-3-3 SR 1.1 on all interfaces capable of human user access. This capability shall enforce such identification and authentication on all interfaces that provide human user access to the component to support segregation of duties and least privilege in accordance with applicable security policies and procedures. This capability may be provided locally by the component or by integration into a system level identification and authentication system. (SL1)

✓ Requirement enhancements

(1) Unique identification and authentication

Components shall provide the capability to uniquely identify and authenticate all human users. (SL2)

(2) Multifactor authentication for all interfaces

Components shall provide the capability to employ multifactor authentication for all human user access to the component. (SL3)

4.1.2 IEC 62443-4-2 CR 1.7 - Strength of password-based authentication

For components that utilize password-based authentication, those components shall provide or integrate into a system that provides the capability to enforce configurable password strength according to internationally recognized and proven password guidelines. (SL1)

✓ Requirement enhancements

(1) Password generation and lifetime restrictions for human users

Components shall provide, or integrate into a system that provides, the capability to protect against any given human user account from reusing a password for a configurable number of generations. In addition, the component shall provide the capability to enforce password minimum and maximum lifetime restrictions for human users. These capabilities shall conform to commonly accepted security industry practices. The component should provide the capability to prompt the user to change their password upon a configurable time prior to expiration. (SL3)

(2) Password lifetime restrictions for all users (human, software process, or device)

Components shall provide, or integrate into a system that provides, the capability to enforce password minimum and maximum lifetime restrictions for all users. (SL4)

4.1.3 IEC 62443-4-2 CR 1.8 - Public key infrastructure certificates

When public key infrastructure (PKI) is utilized, the component shall provide or integrate into a system that provides the capability to interact and operate in accordance with IEC 62443-3-3 SR 1.8. (SL2)

4.1.4 IEC 62443-4-2 CR 1.9 - Strength of public key-based authentication

For components that utilize public-key-based authentication, those components shall provide directly or integrate into a system that provides the capability within the same IACS environment to: (SL2)

a. validate certificates by checking the validity of the signature of a given certificate;

b. validate the certificate chain or, in the case of self-signed certificates, by deploying leaf certificates to all hosts that communicate with the subject to which the certificate is issued;

c. validate certificates by checking a given certificate's revocation status;

d. establish user (human, software process or device) control of the corresponding private key;

e. map the authenticated identity to a user (human, software process or device); and

f. ensure that the algorithms and keys used for the public key authentication

✓ Requirement enhancements

(1) Hardware security for public key-based authentication

Components shall provide the capability to protect critical, long-lived private keys via hardware mechanisms. (SL3)

4.2 Use control

4.2.1 IEC 62443-4-2 CR 2.8 - Auditable events

Components shall provide the capability to generate audit records relevant to security for the following categories: (SL1)

1) access control;

2) request errors;

3) control system events;

4) backup and restore event;

5) configuration changes; and

6) audit log events.

Individual audit records shall include:

1) timestamp;

2) source (originating device, software process or human user account);

3) category;

4) type;

5) event ID; and

6) event result.

4.2.2 IEC 62443-4-2 CR 2.12 - Non-repudiation

If a component provides a human user interface, the component shall provide the capability to determine whether a given human user took a particular action. Control elements that are not able to support such capability shall be listed in component documents. (SL1)

✓ Requirement enhancements

(1) Non-repudiation for all users

Components shall provide the capability to determine whether a given user (human, software process or device) took a particular action. (SL4)

4.3 System integrity

4.3.1 IEC 62443-4-2 CR 3.1 - Communication integrity

Components shall provide the capability to protect integrity of transmitted information. (SL1)

✓ Requirement enhancements

(1) Communication authentication

Components shall provide the capability to verify the authenticity of received information during communication. (SL2)

4.4 Data confidentiality

4.4.1 IEC 62443-4-2 CR 4.1 - Information confidentiality

Components shall

a) provide the capability to protect the confidentiality of information at rest for which explicit read authorization is supported; and

b) support the protection of the confidentiality of information in transit as defined in IEC 62443-3-3 SR 4.1. (SL1)

4.4.2 IEC 62443-4-2 CR 4.3 - Use of cryptography

If cryptography is required, the component shall use cryptographic security mechanisms according to internationally recognized and proven security practices and recommendations. (SL1)

4.5 Resource availability

4.5.1 IEC 62443-4-2 CR 7.1 - Denial of service protection

Components shall provide the capability to maintain essential functions when operating in a degraded mode as the result of a DoS event. (SL1)

✓ Requirement enhancements

(1) Manage communication load from component

Components shall provide the capability to mitigate the effects of information and/or message flooding types of DoS events. (SL2)

4.5.2 IEC 62443-4-2 CR 7.2 - Resource management

Components shall provide the capability to limit the use of resources by security functions to protect against resource exhaustion. (SL1)

4.5.3 IEC 62443-4-2 CR 7.3 - Control system backup

Components shall provide the capability to participate in system level backup operations in order to safeguard the component state (user- and system-level information). The backup process shall not affect the normal component operations. (SL1)

- ✓ Requirement enhancements

(1) Backup integrity verification

Components shall provide the capability to validate the integrity of backed up information prior to the initiation of a restore of that information.(SL2)

4.5.4 IEC 62443-4-2 CR 7.4 - Control system recovery and reconstitution

Components shall provide the capability to be recovered and reconstituted to a known secure state after a disruption or failure. (SL1)

4.5.5 IEC 62443-4-2 CR 7.7 - Least functionality

Components shall provide the capability to specifically restrict the use of unnecessary functions, ports, protocols and/or services. (SL1)

4.6 Software application requirements

4.6.1 IEC 62443-4-2 SAR 3.2 - Protection from malicious code

The application product supplier shall qualify and document which protection from malicious code mechanisms are compatible with the application and note any special configuration requirements. (SL1)

4.7 Embedded device requirements

4.7.1 IEC 62443-4-2 EDR 3.10 - Support for updates

The embedded device shall support the ability to be updated and upgraded. (SL1)

- ✓ Requirement enhancements

(1) Update authenticity and integrity

The embedded device shall validate the authenticity and integrity of any software update or upgrade prior to installation. (SL2)

4.8 Additional cybersecurity requirements other than IEC 62443-4-2

4.8.1 IEC 61162-460 6.2.3.1 - Physical protection

The number of connection points (USB ports, disc drives, etc.) shall be limited to the absolute minimum required for the operation of the system and its lifetime maintenance and support. All other points shall be physically blocked from easy access by a user without a tool or key.

4.8.2 NIST Cybersecurity Framework - Supply chain risk management (ID.SC)

1) ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders
2) ID.SC-2: Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process
3) ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.
4) ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.
5) ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers

5 CONCLUSION

In order to find general cybersecurity requirements suitable for ship's e-Navigation service display device, the international standards for cybersecurity applicable to equipment were analyzed, and in particular, IEC 62443-4-2 applicable to individual equipment is considered to be appropriate.

IEC 62443-4-2 includes universal security capability requirements applicable for all types of equipment, but this standard included too many requirements. Therefore, we conducted cyber risk assessment to figure out and to compress essential requirements optimized for e-Navigation service display device among many requirements. During the cyber risk assessment, risk posed by the use of removable storage media and supply chain risk that can be happened by supplier in manufacturing process, accordingly, additional cybersecurity requirements to treat these risk also are necessary to be considered.

As a result of this study, the key cybersecurity requirements identified for e-Navigation service display device can be summarized as follows.

1) User identification (ID) and authentication (certificate and password)

- Unique identifier(ID) and authentication
- Multi-factor authentication
- The use of an appropriate PKI considering commonly accepted best practice where PKI is utilized
- Authenticator management (password strength and life limit, etc.)

2) Auditable log record

3) Ensure service data integrity and confidentiality

- Provide communication integrity mechanism
- Service data encryption

4) System recovery function

- Important data backup
- System initialization function

5) Minimize function setting

- Restriction on unnecessary communication port and service use

6) Malware protection

- Install antivirus program

- Restriction on installation and use of unnecessary software other than the service

7) Updates to the device

- Software and patch updates

8) Restriction on the use of removable media

- Install USB port blocker
- Media Control Solutions

9) Supply chain risk management

- Supplier's cyber risk management process and its proper implementation
- Protection of confidential information regarding certificates, ID, authenticator(e.g. secret key or password. etc) which are produced during manufacturing process

6 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] ISO 27001 : 2013 Information security management system requirements

[6] ISO 27005 : 2018 Information security risk management

[7] The Guidelines on Cyber Security Onboard Ships V.4 produced and supported by BIMCO, CLIA, ICS, INTERCARGO,INTERTANKO, OCIMF and IUMI.

[8] NIST Cybersecurity Framework

[9] IEC 63154 Maritime navigation and radiocommunication equipment and systems – cyber security – General requirements, methods of testing and required test results.

[10] MSC.1/Circ.1610 Initial descriptions of maritime services in the context of e-Navigation

7 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