Cyber Resilience Approval/Survey Guide for Ship Automation Systems

2024 (Rev.0)

Marine & Ocean Equipment Team

Preface

Dear Valued Customers,

We, KR, are proud to deliver the Cyber Resilience Approval and Survey Guide for Ship Automation Systems. As we stand on the brink of significant digital transformation, this guide presents the culmination of Korean Register's efforts to fostering maritime safety and safeguarding ship automation systems from evolving cyber threats.

The guide provides valuable resources and survey items designed to help clients manage and fortify the systems installed on their ships, achieving cyber resilience. KR has incorporated state-of-the-art technologies and real-life case studies into this resource to provide practical insights and solutions.

KR's series of guides, covering every segment of shipping industry, serves as a compass, guiding clients through the complexities of sophisticated technologies, These guides support clients in obtaining approvals and inspections across all industry segments. KR offers these guides to assist clients prepare for technological changes and strive to overcome challenges, contributing to a safer and more reliable maritime transportation environment.

As part of KR's commitment to delivering cutting-edge technical guide, we sincerely seek your unwavering support.

Thank you.

Korean Register

Executive Vice President of Technical Division

KIM Yeontae

Notice

The integration of ICT technology into international voyage ships is expanding significantly. As satellite connections advance, data transmission between ships and shore is becoming more frequent, increasing exposure to cyber threats. Consequently, the maritime industry is witnessing a rise in cyber-attacks and incidents, prompting regulatory bodies, led by IMO and Shippers' Associations, to implement practical cybersecurity regulations. In response, International Associations of Classification Societies (IACS) issued IACS UR E27, the unified requirements for the cyber resilience of on-board systems and equipment, in 2022. The revised version UR E27 Rev.1 will be uniformly implemented on ships contracted for construction on or after 1 July 2024, applying to major on-board systems and equipment.

Promptly responding to IACS release, Korea Register issued the first cyber resilience guidelines for on-board systems and equipment in April 2024, based on the requirements of IACS UR E27 Rev.1. This guide provides comprehensive guidelines for applying the requirements in Chapters 1 and 3 of the 'Guidance for Cyber Resilience of Ships and Systems' to on-board systems and equipment.' It also incorporates KR's extensive experience in providing cybersecurity technical services, as outlined in the 'Guidance for Conformity Certification of Maritime Equipment Cybersecurity.' The primary aim of this guide is to assist system suppliers and KR surveyors in understanding and applying cyber resilience requirements, as well as in preparing for and implementing the necessary approval and survey processes.

Please note that Korean Register is not responsible for any legal disadvantages that may arise from commercial sale of this guide or from actions that do not align with its intended purpose. Additionally, if any controversy or dispute arises from the use of this document in cyber resilience-related activities, it will not hold legal effect.

The images included in this document are intended solely to aid understanding and are not directly related to the content. If you identify any mistranslation or typographical errors in this document, please contact KR (Marine & Ocean Equipment Team.) Corrections will be made in future revisions of the document.

2024.06.28.

Korean Register

Marine & Ocean Equipment Team

Revision History

Revision No.	Date	Descriptions	Remarks
0	2024.06	Established	

Index

Chapter 1 . Introduction

Section 1 . General

1. Background of implementation cyber resilient requirements

(1) Increasing cyber risk in the maritime domain

The convergence of ICT (Information and Communications Technology) in the maritime domain such as smart ships, autonomous ships and cargo terminals, is accelerating.

The control methods of many important OT (Operation Technology) systems, including propulsion, steering and navigation systems on ships, are transitioning from stand-alone systems to a computer-based systems. As OT systems become interconnected with IT (Information Technology) systems and their interdependence increases, the risk of cyber attacks also rises.

Since the late 2010s, Hackers' cyber attacks, which previously targeted primarily land-based organizations and companies, have begun to focus on the maritime domain. There have been numerous incidents where maritime organizations such as shipowners, port facilities, international organizations and classification societies have suffered from cyber attacks. Reports of such incidents are increasing and are expected to continue rising.

Given these developments, cybersecurity is imperative to protect critical systems onboard ships. Cyber attacks can significantly impact personal information, human safety, ship safety and the marine environment. International awareness of the importance of cybersecurity is expected to increase.

(2) Vulnerabilities of onboard OT systems

Cyber attackers may target any combination of people and technology to achieve their goals, exploiting remote connections between onboard systems and ashore, or any other accessible points. As the technology and sophistication of cyber attacks evolve each year, safeguarding ships against both current and emerging threats involves a range of measures that are constantly evolving and meticulously managed. Establishing a common set of minimum functional and performance criteria is essential to ensure a ship can be described as cyber resilient.

OT systems require operation and management for up to 20 years post- installation, unlike IT systems. This extended operational time presents challenges in applying the latest security patches and managing vulnerabilities effectively due to the unique operating environments of ships.

Critical OT systems have traditionally undergone hardware environmental tests and software functional tests for Category II and Category III systems, as specified in Part 6, Chapter 2 of class rules; previously, cybersecurity verification was not required. Consequently, proactive measures are now vital to prevent significant cyber incidents, given the vulnerability of critical onboard systems.

(3) Progress of IACS discussion

Responding to global calls for cybersecurity regulations for ships, IACS established Cyber System Panel in 2016, resulting in 'Rec. 166 Recommendation on Cyber Resilience' by 2020. Building upon these recommendations, IACS released UR E26 and UR E27 in 2022, comprehensive unified requirements to implement cyber resilience on ships and their onboard equipment.

- UR E26 : Cyber resilience of ships
- UR E27 : Cyber resilience of on-board systems and equipment

IACS UR E26 outlines the minimum requirements for cyber resilience of ships, defining specific criteria across five (5) distinct components: Identify/Protect/Detect/Respond/Recover, in accordance with the NIST (National Institute of Standards and Technology) CSF (Cyber Security Framework).

IACS UR E27 specifies the minimum requirements for cyber resilience of critical on-board systems and equipment. It provides selected requirements from IEC 62443-3-3, the international standard for cybersecurity of industrial automation systems. These standards are intended to be applied globally, enhancing cybersecurity functions for ships.

Initially, IACS planned to apply the UR (Unified Requirements) for cyber resilience to ships and onboard systems contracted for construction after January 1, 2024. However, the original UR E26 and UR E27 versions needed document approval and survey requirements for practical application. Consequently, IACS revised these URs to further include documentation and survey requirements, ensuring practical application by stakeholders, including ship owners, shipyards and suppliers. The revised Unified Requirements, UR E26 Rev.1 and UR E27 Rev.1, were officially published in the second half of 2023. The original versions of UR E26 and E27 were withdrawn, and the application date of the revised Unified Requirements was postponed by six months, with the new implementation date set for ships contracted for construction on or after 1 July 2024.

IACS emphasizes that cyber incidents considered in UR E26 and E27 are those caused by cyber attacks targeting ship's OT systems. For system and equipment hardware failures or functional

failures caused by software bugs, it is necessary to meet the requirements outlined in the Rules for the Classification of Steel Ships Part 6, Chapter 2, rather than the requirements for cyber resilience.

2. Goals and objectives of technical guide document

The ultimate goal of KR Guidance for Cyber Resilience of Ships and Systems (hereinafter referred to as Guidance for Cyber Resilience) is to ensure the cyber resilience of ships, which is comprise various systems essential for navigation and operation.

Critical OT systems that perform key functions must have cyber resilience capabilities to achieve a cyber resilient ship. Therefore, ensuring cyber resilience for systems is the starting point and a prerequisite for building a cyber resilient ship. In this regard, Guidance for Cyber Resilience defines cyber resilience requirements for ships in Chapter 2 and cyber resilience requirements for systems on ships necessary for overall ship cyber resilience in Chapter 3.

This technical guide document relates to Chapter 3 of Guidance for Cyber Resilience, providing directions for applying cyber resilience requirements to systems, mainly for system suppliers. Additionally, it offers detailed information on the preparations and survey procedures required for KR cyber resilience type approval and individual product surveys. This document aims to minimize the trial and error of customers' preparation and implementation of cyber resilience testing by KR and to improve customer satisfaction with KR survey services.

3. Foundations of cyber resilience

The following sections outline the fundamental cybersecurity and cyber resilience theories necessary for understanding the Guidance.

(1) Understanding information security, cybersecurity and cyber resilience

Information security generally refers to security of IT systems. The most widely applied international standard for information security is ISO 27001, a well-established international certification system. ISO 27000 focuses on preserving the confidentiality, integrity, and availability of information assets.

In contrast, cybersecurity focuses on protecting of the services provided by OT systems. The most representative standard for cybersecurity is the IEC 62443 series of standards developed by the International Society of Automation (ISA). IEC 62443-1-1 defines cybersecurity as the measures necessary to prevent unauthorized use, denial of service, modification, disclosure, loss of revenue and/or destruction of critical systems or information assets. The primary purpose of cybersecurity is to protect the confidentiality, integrity and availability of OT systems. While in information security prioritizes confidentiality, cybersecurity places greater

emphasis on the availability of assets.

Cyber resilience is a recently introduced concept by IACS to ensure that ships can maintain minimumsafe operations during a cyber incident. This concept enhances current cybersecurity measures by including recovery and response. According to UR E26 Rev.1, cyber resilience is defined as follows :

"The capability to reduce the occurrence and mitigate the effects of cyber incidents arising from the disruption or impairment of operational technology (OT) used for the safe operation of a ship, which potentially lead to dangerous situations for human safety, safety of the vessel and/or threats to the environment."

While both information security and cybersecurity aim to protect assets from cyber attacks, cyber resilience focuses on ensuring that essential operations can continue functioning effectively during a cybersecurity incident.

(2) The primary purpose of cybersecurity

In general, the three (3) elements of cybersecurity often mentioned in industry are confidentiality, integrity and availability, collectively known as the CIA model. Below is a list of the implications of each element:

1) Availability: Ensuring timely and reliable access to and use of system information and functions.

2) Integrity: Protecting the accuracy and completeness of assets.

3) Confidentiality: Preserving recognized restrictions on access to and disclosure of information.

[Figure 1] Three elements of cybersecurity

The primary purpose of cybersecurity is to protect the confidentiality, integrity and availability of OT systems from external cyber threats. Among these three (3) core elements, the priority

from a cybersecurity perspective is availability, followed by integrity and confidentiality.

Category	IT system	OT system
Security Priority	C > I > A	A > I > C
Security Target	Information, IT Asset	Field devices, OT asset
Risk factor	Data	Cyber Physical System
OS	OS (Windows, Linux..)	Industrial OS
Communication	IT Protocol (TCP/IP)	OT Protocol (S7, Modbus, etc)
Component Lifetime	3~5 years	15~20 years
System Patch	Essential	Operational impact

[Figure 2] Comparison of characteristics of IT and OT systems

For instance, if a disruption occurs in the availability of the propulsion system, the ship can face critical issues since the system provides pivotal services. Similarly, a problem with the integrity of navigational equipment like ECDIS can lead to navigator misjudgments, potentially causing a ship accident. Lastly, if confidentiality is compromised and information of important cargo on the ship is leaked to pirates, the ship becomes a prime target.

(3) Onboard computer-based system

According to Chapter 1 Clause 103 of Guidance for Cyber Resilience, cyber resilience on ships covers only computer-based systems that provide critical services. This focus is due to the nature of cyber attacks, which primarily target computer-based systems running on software rather than physical systems.

Chapter 1 Section 2 of Guidance for Cyber Resilience defines a computer-based system as "a programmable electronic device, or interoperable set of programmable electronic devices, organized to achieve one or more specified purposes such as collection, processing, maintenance, use, sharing, dissemination, or disposition of information. CBSs onboard include IT and OT systems. A CBS may be a combination of subsystems connected via network. Onboard CBSs may be connected directly or via public means of communications (e.g., Internet) to ashore CBSs, other vessels' CBSs and/or other facilities".

4. Limitations

This technical guide is the initial document created prior to the effective date of Guidance for Cyber Resilience and provides application examples for the design of cyber resilience functions for systems and equipment. The actual design and implementation may differ based on the customer's development environment and the unique characteristics of their system. This guidance does not mandate strict adherence to the provided examples but serves to aid

understanding. Ultimately, the responsibility for the design and implementation lies with the customer.

Korean Register is not liable for any inaccuracies or omissions in this document. The customer is responsible for understanding their systems and applying the necessary security controls and requirements. This guide aims to provide a framework that addresses some possible security contingencies.

Section 2 . Scope of applicability

1. General

Whether a system is subject to cyber resilience is ultimately confirmed through class approval of the asset list and the application exclusion risk assessment submitted by the shipyard at the new building stage. Since system suppliers need to implement cyber resilience functions and prepare for type approval in advance, confirming applicability only at the new building stage can present challenges. Therefore, it is beneficial for suppliers to identify and prepare for the applicability of Guidance for Cyber Resilience to the systems they provide well ahead of time.

2. Determine system is required cyber resilient

Determining whether a system is subject to cyber resilience requirements can be reviewed in the following order:

(1) Is the ship where the system is installed subject to 'Guidance for Cyber Resilience'?

According to Chapter 1 of Guidance for Cyber Resilience, the cyber resilience requirements apply to ships contracted for construction on or after 1 July 2024, The types of ships subject to compulsory application are as follows:

1) Passenger ships, including passenger high-speed craft, engaged in international voyages
2) Cargo ships of 500 GT and upwards engaged in international voyages
3) High speed craft of 500 GT and upwards engaged in international voyages
4) Mobile offshore drilling units of 500 GT and upwards
5) Self-propelled mobile offshore units engaged in construction, such as wind turbine installation maintenance and repair, crane units, drilling tenders, accommodation, and others.

(2) Are the systems within the scope of cyber resilience requirements?

Systems within the scope of cyber resilience requirements are installed on ships subject to mandatory application. These systems are limited to computer-based systems that may affect the safety of human life, safety of ships and marine pollution in the event of a cyber incident.. In this regard, the scope of system specified in Chapter1, Clause 103.2 of Guidance for Cyber

Resilience includes:

1) Operational Technology (OT) systems onboard ships
Operational Technology (OT) systems onboard ships, specifically CBSs that use data to control or monitor physical processes, can be vulnerable to cyber incidents. If compromised, these systems could lead to dangerous situations for human safety, the safety of the vessel and/or environmental threats. The CBSs used for the operation of the following ship functions and systems, if present onboard, shall be considered:
(a) Propulsion
(b) Steering
(c) Anchoring and mooring
(d) Electrical power generation and distribution
(e) Fire detection and extinguishing systems
(f) Bilge and ballast systems, loading computer
(g) Watertight integrity and flooding detection
(h) Lighting, including emergency lighting, low-locations lightning, and navigation lights.
(i) Any required safety system whose disruption or functional impairment may pose risks to ship operations, such as emergency shutdown systems, cargo safety systems, pressure vessel safety systems, and gas detection systems

2) Navigation and communication systems
(a) Navigational systems required by statutory regulations
(b) Internal and external communication systems required by the Class rules and statutory regulations

Even if a system is not included in the list mentioned above, it should be considered within the scope of cyber resilience if it falls under system category II or III, according to KR Rules for the Classification of Steel Ships Part 6, Chapter2, Section4.

(3) Is the system acceptable to do risk assessment for exclusion?
Even if a system satisfies all of the criteria in (1) and (2) above, it can be excluded from the requirements if the Society verifies that it meets all the minimum acceptable criteria and additional acceptance criteria through a cyber risk assessment for exemption, in accordance with Chapter 1, Section3 of Guidance for Cyber Resilience. For further instructions, see Section 3.

3. Recommendations for system suppliers to respond exclusion
(1) For systems that do not meet all four (4) minimum acceptance criteria
Since exclusion from application is anticipated to be challenging, it is necessary to prepare for

a class survey, including cyber resilience type approval, in advance.

(2) For systems that meet all four (4) minimum acceptance criteria

In this case, it is recommended to refer to the information described in Section 3 to identify and respond to the possibility of exclusion from the system.

If the supplier's own review indicates a high probability of exclusion, an exemption from the Society can be pursued through an exclusion risk assessment conducted at the ship's new building stage.

However, it is necessary to be aware in advance that, for system category III and complex systems, achieving exclusion through risk assessment may be difficult due to the low possibility of exclusion. For details on the review of exclusions, see section 3.

Section 3 . Risk Assessment for Exclusion

1. General

Even if a system is within the scope of application, it can be excluded if a risk assessment is carried out for exclusion in accordance with Guidance for Cyber Resilience Chapter 1, Section 3 and it is accepted by this Society that system meets the relevant acceptance criteria outlined in Guidance for Cyber Resilience Chapter1, Clause 304.

The risk assessment for exclusion is carried out for the OT systems to be installed on a particular ship. The system integrator or shipyard is responsible for conducting the risk assessment and submitting the assessment report to the Society. Technical support and cooperation from system suppliers are required, and it is also possible for a system integrator to outsource the risk assessment to an external expert organization.

(1) Contents of the Risk Assessment

The risk assessment covers the systems installed on a specific new building vessel and should include all systems that are eligible for exemption. The contents of the risk assessment should demonstrate, with evidence, that the cyber risk associated with the system for exemption is below the acceptable level of risk.

(2) Methods of Risk Assessment

The methodology of risk assessment should be defined and documented in advance before conducting a risk assessment.

Cyber risk assessment methods and processes can be found in various documents such as ISO

27005, IEC 62443-3-2, NIST SP 800-30 and onboard ship cybersecurity guidelines.
The following are examples of cyber risk assessments presented by 'The guidelines on cybersecurity onboard ships,' jointly published by international maritime organizations such as BIMCO, ICS, and OCIMF.

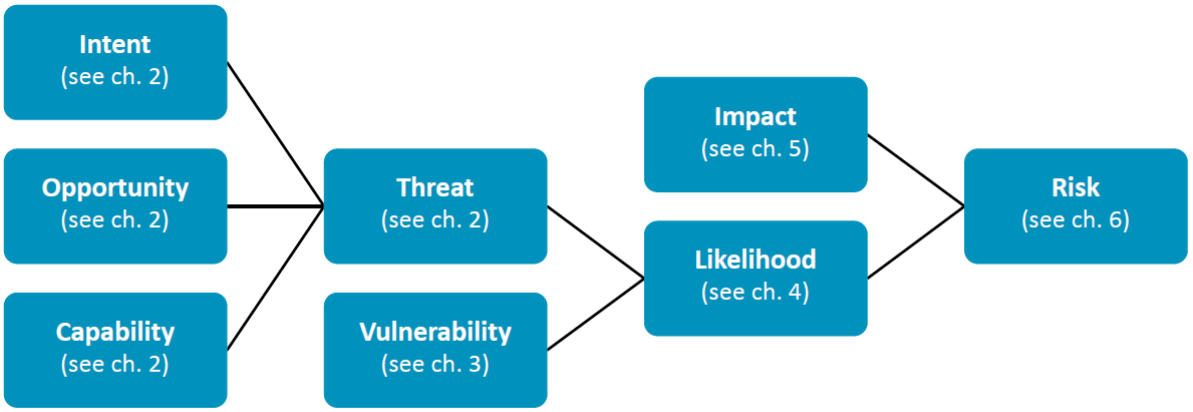


Figure 9: The relationship between different factors influencing the risk. The lines represent multiplication, ie "Likelihood" is multiplied with "Impact" to produce "Risk".

[Figure 3] Example of risk assessment

In general, many international standards or guidelines define the risk level for a cyber incident as the product of the of Cyber Threat Index, Vulnerability Index and Impact Index of the Incident, as shown below.

[Figure 4] Example cyber risk estimation

Threat Index and Vulnerability Index are multiplied to determine as the likelihood. Incident Impact Index relates to the severity of the cyber incident on the target system onboard ship and is closely linked to the system category (I, II, III). In this regard, Guidance for Cyber Resilience Chapter 1, Section 3 requires the following additional considerations when conducting a cyber risk assessment:

1) Vulnerabilities in the system
2) Internal and external threats
3) The potential impact of cyber incidents affecting assets in terms of human safety, safety of the vessel and/or threat to the environment

4) Possible effects related to the integration of systems or interfaces between systems, including systems that are not onboard, such as, where remote access to systems onboard is provided.

(3) Submission and approval of risk assessment

A cyber risk assessment should be submitted by the system integrator or shipyard to this Society's plan approval team. Upon review and verification, exemptions for certain systems may be granted.

2. Review of the system's exclusion through risk assessment

To exempt a system from following Guidance for Cyber Resilience, the system integrator or shipyard should submit a risk assessment for approval during the design and construction phases. From the supplier's perspective responding to class surveys at the ship construction stage can be challengingas it is too late to determine the system's cyber resilience applicability. Therefore, system suppliers should make an early policy judgment on whether to seek an exemption. If the probability of exclusion is high, prepare a risk assessment; if low, obtain type approval for cyber resilience requirements in advance. The possibility of exclusion can be judged based on the review criteria in (1) to (2) below.

(1) Meets all mandatory acceptance criteria

Meeting all four (4) of the following acceptance criteria is a prerequisite for conducting a risk assessment:

1) The CBS shall be isolated, having no IP-network connections to other systems or networks.

2) The CBS shall have no accessible physical interface ports. Unused interfaces shall be logically disabled, preventing unauthorized devices to the CBS

3) The CBS shall be located in areas with to controlled physical access.

4) The CBS shall not be an integrated control system serving multiple ship functions as specified in the scope of applicability. See Guidance for Cyber Resilience Chapter 1, Clause 103.

(2) Whether additional acceptance criteria are met

For the following three (3) additional acceptance criteria, it is necessary to submit a risk assessment with appropriate evidence to ensure that the company is adequately satisfied with the Society

1) The CBS should not serve ship functions of category III.

2) Known vulnerabilities, threats, potential impacts deriving from a cyber incident affecting the CBS have been duly considered in the risk assessment.

3) The attack surface for the CBS is minimized, considering its complexity, connectivity, physical and logical access points, including wireless access points.

In relation to the above additional criteria, it can be considered that, for systems in category I

or II, it is easier to meet the additional acceptable criteria through risk assessment, making exclusion possible. In contrast, special attention is required for system category III, even though Section 3 of KR Cyber Resilience Guidelines stipulates that not all of the additional acceptable criteria need to be met.
As explained earlier, cyber risk is determined by multiplying the impact index of an asset (system) by the probability of an incident (threat index X vulnerability index). Therefore, in system category III, where the impact (or severity) of the system is high, it is difficult to assess the risk as acceptable unless the likelihood of occurrence is low.

For example, in the case of VHF radios and ECO Sounders, which fall under system category III, may be exempt if they have few access points for cyber attacks and minimal cyber attack scenarios due to the simplicity and maintenance-free of nature. Conversely, general PC-based equipment (servers and workstations) and complex PLC-based control systems may be difficult to be excluded due to the high number of potential attack surfaces, making the likelihood of cyber attacks significant.

(3) System case by case exclusions

Please refer to the table below as an example of a hypothetical evaluation of the possibility of exclusion depending on the type of system for ease of understanding for the reader.

1) In the case of system A and system B, it is expected that these systems will be easily excluded through cyber risk assessment at the stage of ship design and construction.
2) In the case of C and D systems, it is expected that these systems may be excluded if the risk assessment confirms that the cyber risk is low. Additional safeguards may be required to reduce risk if requested by the Society.
3) In the case of the E system, the possibility of cyber attack is not low due to the high complexity of the system and the many possible points of attack, making the likelihood of exclusion low.

Review criteria	System A	System B	C System	D System	E System
System categories (I / II / III)	I	II	II	III	III
Meets all mandatory acceptance criteria (Yes/No)	Yes	Yes	Yes	Yes	Yes
Attack points (Many / Few[1])	Many	Few	Many	Few	Many
Exclusion possibility by risk assessment	High	High	Medium	Medium	Low

[Table 1] Example of exclusion possibility by risk assessment

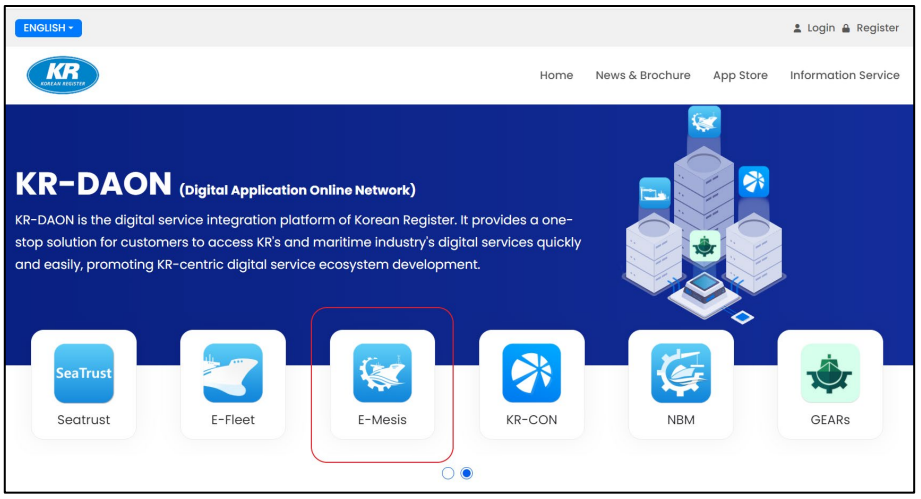
[1] Note: "Many" and "Few" refer to the expected number of cyber attack targets. "Many" indicates more potential attack points, making the system susceptible to cyber-attacks. "Few" indicates fewer potential attack points, reducing the system's cyber-attack vulnerability.

Chapter 2 . Type Approval Procedure

Section 1 . How to apply for type approval

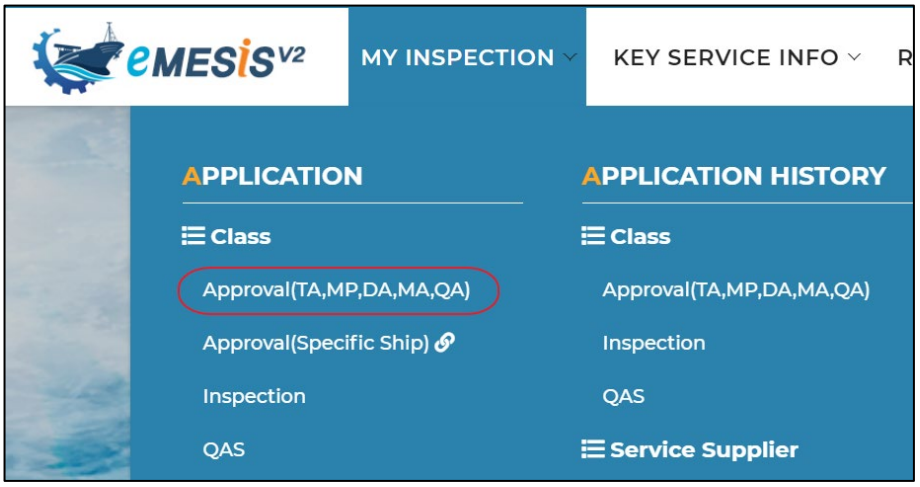
To apply type approval, Suppliers can visit and submit an online application through KR-DAON -> eMESIS at the following address :

- • https://daon.krs.co.kr/



[Figure 5] KR-DAON

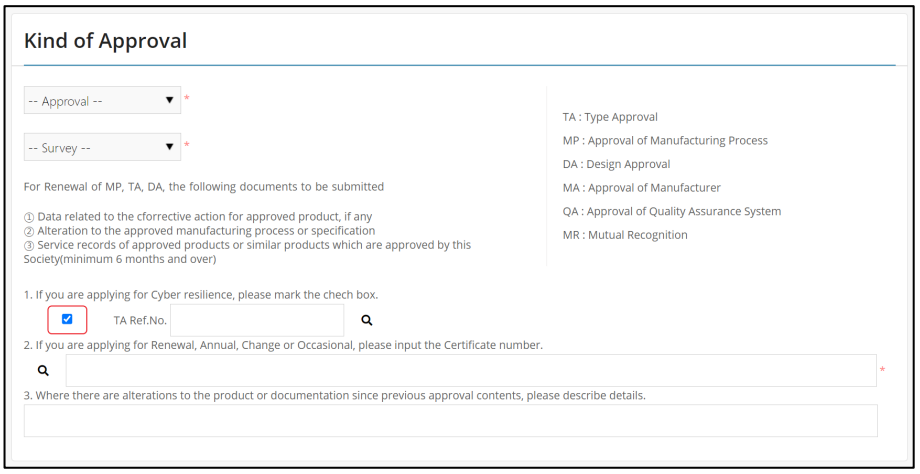
eMESIS can be accessed after registering as a KR-DAON member[2], and existing users can log in and apply through the following menu path: My Inspection -> Application -> Society -> Approval (TA, MP, DA, MA, QA)



[Figure 6] Cyber resilience type approval application menu example

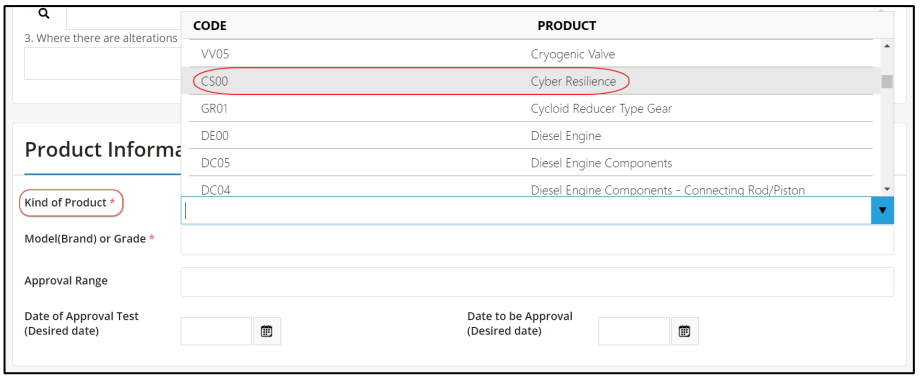
[2] Membership registration/access are available directly through eMESIS until December 2024. Starting from 2025, eMESIS can only be accessed through KR-DAON.

On the application screen, enter the necessary information of the supplier and system. In the 'Kind of Approval' menu, check the box labeled'1. If you are applying for cyber resilience, please mark the check box'.



[Figure 7] Cyber resilience type approval application example

In the 'Product Information' menu, select CS00 Cyber Resilience from the 'Kind of Product' item.



[Figure 8] Cyber resilience type approval application example

Items marked with a red asterisk (*) are mandatory. Complete the application by attaching the necessary documents, entering all required information, and clicking the submit button.

Section 2 . Procedure of type approval

Once the application for type approval is submitted, the documents are reviewed. The required approval documents and information documents are as follows:

1. Documents for approval

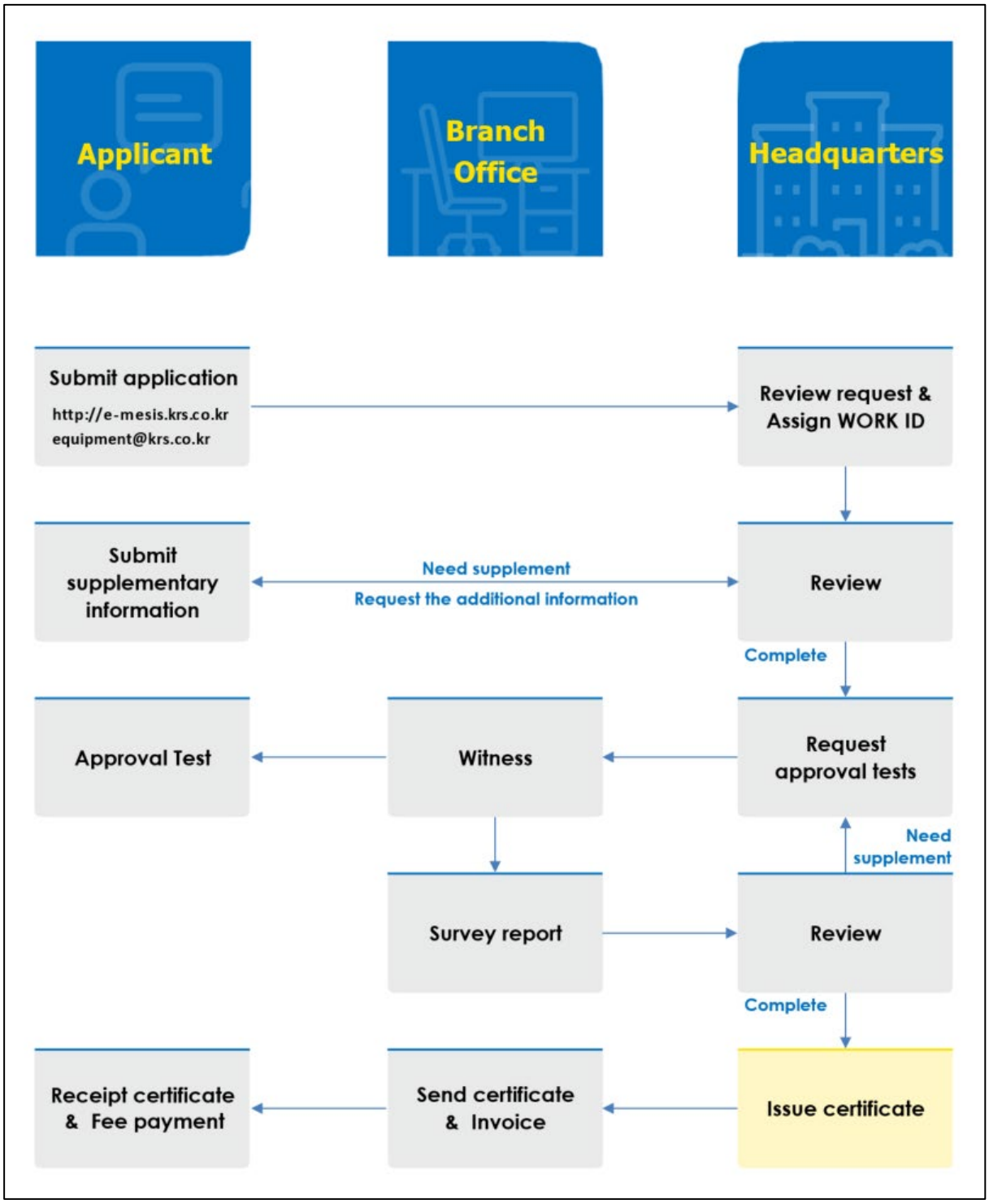
(1) CBS[3] asset inventory
(2) Topology diagrams
(3) Description of security capabilities
(4) Test procedure of security capabilities
(5) SDLC[4] documents

2. Documents for information
(1) Security configuration guidelines
(2) Plans for maintenance and verification of the CBS
(3) Information supporting the owner's incident response and recovery plan
(4) Management of change plan
(5) Test reports

Among these documents, the test reports (5)[5] are submitted after test is completed, unlike the other documents that should be submitted and approved before type test.

The type test is carried out once all documents, except the test report, are approved by this Society. The type test is conducted in the presence of this class surveyor according to the approved 'Test procedure of security capabilities'(4) and is not outsourced to an external testing agency. Additionally, a plant audit is not required[6] at the cyber resilient type approval stage. After type test is completed, the supplier should update test results of photos, and images, within the existing approved test procedure and submit it to this Society. Upon completion of submission, the Society issues a cyber resilience type approval certificate to the supplier, completing the approval process.

[3] Computer-Based System
[4] SDLC : Secure Development Life Cycle
[5] This document is submitted to the Society after completing the type test according to the test procedure and updating the result photos and images.
[6] It applies only to cyber resilience type approval. Note that a plant audit is required for type approval in accordance with 'Guidance for Approval of Manufacturing Process and Type Approval', among others.



[Figure 9] Procedure of cyber resilient type approval

Chapter 3 . Drawing approval for equipment procedure

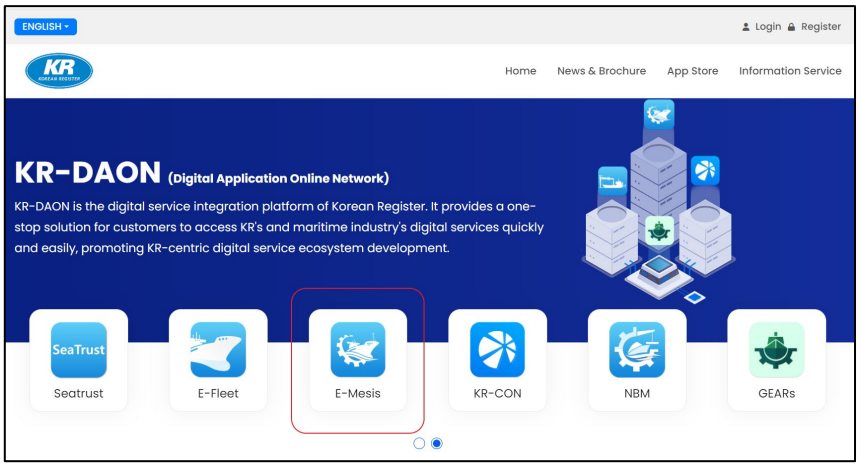
Section 1 . How to apply for drawing approval

1. How to apply for drawing approval for equipment

(1) Accessing the eMESIS webpage and moving to the EDAS screen

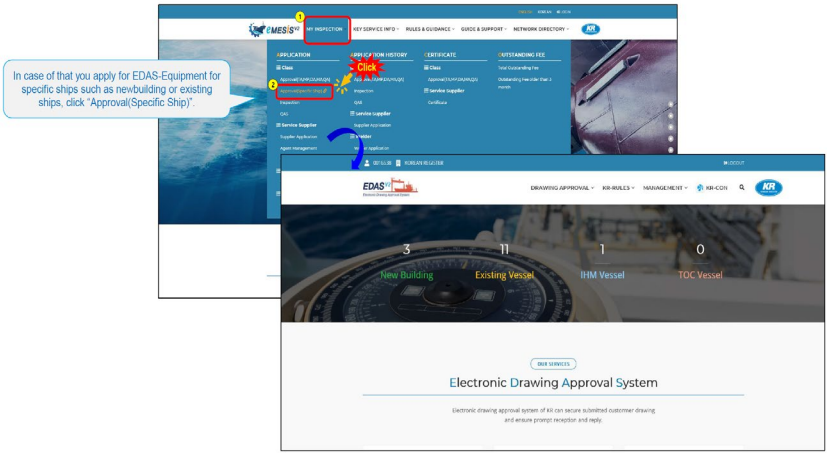
To apply for drawing approval, suppliers may log in and submit an online application through KR-DAON -> eMESIS at the following address:

- https://daon.krs.co.kr/



[Figure 10] KR-DAON

eMESIS can be accessed after registering as a KR-DAON member[7]. Existing users can log in and apply through the following menu: My Inspection -> Application -> The Society -> Approval (Specific Ship)

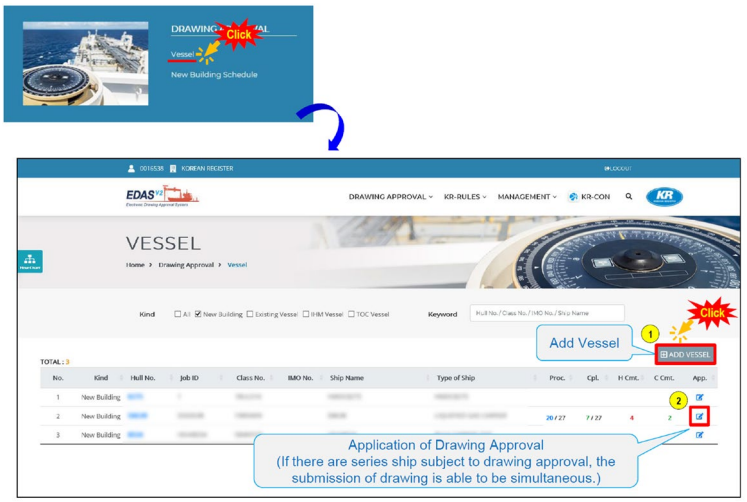


[Figure 11] Drawing approval for equipment application menu example

[7] Membership registration/access are available directly through eMESIS until December 2024. Starting from January 2025, it can only be accessed through KR-DAON.

(2) Access to drawing approval application menu (EDAS) from eMESIS menu

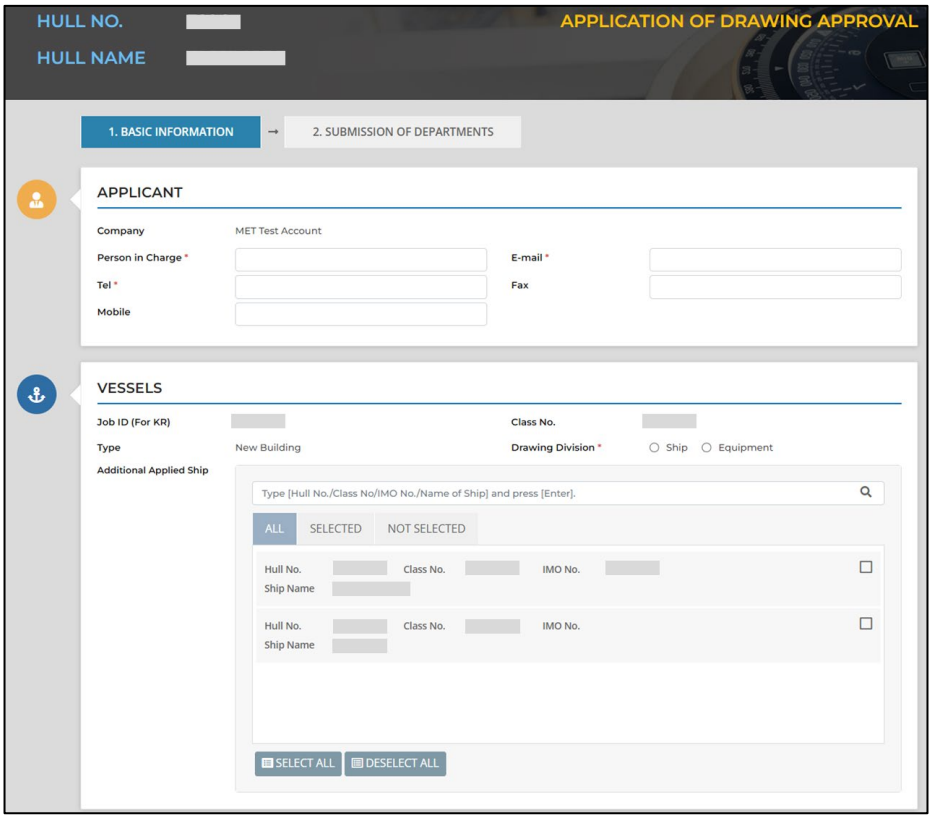
To begin, click on "DRAWING APPROVAL" -> Select "Vessel" at the top menu. This action will display a list of vessels, as shown in the figure below. If the vessel you are looking for is not listed, click "Add Vessel" to include it in the list. Once the vessel is added, click the icon in the "App." column to navigate to the application screen for drawing approval of the ship's equipment. If the vessel is already listed, simply click the icon in the "App." column corresponding to that vessel. Click the icon to proceed to the drawing approval request screen.



[Figure 12] Drawing approval for equipment menu example

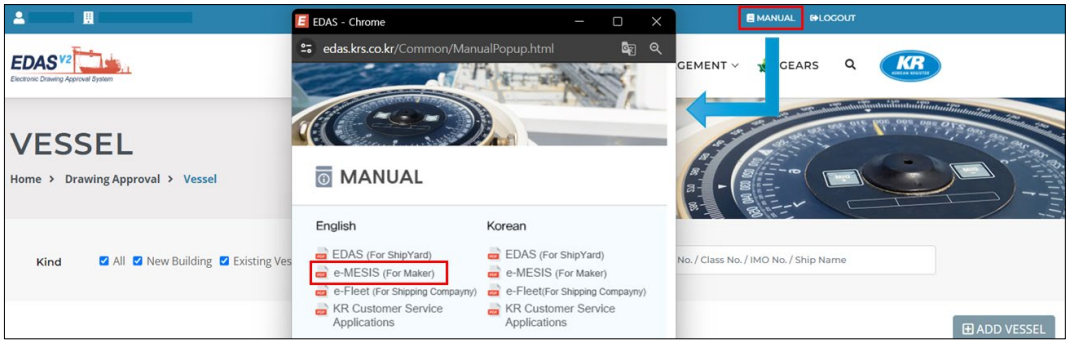
2. Application for drawing approval of equipment for ship

On the drawing approval application screen, enter the necessary application information and upload the required drawings and documents for approval.



[Figure 13] Example of application for drawing approval of ship equipment

For detailed instructions on entering information and uploading data on the drawing approval application screen, please refer to the e-MESIS manual by clicking the icon in the upper right corner of the EDAS screen.

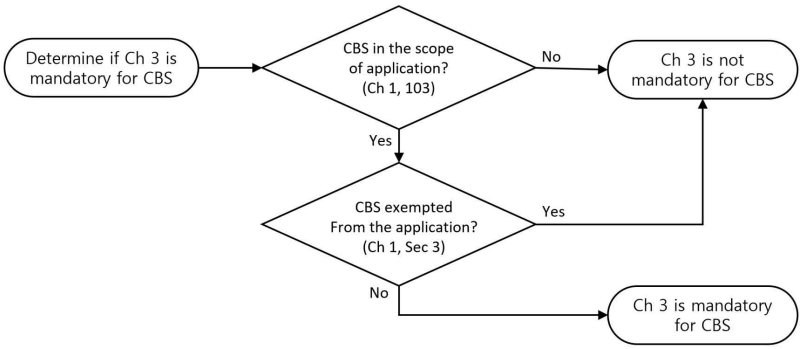


[Figure 14] Application for drawing approval of equipment for ship example

Section 2 . Drawing approval and survey procedure for ship

1. Determine if cyber resilience applies

Suppliers, in cooperation with the System integrator or shipyard, should determine if cyber resilience requirements are mandatory for the CBS

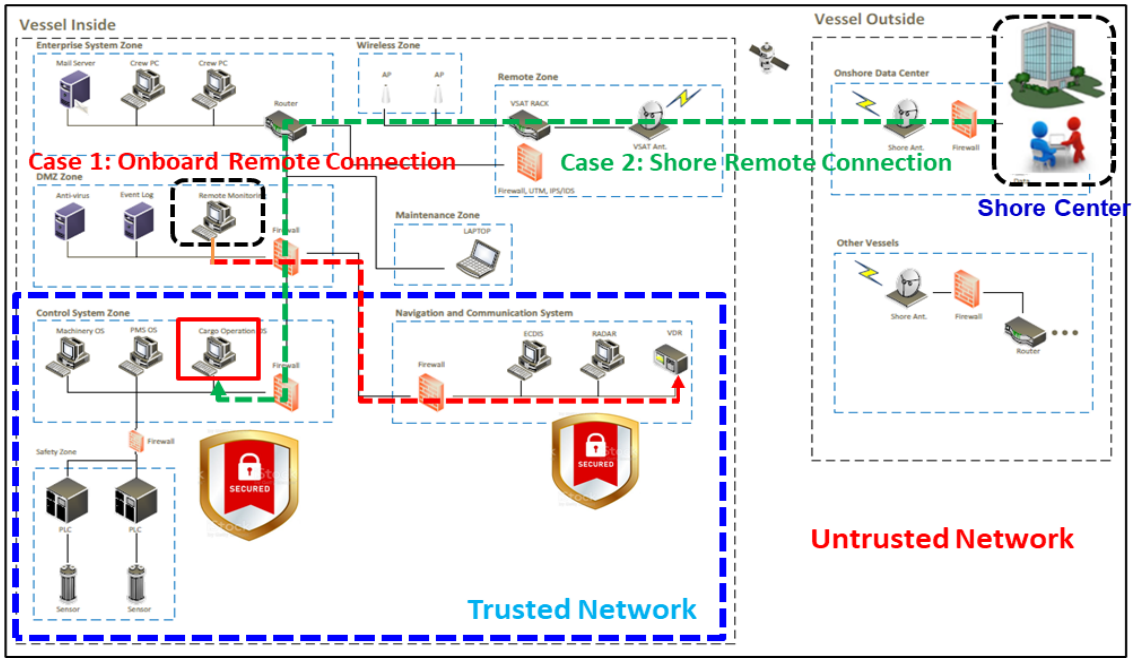


[Figure 15] Determine if cyber resilient requirements are mandatory for the CBS

2. Check the remote connection interface of the system

If the system installed onboard is identified as requiring cyber resilience, the supplier should consult with the system integrator to ensure that it provides a remote connectivity interface.

A remote connection exists between a system with applied cyber resilience requirements and an untrusted network. The system that meets these cyber resilience requirements is considered a trusted network, while the system that does not is regarded as an untrusted network.



[Figure 16] Remote connection interface example

There are two (2) main types of remote connections onboard:

1) System within the scope of application is connected to an onshore system outside the ship (e.g., remote maintenance, and others.)
2) System within the scope of application is connected to other systems or equipment located on the ship's untrusted network (e.g., collecting data from the shipowner.)

(1) For systems without remote connections:

Meet security capability requirements in accordance with Guidance for Cyber Resilience Chapter 3, Clause 401

- thirty (30) mandatory security functions are required

(2) For systems with remote connections:

Meet security capability requirements in accordance with Guidance for Cyber Resilience Chapter 3, Clause 401 and 402.

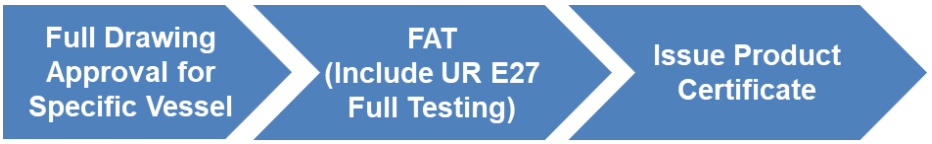
- forty-one (41) security functions are required (thirty (30) mandatory security functions + eleven (11) additional security functions.)

3. Drawing approval procedure for ship-specific

(1) Systems cyber resilience type approved

A reduced set of vessel-specific drawing approval is required for systems cyber resilience type approved (see Chapter 4, Section 1.) A cyber resilience test during FAT is not required unless specified by the Society. Shop tests must be carried out in accordance with Rules for the Classification of Steel Ships Part 6, Chapter 2, 301.2.

(2) Systems not cyber resilience type approved



A complete set of vessel-specific drawing approvals is required. Additionally, a cyber resilience test during FAT is mandatory.

(3) Systems cyber resilience type approved, but are not required to be approved and surveyed in Rules for the Classification of Steel Ships Part 6 Chapter 2 (e.g., GMDSS, RADAR, ECDIS , others.)

While systems, such as **GMDSS, RADAR, and ECDIS,** may not require a survey under Rules for the Classification of Steel Ships Part 6 Chapter 2, they are subject to Guidance for Cyber Resilience Chapter 1. Common examples include navigation and radiocommunication systems required by SOLAS or emission reduction systems required by MARPOL. In case these systems have received cyber resilience type approval, no equipment survey is required, allowing for delivery to the system integrator after reduced drawing approval for the specific vessel.

4. Drawing approval procedure for specific vessel

As described above, reduced drawing approval is accepted for cyber resilient type-approved system by the Society. Otherwise, full drawing approval is required including type approval.
Supplier applications for drawing approval for specific vessels are processed through EDAS. For detailed documents requirements, please refer Chapter 4.

5. Exceptions for navigation and radio communication equipment

In accordance with Guidance for Cyber Resilience Chapter 1, Clause 106, the application of equivalent standards such as IEC 61162-460 for navigation and radio communication equipment may be accepted by this Society.

In case where an equivalent standard is applied instead of the security function requirements of Guidance for Cyber Resilience Chapter 3, Section 4, the supplier should seek ship-specific drawing approval. Surveys should be conducted for ship-specific drawing approval, and, if necessary, these surveys should take place at the supplier's factory.

Additional verification is required to ensure the system meets Guidance for Cyber Resilience Chapter 2 requirements at the equipment drawing approval stage. Additional data submission and testing may be required, if the Society deems it necessary.

Chapter 4 . Required documents for submission

Section 1 . Documents list for submission

1. Documents list for submission

System supplier subject to cyber resilience approval should apply type approval and drawing approval for specific vessel in accordance with Guidance for Cyber Resilience Chapter 3, Clause 202.

Table 3.2.1 below lists the documents and requirements that suppliers should submit for approval following specific vessel type approval or drawing approval.

As mentioned in Chapter 3, a reduced set of drawing approvals is required for cyber resilient type-approved systems. However, full drawing approval is necessary if the system is not type-approved.

Table 3.2.1 Document list for submission

No.	Document	Requirements	TA	Drawing approval	
				with TA	without TA
1	CBS asset inventory	To be incorporated in Vessel asset inventory (Ch 2, 401. 1)	Approve	Approve	Approve
2	Topology diagrams	Enabling System integrator to design security zones and conduits (Ch 2, 402. 1)	Approve	Approve	Approve
3	Description of security capabilities	Required security capabilities (Ch 3, 401.)	Approve		Approve
		Additional security capabilities, if applicable (Ch 3, 402.)			
4	Test procedure for security capabilities	Required security capabilities (Ch 3, 401.)	Approve		Approve
		Additional security capabilities, if applicable (Ch 3, 402.)			
5	Security configuration guidelines	Network and security configuration settings (Ch 3, 401. item no.29)	Info		Info
6	Secure development lifecycle	SDLC requirements (Ch 3, Sec 5)	Approve		Approve
7	Plans for maintenance and verification	Security functionality verification (Pt 6, Ch 2 Sec 4 of the Rules)	Info		Info
8	Information supporting incident response and recovery plans	Auditable events (Ch 3, 401. item no.13)	Info		Info
		Deterministic output (Ch 3, 401. item no.20)	Info		Info
		System backup (Ch 3, 401. item no.26)	Info		Info
		System recovery and reconstitution (Ch 3, 401. item no.27)	Info		Info
9	Management of change plan	Management of change process (Pt 6, Ch 2 Sec 4 of the Class Rules)	Info		Info
10	Test reports	Configuration of security capabilities and hardening (Ch 3, 301. 5, 501. 7)	Info	Info	Info

2. Requirements for documentation

(1) CBS asset inventory

CBS asset inventory is a document that lists information about the assets (components) that make up the system and should include a list of components for both system hardware and software.

1) List of hardware components

The list should include name, brand/ manufacturer, model/type, short description of functionality/purpose, physical interfaces, name/type of the system software[8], version/patch level of system software and supported communication protocols.

2) List of software components

The list should include hardware component where software is installed, brand/manufacturer, model/type, short description of functionality/purpose and software version information.

(2) Topology diagrams

A topology diagram is a document that shows the system connection of components. Both physical topology diagram and logical topology diagram should be submitted. A combined topology diagram is acceptable in case it includes all required information as one diagram.

1) Physical topology diagram

A diagram should be prepared to confirm the physical architecture (configuration) and identify hardware components in the CBS asset list. In addition, the diagram should illustrate all endpoint and network devices that make up the network, including redundant units. Cable information should be provided for all communication cables such as hardwired I/O, serial communications including RS 422/485, and ethernet communications. If the system is connected to other systems networks, the network and communication cable information should also be illustrated.

2) Logical topology diagram

A logical topology diagram displays the construction structure of a logical network and should be designed to clearly illustrate the data flow among the system components. The flow includes information about network devices, such as switches, routers, firewalls, and so on, and terminal devices, such as servers, workstations, HMI, PLC devices, and similar machines at communication endpoints. It should present how the data flows and the communication

[8] System software: Software that directly controls, integrates and manages hardware components. System software includes operating system (OS), drivers, utilities, firmware, database management system (DBMS). System software serves as the counterpart to application software.

protocol information between the devices should be illustrated. Communication endpoints should also cover virtual machines (e.g., VMWARE) if used and the physical and virtual communication paths (e.g., VLANs) should be shown.

(3) Description of security capabilities

The description of security capabilities is a document describing how supplier's system meets the security function requirements in Guidance for Cyber Resilience Chapter3, Section 4. It should detail satisfaction of requirements for thirty (30) mandatory security functions and eleven (11) additional security functions.

All network interfaces, covering the system's both internal and external parts, should be detailed, using information from the CBS asset list and topology diagram. If the system connects to an untrusted network[9], and if there is, eleven (11) additional security features should be applied. If the system does not connect to an untrusted network, only the thirty (30) mandatory security functions should be described.

(4) Test procedure of security capabilities

The test procedure of security capabilities document outlines how to demonstrate, through testing, that the supplier's system meets the security function requirements of Guidance for Cyber Resilience Chapter 3, Section 4.

The document should have the necessary test setup, equipment, initial conditions, detailed test steps, methodology, and expected results/acceptance criteria. After completing the type test, the supplier should add the photos and images of the test results to the test procedure and send the test report to the Society. The test procedure should leave room for the test result update.

(5) Security configuration guidelines

Security configuration guidelines are documents that guides outline configuration settings and initial values of security functions. Upon installation onboard, the configuration should be set up according to the security setting instructions. This should be followed by a verification process to ensure the adequacy of the security settings. The initial values to be configured include:

1) User accounts
2) Authorization
3) Password policies

[9] Networks not covered by Guidance for Cyber Resilience, such as onshore connections and network connections to onboard systems not subject to this guidance and related references.

4) Safe state of machinery
5) Firewall rules, if a firewall is provided

(6) Secure development lifecycle (SDLC) documentation

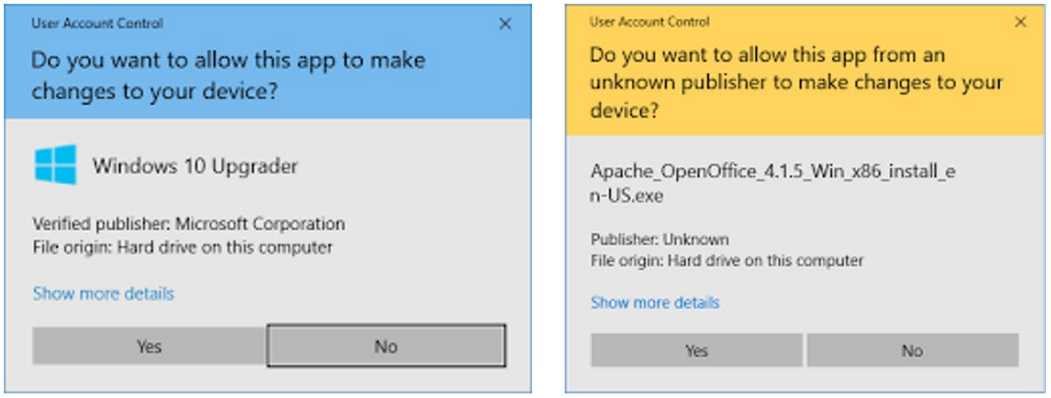
Secure Development Lifecycle (SDLC) requirements are process requirements aimed at ensuring the security of a product across its entire lifecycle, from development to retirement. Based on the requirements of IEC 62443-4-1, these requirements include seven (7) quality processes and procedures that supplier must adhere to for managing the system post-delivery. Suppliers are mandated to establish processes in accordance with SDLC requirements and to prepare and implement suppliers' policies/procedures accordingly.

1) Controls for private keys (IEC 62443-4-1/SM-8)

In case where code signing is applied, supplier should implement procedures and technical controls in place to protect the private key used for code signing.

Code signing is a method of digitally signing an application software to verify the origin, supplier or provider, of the program and ensure it has not been tampered with since its original creation. As shown on the left side of [Figure 17], when a user runs a code signed program distributed by the supplier, the supplier's information is displayed. In case program has been tampered with, the signature will be damaged and a warning message will be displayed when the program is run, as shown on the right side of [Figure 17]. In case a user runs a program that is not code signed, a warning message will also be displayed.

The supplier needs to obtain a certificate for code signing and must be able to sign executable files and update files using a code signing tool, such as Digital Signature Wizard Code Signing, or similar components.



[Figure 17 Example of running a code signed file (left) and running an unsigned file (right)

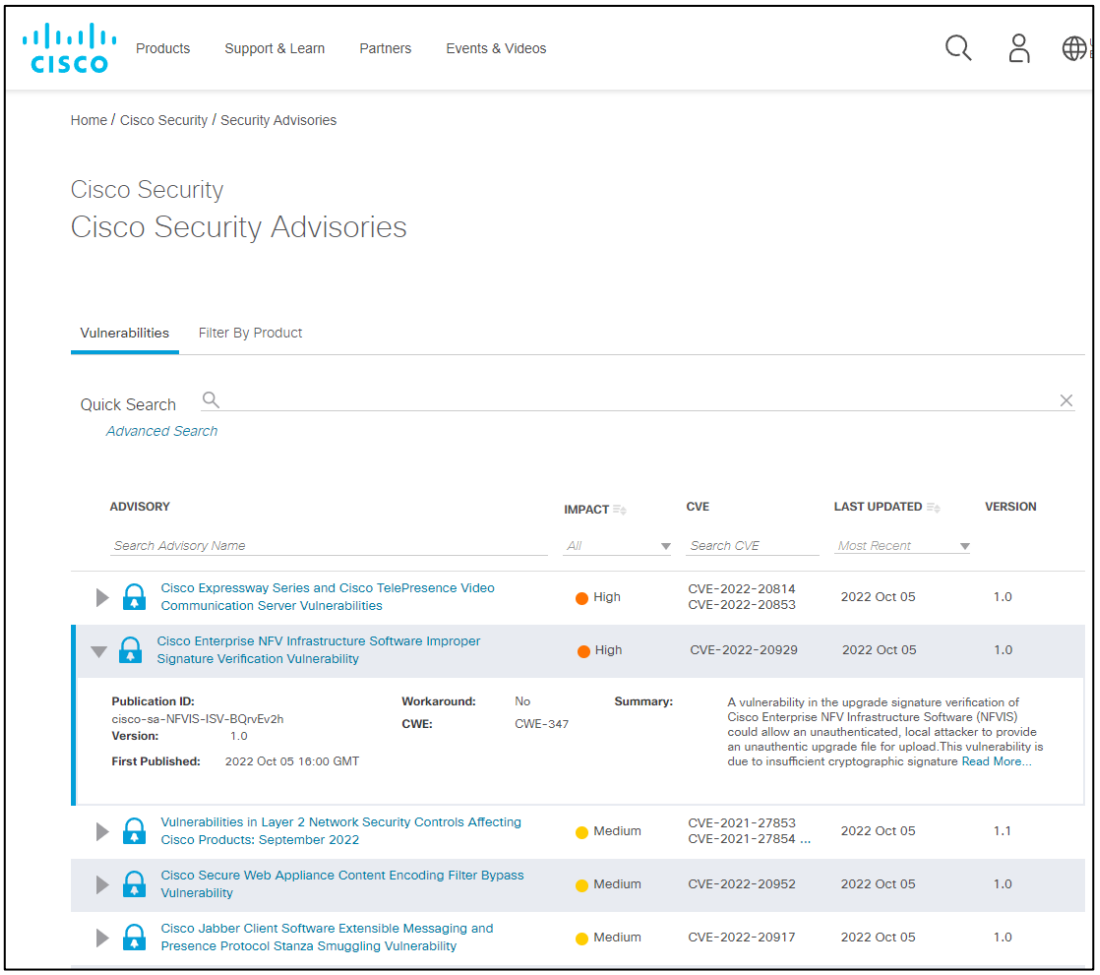
The private key is included within the certificate used for code signing. If passwords for these

certificates and signatures are compromised and leaked, hackers can maliciously distribute files under the guise of legitimate suppliers. This poses a significant risk, as users may mistakenly perceive such files as safe and inadvertently execute them. Therefore, suppliers employing code signing should establish robust manage policies and procedures to protect their private keys, password and certificate.

2) Security update documentation (IEC 62443-4-1/SUM-2)

Security updates should be conducted using approved patch files provided by the supplier, with a secure delivery process in place. The product supplier should provide documentation detailing the available security patches, instructions on how to install authorized patches, methods for recognizing the patch status of the system and procedures for identifying unauthorized patches. Provision can be made through various channels such as documents, sending e-mails or postings on the website. The processes should include, at minimum, the following details:

- The product version number(s) to which the security patch applies
- Instructions on how to apply approved patches manually and via an automated process
- Description of any impacts that applying the patch to the product can have, including reboot
- Instructions on how to verify that an approved patch has been successfully applied
- Risks associated with not applying the patch and possible mitigations for patches that are not approved or deployed by the asset owner.



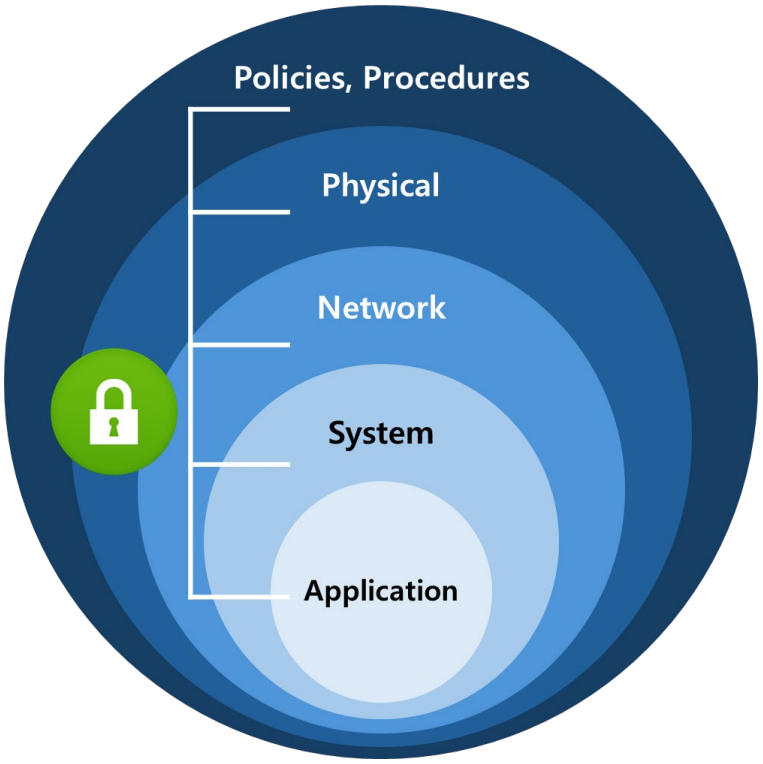
[Figure 18] Example of providing security update <source: CISCO>

3) Dependent component or operating system security update documentation (IEC 62443-4-1/SUM-3)

A dependent component is an external component that the system depends on. For example, if a supplier's system purchases and uses Oracle's MySQL, and the system is not feasible to operate without MySQL, then MySQL becomes a dependent component of the system. Dependent components and operating system of Windows, Linux, and other OS, that configure the system provide security updates. However, users often hesitate to update them due to the risk of system malfunctions. To provide an appropriate service, suppliers should provide users with information about whether security updates for the operating system and dependent components are compatible with the system and have a process for doing so.

4) Security update delivery (IEC 62443-4-1/SUM-4)

Security updates delivered to users should be verifiable as authentic. Patch files containing malware or corrupted updates can cause serious problems in the system. For instance, distributing code-signed patch files is an example where suppliers should have an internal testing process in place before distribution.



[Figure 19] Example of defense in depth model

5) Product defense in depth (IEC 62443-4-1/SG-1)

Defense in depth is the concept of applying multiple layers of independent security controls across a system. This approach guarantees that even if one security control and defense is compromised by a specific attack, the remaining effective security controls will continue to protect the system.

The protection layer of defense-in-depth strategy can be broadly categorized into three (3) areas: physical, technical and administrative.

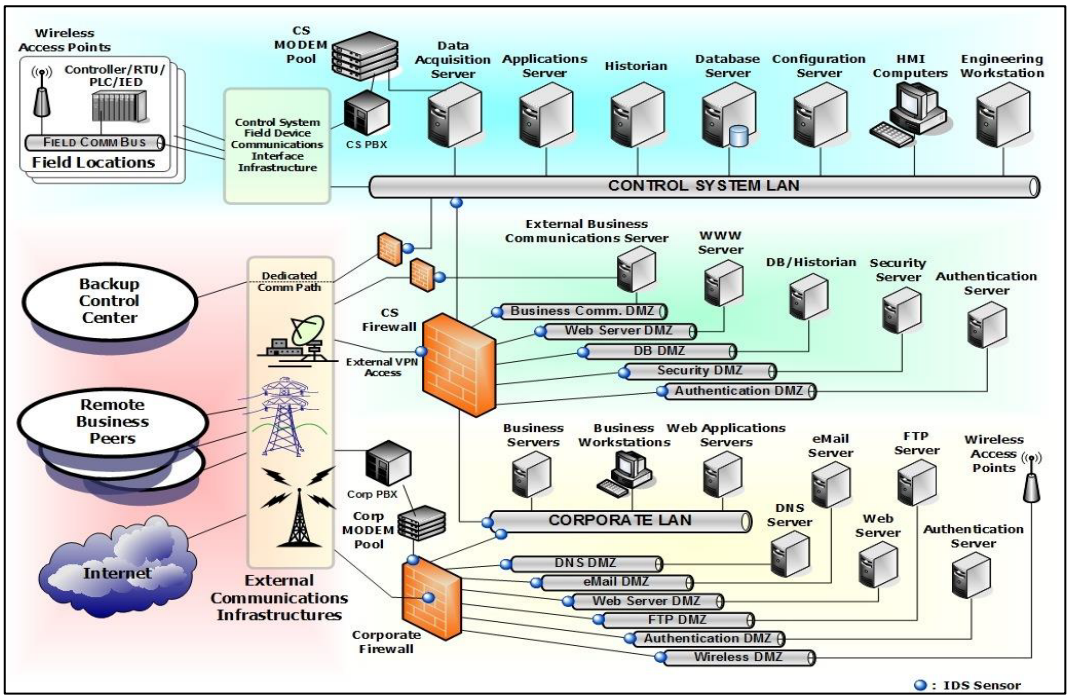
1) Administrative controls: Organizational policies and procedures, security-related guidelines, education and training.

2) Physical controls: Measures that restrict physical access to the system

3) Technical controls: Technical security measures for system hardware or software and networks.

The 'SG' in IEC 62443 4-1 stands for Security guidelines. SDLC requirements set forth in Guidance for Cyber Resilience focus on post-delivery management. Suppliers should establish a defense-in-depth strategy to support the installation, operation and maintenance of their system. Additionally, a process for generating documentation describing these strategies should be in place. The process should include the following at the minimum:

- Security capabilities implemented by the product and their role in the defense-in-depth strategy
- Threats addressed by the defense-in-depth strategy
- Threats addressed by the defense-in-depth strategy



[Figure 20] Recommended Defense In Depth Architecture <source : NIST SP 800-82 R.2>

6) Defense in depth measures expected in the environment (IEC 62443-4-1/SG-2)

A process shall be employed to create product user documentation that describes the security defense-in-depth measures expected to be provided by the external environment in which the product is to be used. Examples of a security-related environment:

- Location on the network
- Physical or cybersecurity measures in the environment where the product is installed
- Network Isolation
- Potential environmental impacts, if verifiable, such as loss of life, personal injury, loss of production, and so on.

7) Security hardening guidelines (IEC 62443-4-1/SG-3)

A process shall be employed to create product user documentation that includes guidelines for hardening the product when installing and maintaining the product. The guidelines shall include a comprehensive set of instructions, rationale and recommendations pertaining to, though not restricted to, the following:

- Integration of the product, including third-party components, with its product security context

- Security requirements for API[10] and protocol integration when the user's software application is integrated with the system.
- How to apply and maintain the system's defense in depth strategy
- Recommended configurations and security options/features to support security policies for the use of each part of the system (local) that the user uses
- How to use and recommendations for all security-related tools/utilities for management, monitoring, incident response and assessment of system security
- How to carry out recommended regular security maintenance activities
- Best practices for maintaining and managing the system

(7) Plans for maintenance and verification of the CBS

Plans for maintenance and verification of the CBS should include procedures for security-related maintenance and testing of systems. This document supports the verification of the correct operation of the system's security functions as required by Cyber Resilience Guideline Chapter3, Section 401 requirements item no. 19. According to IEC 62443-3-3 SR 3.3, which is the reference for this requirement, the basis of the standard and examples of security verification functions according to the supplementary guidelines are as follows:

1) Verification of antivirus measures by European Institute for Computer Antivirus Research (EICAR) through testing of the computer-based system's file system. The EICAR test file is available at the following address:

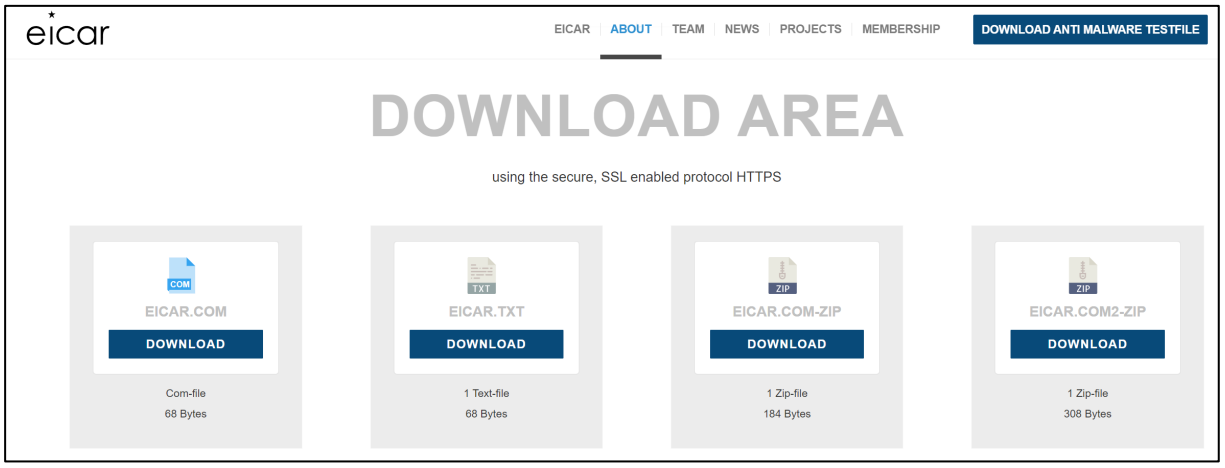
https://www.eicar.org/download-anti-malware-testfile/

If an antivirus program is available, using a real virus to test its malware detection ability poses significant risks. To ensure safety, EICAR collaborates with antivirus companies to distribute EICAR test file. The file is not an actual virus but is designed to be recognized as one by antivirus programs, allowing for secure testing.
The EICAR test file is as follows:

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

To test the antivirus program, paste the above string into a notepad and a text editor and save the file. The antivirus program should then notify you that a virus has been detected.

[10] API (Application Programming Interface): A connection between a computer or a computer program. An interface that connects computers or software to each other, as opposed to a user interface that connects a computer and a human.



[Figure 21] Example of download EICAR test file <source : www.eicar.org>

2) Verification of the identification, authentication and use control measures by attempting access with an unauthorized account.
3) Verification of IDSs as a security control by including a rule in the IDS that triggers irregular activity. (if an IDS provided)
4) Confirmation that audit logging is active as required by security policies and procedures and has not been disabled by any internal or external entity.

(8) Information supporting the owner's incident response and recovery plan

This document provides the foundational information that ship owners need to develop an incident response and recovery plan in accordance with the requirements of Guidance for Cyber Resilience Chapter 2, Clause 404.1 (Incident Response Plan) and Clause 405.1 (Recovery Plan) during the operational phase of the vessel. This document shall include procedures and descriptions of:

1) Local Independent Control (see KR Cyber Resilience Guideline Chapter 2, Clause 404.2)
2) Network isolation (see KR Cyber Resilience Guidelines Chapter 2, Clause 404.3)
3) Forensics using audit records (see Required security capabilities No. 13)
4) Deterministic output (see Required security capabilities No. 20)
5) Backup (see Required security capabilities No. 26)
6) Recovery (see Essential Security Features No. 27)
7) Controlled shutdown, reset, rollback and restart (see Cyber Resilience Guidelines Chapter 2, Clause 405.3)

(9) Management of change plan

The management of change plan is a document for the managing changes to the software. It covers the procedures for changing the software, identifying the version, analyzing the impact of the change, rolling back in case of failure, confirming/verifying the change, recording the

change. This plan is also required in KR Rules for the Classification of Steel Ships Part 6, Chapter 2, Section 4. For details, refer to the relevant requirements.

(10) Test reports

After conducting tests in accordance with the approved security function test procedures, the test results should be updated, and the test report should be submitted to the Society.

Chapter 5 . Security function requirements

Section 1 . General

1. Identify remote connection interface

System supplier shall identify the equipment that provides remote connection interfaces among the system components. This distinction is essential because components without remote connection interfaces only need to meet the thirty (30) mandatory security feature requirements. In contrast, components with remote connection interfaces should meet these mandatory requirements in addition to an additional eleven (11) security features.

The system integrator or shipyard confirms the use of remote connection interfaces during the installation of the actual in-ship system during the design and construction phase. However, since the scope of application of the requirements of type approval varies from the supplier's perspective, who needs to prepare for type approval in advance, the system supplier must review the need for a remote connection interface in advance, consult with the system integrator or shipyard, and prepare for type approval. For details on remote connectivity, see Chapter 3 of the Technical Guide.

2. Determine the scope of coverage of security feature requirements for each component of the system

Depending on whether a remote connection interface is provided among the system components, the scope of application of the requirements for each component varies:

(1) If there is no remote connection interface: thirty (30) security capability requirements apply

Components of a system without a remote connection interface should meet the requirements for mandatory security capabilities as follows:

1) Mandatory Security capabilities (thirty (30) requirements)

Objective	Q'ty of Requirements	Reference
FR.1 Identification and Authentication control (IAC)	7 EA	Ch.3, 401. KR Guidance for Cyber Resilience IEC62443-3-3
FR.2 Use Control (UC)	9 EA	
FR.3 System Integrity (SI)	4 EA	
FR.4 Data Confidentiality (DC)	2 EA	
FR.6 Timely Response to Events (TRE)	1 EA	
FR.7 Resource Availability (RA)	7 EA	
Total	**30 EA**	

[Figure 22] Required (Mandatory) security capabilities

(2) If there is a remote connection interface: forty-one (41) security feature capability

requirements apply

System components with a remote connection interface should meet the thirty (30) required security capability requirements, along with the eleven (11) additional security capability requirements as follows:

1) Mandatory Security capabilities (thirty (30) requirements)

Objective	Q'ty of Requirements	Reference
FR.1 Identification and Authentication control (IAC)	7 EA	Ch.3, 401. KR Guidance for Cyber Resilience IEC62443-3-3
FR.2 Use Control (UC)	9 EA	
FR.3 System Integrity (SI)	4 EA	
FR.4 Data Confidentiality (DC)	2 EA	
FR.6 Timely Response to Events (TRE)	1 EA	
FR.7 Resource Availability (RA)	7 EA	
Total	**30 EA**	

[Figure 23] Required (Mandatory) security capabilities

2) Additional security capabilities (eleven (11) requirements)

Objective	Q'ty of Requirements	Reference
FR.1 Identification and Authentication control (IAC)	6 EA	Ch.3, 402. KR Guidance for Cyber Resilience / IEC 62443-3-3
FR.2 Use Control (UC)	1 EA	
FR.3 System Integrity (SI)	4 EA	
Total	**11 EA**	

[Figure 24] Additional security capabilities

3. Application of compensation measures

Suppliers may encounter difficulties in applying some security functions due to the system's operating environment and the equipment's characteristics. In such cases, according to Guidance for Cyber Resilience Chapter 3, Clause 104.4, compensation measures can be applied in place of one or more difficult-to-satisfy security functions.

When applying compensation measures, the supplier should specify the security functions to which the compensation measures are applied in the security function description submitted at the stage of type approval or drawing approval of equipment for the arc. The supplier should describe the compensation measures and demonstrate in the documentation that these measures provide security equivalent to or greater than the original security features.

Section 2 . Required security capabilities explanation and example

1. Identification and authentication (KR Guidance for Cyber Resilience CH 3.401)

(1) Understanding security functional requirements

Identification refers to verifying the user's identity, while authentication confirms that the

user's identity has been verified, To connect to the server that provides service, the user should log in by entering an ID and password. In this context, the ID served as the identifier and the password as the authenticator. An account includes both an identifier and an authenticator. Besides passwords, other types of authenticators include OTPs[11], security cards, certificates, and similar authentication tools.

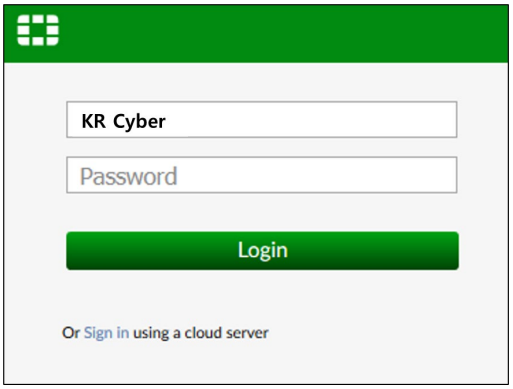
The system should implement identification and authentication functions for interfaces accessible to human users, such as a human machine interface(HMI). If the system includes a wireless network, identification and authentication should be applied to it. Additionally, the system should support the generation and management of IDs and PWs. If any authenticators use passwords, a password complexity function is required. This function enforces a specific number of digits and combinations of numbers and letters when creating passwords, protecting against brute-force attacks. The input value (feedback) of authenticator should be obscured such as **** to prevent exposure of the authentication input. In case authenticator failure, the system should avoid providing information about whether the ID or PW is incorrect.

[Figure 25] Example of Fortinet firewall log in
<source : Fortinet>

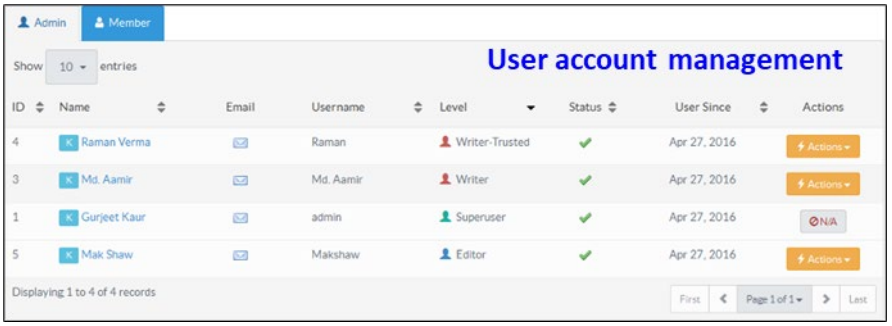
(2) Explanation and examples of security functional requirements

Objective	1. Human user identification and authentication	Standard	IEC62443-3-3/SR1.1
Require-ments	The CBS shall identify and authenticate all human users who can access the system directly or through interfaces		
Target	The requirement should be applied to all CBS. Where the implementation is not feasible, a detailed explanation of compensation measures may be required.		
Explan-ation	All human users need to be identified and authenticated for all access to the computer based system. Authentication of the identity of these users should be accomplished by using methods such as passwords, tokens, biometrics or, in the case of multifactor authentication, some combination thereof. The geographic location of human users can also be used as part of the authentication process. This requirement should be applied to both local and remote access to the computer based system. In addition to identifying and authenticating all human users at the computer based system level (for example, at system logon),		

[11] OTP : One Time Password

	identification and authentication mechanisms are often employed at the application level. Where human users function as a single group (such as control room operators), user identification and authentication may be role-based or group-based. For some computer based systems, the capability for immediate operator interaction is critical. It is essential that local emergency actions as well as computer based system essential functions not be hampered by identification or authentication requirements. Access to these systems may be restricted by appropriate physical security mechanisms. An example of such a situation is a critical operations room where strict physical access control and monitoring is in place and where shift plans allocate responsibility to a group of users. These users may then be using the same user identity. In addition, the designated operator workstation clients should be authenticated or the use of this shared account should be limited to the constrained environment of the control room.
Example	The system can be used after undergoing identification and authentication procedures such as logging in at an interface accessible to human users (e.g. HMI, and others.). However, due to the importance of availability in onboard systems, certain essential functions accessible without identification and authentication, such as monitoring function of the control system, emergency stop function, are always provided, alarm setting values can be changed, after log in.  [Figure 26] Example of Fortinet firewall log in <source : Fortinet>

Objective	2. Account management	Standard	IEC62443-3-3/SR1.3
Require-ments	The CBS shall provide the capability to support the management of all accounts by authorized users, including adding, activating, modifying, disabling and removing account.		
Target	This requirement should be applied to all CBS. Where implementation is not feasible, a detailed explanation of compensation measures may be provided.		
Explan-ation	Account management may include grouping of accounts (for example, individual, role-based, device-based and computer based system), establishment of conditions for group membership and assignment of associated authorizations. In certain CBS instances, where individual accounts are determined to be unnecessary from a risk-analysis and/or regulatory aspect, shared accounts are acceptable as long as adequate compensating		

	countermeasures (such as limited physical access or organizational measures for approval) are in place and documented.
Example	Provides a function to support management of all accounts from a specific account, such as an administrator account.  [Figure 27] Example of account management <source : www.phpkb.com>

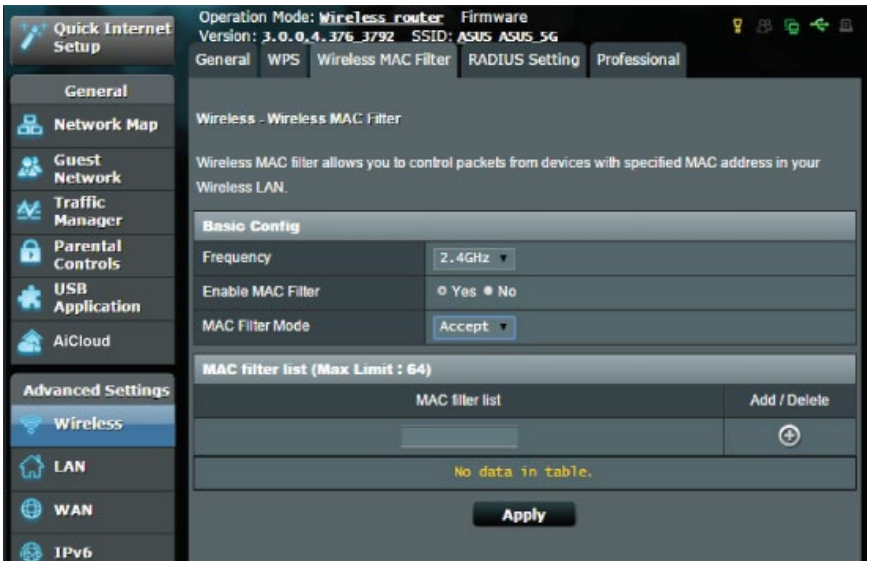
Objective	3. Identifier management	Standard	IEC62443-3-3/SR1.4
Require-ments	The CBS shall provide the capability to support the management of identifiers by user, group and role.		
Target	The requirements applies to all CBS. Where implementation is not feasible, a detailed explanation of compensation measures may be provided.		
Explan-ation	Identifiers are distinguished from the privileges which they permit an entity to perform within a specific computer based system control domain or zone. Where human users function as a single group (such as control room operators), user identification may be role-based, group-based or device-based. For some computer based systems, the capability for immediate operator interaction is critical. Local emergency actions for the computer based system should not be hampered by identification requirements. Access to these systems may be restricted by appropriate compensating countermeasures. Identifiers may be required on portions of the computer based system but not necessarily the entire computer based system. For example, wireless devices typically require identifiers, whereas wired devices may not.		
Example	Provides the capability to manage each user's identifier (ID).		

Objective	4. Authenticator management	Standard	IEC62443-3-3/SR1.5
Require-ments	The CBS shall provide the capability to: - Initialize authenticator content - Change all default authenticators upon computer based system installation - Change/refresh all authenticators - Protect all authenticators from unauthorized disclosure and modification when stored and transmitted.		

Target	These requirements applies to all CBS. Where implementation is not feasible, a detailed explanation of compensating measures may be provided.
Explan-ation	In addition to an identifier an authenticator is required to prove identity. Computer based system authenticators include, but are not limited to, tokens, symmetric keys, private keys (part of a public/private key pair), biometrics, passwords, physical keys and key cards. Human users should take reasonable measures to safeguard authenticators, including maintaining possession of their individual authenticators, not loaning or sharing authenticators with others and reporting lost or compromised authenticators immediately. Authenticators have a lifecycle. When an account is created automatically a new authenticator needs to be created, in order for the account owner to be able to authenticate. For example, initial authenticator content could be interpreted as the administrator defining the initial password which the account management system sets for all new accounts. Being able to configure these initial values makes it harder for an attacker to guess the password between account creation and first account use (which should involve the setting of a new password by the account owner). Some computer based systems are installed with unattended installers which create all necessary accounts with default passwords and some embedded devices are shipped with default passwords. Over time, these passwords often become general knowledge and are documented on the Internet. Being able to change the default passwords protects the system against unauthorized users using default passwords to gain access. Passwords can be obtained from storage or from transmission when used in network authentication. The complexity of this can be increased by cryptographic protections such as encryption or hashing or by handshake protocols which do not require transmission of the password at all. Still, passwords might be subject to attacks, for example brute force guessing or breaking the cryptographic protection of passwords in transit or storage. The window of opportunity can be reduced by changing/refreshing the passwords periodically. Similar considerations apply to authentication systems based on cryptographic keys. Enhanced protection can be achieved by using hardware mechanisms such as hardware security modules like trusted platform modules (TPMs). The management of authenticators should be specified in applicable security policies and procedures, for example, constraints to change default authenticators, refresh periods, specification of the protection of authenticators or firecall procedures. Lockout or loss of control due to security measures is not acceptable. If the computer based system is required to have a high level of availability, measures should be taken to maintain this high level of availability (such as compensating physical countermeasures, duplicate keys and supervisory override). Besides the capabilities for authenticator management specified in this requirement, the strength of the authentication mechanism depends on the strength of the chosen authenticator (for example password complexity or key length in public key authentication) and the policies for validating the authenticator in the authentication process (for example how long a password is valid or which checks are performed in public key certificate validation).
Example	The system provides management functions for authenticators. For instances, where the authenticator is a password, the following functions are included:

	- If the user forgets the password or cannot use it for other reasons, a function is provided to reset the password through administrator privileges or separate user confirmation. - A function is provided that forces the user to change and use the initial password assigned when first using the system. - A periodic password change function is provided. - When saving a password in the server's DB (Data Base), the system stores the hash value of the password instead of the actual password This function ensures that the user's actual password remains unknown even if the password is leaked externally.

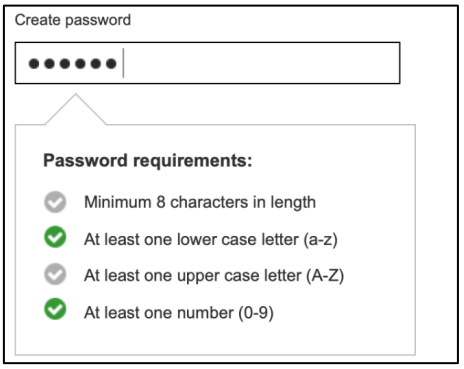
Objective	5. Wireless access management	Standard	IEC62443-3-3/SR1.6
Require-ments	The CBS shall provide the capability to identify and authenticate all users (humans, software processes or devices) engaged in wireless communication.		
Target	This function applies only when CBS uses wireless network communication.		
Explan-ation	Any wireless technology can, and in most cases should, be considered just another communication protocol option, and thus subject to the same C security requirements as any other communication type utilized by the CBS. However, from a security point of view, there is at least one significant difference between wired and wireless communications: physical security countermeasures are typically less effective when using wireless. For this and possibly other reasons (for example regulatory differences), a risk analysis might legitimately result in a higher security level for wireless communications versus a wired protocol being used in an identical use case. Wireless technologies include, but are not limited to, microwave, satellite, packet radio, Institute of Electrical and Electronics Engineers (IEEE) 802.11x, IEEE 802.15.4 (ZigBee, IEC 62591 – WirelessHART®, ISA-100.11a), IEEE 802.15.1 (Bluetooth), wireless LAN mobile routers, mobile phones with tethering and various infrared technologies.		
Example	When wireless network devices are included in the system, they provide identification and authentication capabilities for all wireless users.		

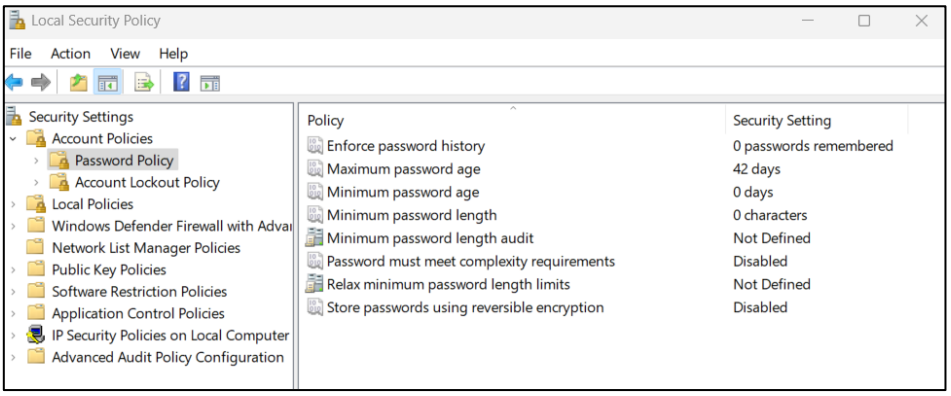


[Figure 28] Example settings menu for wireless network users

Objective	6. Strength of password-based authentication	Standard	IEC62443-3-3/SR1.7
Require-ments	The CBS shall provide the capability to enforce configurable password strength based on minimum length and variety of character types.		
Target	This function becomes active when CBS manages passwords authenticators, as defined in “4. Authenticator Management.”		
Explan-ation	User authentication based on a username and a secret password is a very commonly used mechanism. Many attacks on such mechanisms focus on guessing the password (for example, dictionary attacks or targeted social engineering) or breaking the cryptographic protection of the stored password representation (for example, using rainbow tables or brute-forcing a hash collision). Increasing the size of the set of valid passwords by increasing the number of allowed characters makes such attacks more complex, but only if the increased set size is actually used (generally users would tend to not include special characters in a password as they are perceived as harder to remember). Limiting the lifetime of a password decreases the window of opportunity for an attacker to breach a given password’s secrecy. In order to prevent users from circumventing this control by once changing their password to a new one and then immediately changing back to their original password, a minimum lifetime for a password is commonly enforced as well. A notification to change the password prior the expiration allows the user to change the password at a convenient time according to process operations conditions. This protection can be further enhanced by limiting the reuse of passwords (preventing small sets of alternating passwords), which further decreases the usefulness of a once-		

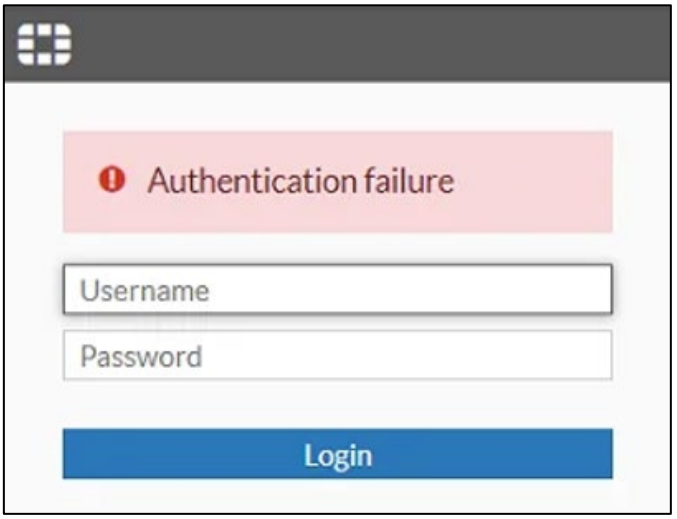
	breached password. Extended protection beyond password based mechanisms can be achieved using multifactor authentication.
Example	Provides a function to enforce complexity when setting a user's password. Examples of complexity include: Passwords are required to be at least 6 characters long and contain characters from three of the following four categories: - English capital letters (A - Z) - English lowercase letters (a - z) - Digits 10 numbers (0 - 9) - Non-alphabetic characters, such as !, $, #, %





[Figure 29] Example password complexity setting

Objective	7. Authenticator feedback	Standard	IEC62443-3-3/SR1.10
Require-ments	The CBS shall obscure feedback during the authentication process.		
Target	This requirement applies to all CBS. Where implementation is not feasible, a detailed explanation of compensatory measures may be required.		
Explan-ation	Obscuring feedback protects the information from possible exploitation by unauthorized individuals, for example, displaying asterisks or other random characters when a human user types in a password obscures feedback of authentication information. Other examples		

	include the entry of wired equivalent privacy (WEP) keys, secure socket shell (SSH) token entry and RSA one-time passwords. The authenticating entity should not provide any hint as to the reason for the authentication failure, such as “unknown user name”.
Example	When using a password, the input is marked with asterisks of ****, ensuring the value remains hidden.. In the event of incorrect ID/PW entry, the system does not specify which part is incorrect.  [Figure 30] Managing authenticator feedback

2. Use control and audit records

(1) Understanding security functional requirements

This section details ‘Use control,’ which defines the security functional requirements for enforcing the assignment of privileges to authenticated users and monitoring the use of those privileges. These requirements ensure that users are granted the minimum level of access necessary to perform their duties, with their authority restricted to the minimum required for their roles. The scope of the application should encompass all possible areas, including all interfaces accessible to human users. The system should assign permissions on all such interface.

Functionalities for authorization, monitoring, and restriction of wireless connections should be provided when using a wireless network. Where portable and mobile devices, such as laptops and USB drives, are used, the system must implement controls over their usage.

Mobile code refers to programs transferred between systems that run without explicit installation. Examples include JavaScript, ActiveX controls, and browser extensions including Chrome by Google. In case the system provides mobile code functionalities, it should also incorporate a control function.

A session is a semi-permanent, traceable exchange of interactive information between two or more communicating components over a network connection. Once logged in, users can navigate the system without re-entering credentials for each page, as a session is established to manage data transmission between users and servers. However, session hijacking poses a significant security risk. An unauthorized user can exploit a compromised session to gain access without logging in. Therefore, computer-based system should provide session protection functions to prevent hijacking. These measures include automatic session termination after a predetermined period of inactivity or manual logout by the user. Additionally, if remote access is supported, the system should also allow remote session termination.

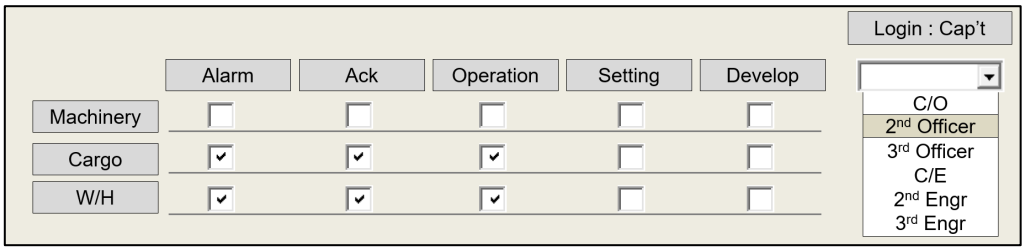
Computer based system should also generate and maintain security-related audit records and respond to failures in audit processing. The minimum data recorded in these logs should include:

- Access control events
- Operating system events
- Backup and restore events
- Configuration changes
- Loss of communication

Access control audit records capture critical information related to user access, including logins/logouts and login failures. Audit records of operating system events include entries for reboots, shutdowns, and similar activities. Examples of audit records for communication loss include monitoring the connection status between the internal and external parts of the system and recording any communication failures. Each audit records should include timestamps to indicate when events occurred, guaranteeing users can determine the exact time of each event.

Audit processing failure should not result in the loss of essential services and functions of the system. The system must allocate sufficient storage capacity for audit records and ensure that critical services are not compromised. For instance, if the storage space for audit records is shared with that of essential services, accumulating audit records over time could lead to insufficient storage space for critical services, potentially causing issues. If the storage capacity for audit records reaches a certain level, the system should automatically delete old records or prevent the saving of new records. Additionally, the system should provide alarms to alert users when storage capacity is nearly complete. Audit records should be accessible only for reading to prevent unauthorized modification/deletion by users.

(2) Security function requirements explanation and examples

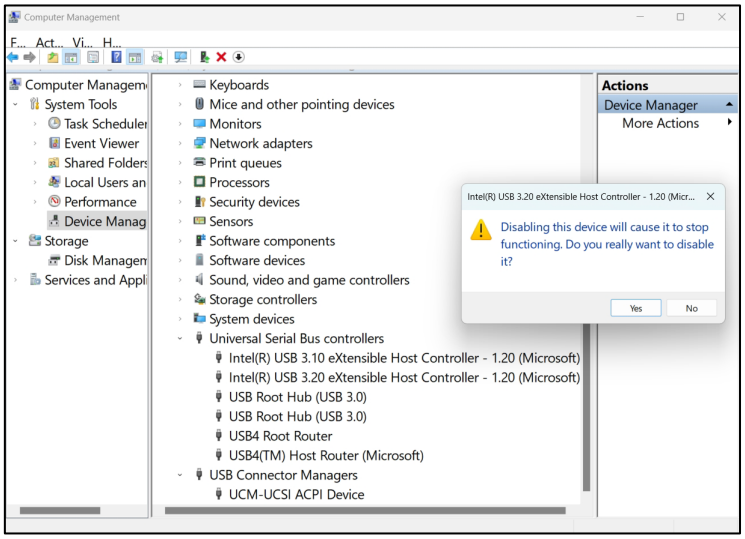
Objective	8. Authorization enforcement	Standard	IEC62443-3-3/SR2.1
Require-ments	On all interfaces, human users shall be assigned authorizations in accordance with the principles of segregation of duties and least privilege.		
Target	This requirement applies to all CBS. Where implementation is not feasible, a detailed explanation of compensation measures may be required.		
Explan-ation	Use control policies (for example, identity-based policies, role-based policies and rule-based policies) and associated read/write access enforcement mechanisms (for example, access control lists, access control matrices and cryptography) are employed to control usage between users (humans, software processes and devices) and assets (for example, devices, files, records, software processes, programs and domains). After the computer based system has verified the identity of a user (human, software process or device), it also has to verify that a requested operation is actually permitted according to the defined security policies and procedures. For example, in a role-based access control policy, the computer based system would check which roles are assigned to a verified user or asset and which privileges are assigned to these roles – if the requested operation is covered by the permissions, it is executed, otherwise rejected. This allows the enforcement of segregation of duties and least privileges. Usage enforcement mechanisms should not be allowed to adversely affect the operational performance of the computer based system. Planned or unplanned changes to computer based system components can have significant effects on the overall security of the computer based system. Accordingly, only qualified and authorized individuals should obtain the use of computer based system components for purposes of initiating changes, including upgrades and modifications.		
Example	Provides a function to separate system usage roles by duties and assign the minimum necessary authority to each job.  [Figure 31] Example of authorization settings menu		

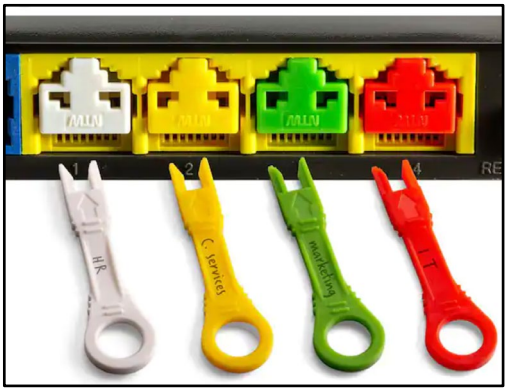
Objective	9. Wireless use control	Standard	IEC62443-3-3/SR2.2
Require-ments	The CBS shall provide the capability to authorize, monitor and enforce usage restrictions for wireless connectivity to the system according to commonly accepted security industry practices.		
Target	This requirement applies specifically when CBS uses wireless network communication.		

Explan-ation	Any wireless technology can, and in most cases should, be considered just another communication protocol option, and thus subject to the same CBS security requirements as any other communication type utilized by the CBS. However, a risk analysis may result in a requirement for wireless CBS components to support higher use control capabilities than are typically required of wired systems for the same use case and security level. Regulatory differences may also result in different required capabilities between wired and wireless communications.
Example	If the system includes a wireless network device, only authorized users should be able to access it. Additionally, the system should feature functionality to monitor the status of user's wireless network connections and impose restrictions as needed.  [Figure 32] Example of monitoring menu for wireless connection

Objective	10. Use control for portable and mobile devices	Standard	IEC62443-3-3/SR2.3
Require-ments	When the CBS supports use of portable and mobile devices, the system shall include the capability to a) Limit the use of portable and mobile devices only to those permitted by design b) Restrict code and data transfer to/from portable and mobile devices Note: Port limits / blockers (and silicone) could be accepted for a specific system		
Target	This requirement applies to all CBS. Unless portable and mobile devices are not used, it does not apply.		
Explan-ation	Portable and mobile devices may introduce undesired network traffic, malware and/or information exposure, so there should be specific control associated with their usage in the typical computer based system environment. Security policies and procedures may not		

	allow certain functions or activities via portable and/or mobile devices. Protecting information residing on portable and mobile devices (for example, employing cryptographic mechanisms to provide confidentiality and integrity protections during storage and while in transit when outside of controlled areas) is covered elsewhere.
Example	When supporting the use of portable and mobile devices such as laptops and USB, the system provides functions that are restricted to authorized devices only. If implementing this restriction digitally is not feasible, physical port restrictions and blockers. are provided instead.





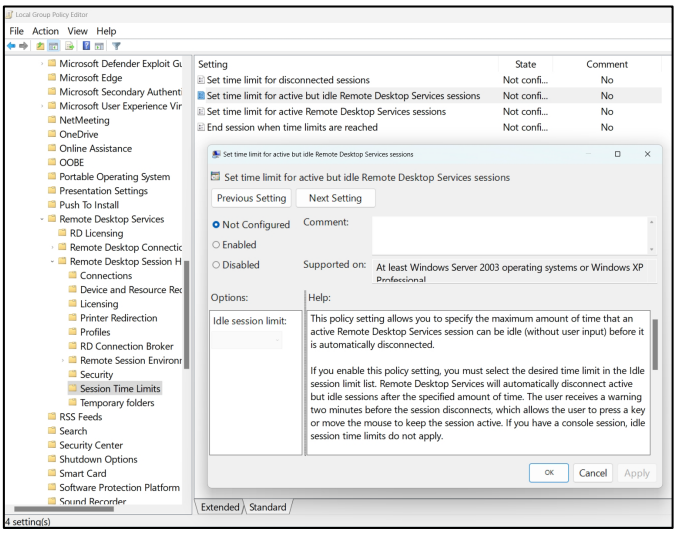
[Figure 33] Examples of controls for portable and mobile device

Objective	11. Mobile code	Standard	IEC62443-3-3/SR2.4
Require-ments	The CBS shall control the use of mobile code such as java scripts, ActiveX and PDF.		
Target	The requirements should be applied to all CBS.		

	If CBS does not have an operating system (OS) or is unable to access a web browser, this requirement may not apply. Instead, a detailed explanation of compensatory measures may be necessary.
Explan-ation	Mobile code technologies include, but are not limited to, Java, JavaScript, ActiveX, portable document format (PDF), Postscript, Shockwave movies, Flash animations and VBScript. Usage restrictions apply to both the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations. Control procedures should prevent the development, acquisition or introduction of unacceptable mobile code within the computer based system. For example, mobile code exchanges may be disallowed directly with the computer based system, but may be allowed in a controlled adjacent environment maintained by CBS personnel.
Example	When using mobile codes, functions to control usage are provided.

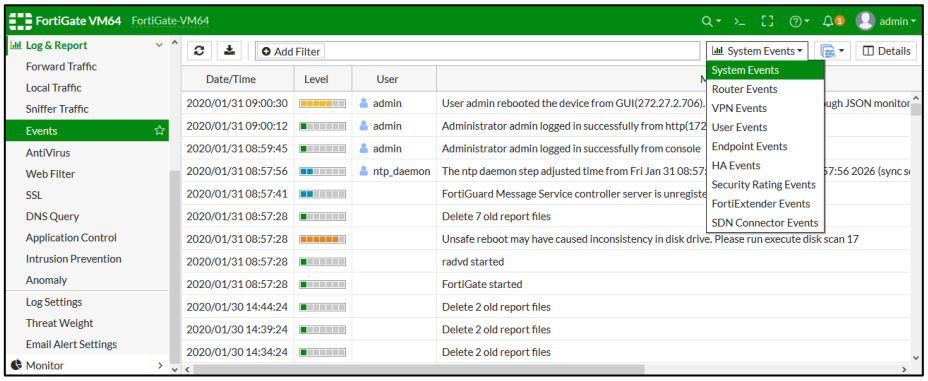
Objective	12. Session lock	Standard	IEC62443-3-3/SR2.5
Require-ments	The CBS shall be able to prevent further access after a configurable time of inactivity or following activation of manual session lock.		
Target	The requirement should be applied to all CBS. However, CBS requiring immediate operator response in emergencies may be exempted from this requirement.		
Explan-ation	The entity responsible for a computer based system should employ session lock to prevent access to specified workstations or nodes. The computer based system should activate session lock mechanisms automatically after a configurable time period for designated workstations or nodes. In some cases, session lock for computer based system operator workstations or nodes is not advised (for example, sessions which are required for immediate operator responses in emergency situations). Session locks are not a substitute for logging out of the computer based. In situations where the computer based cannot support session lock, the responsible entity should employ appropriate compensating countermeasures (for example, providing increased physical security, personnel security and auditing measures).		

Example	Provides a system session lock function triggered by a system inactivity for a specified period or manual user action. .



[Figure 34] Example of session lock function

Objective	13. Auditable events	Standard	IEC62443-3-3/SR2.8
Require-ments	The CBS shall generate audit records relevant to security for at least the following events: access control, operating system events, backup and restore events, configuration changes, and loss of communication.		
Target	The requirement should be applied to all CBS. Where implementation is not feasible, a detailed explanation of compensation measures may be required.		
Explan-ation	The purpose of this requirement is to record the occurrence of important events which need to be audited as significant and relevant to the security of the computer based system. Auditing activity can affect computer based system performance. The security audit function is usually coordinated with the network health and status monitoring function which may be in a different zone. Commonly recognized and accepted checklists and configuration guides should be considered when compiling a list of auditable events. The security policies and procedures should define auditable events that are adequate to support after-the-fact investigations of security incidents. In addition, audit records should be sufficient to monitor the effectiveness and proper operation of the security mechanisms utilized to meet the requirements in this standard. It should be noted that the requirement for event recording is applicable within the given system functionality, specifically given system security requirements on a given level. Events may occur in any computer based system component (for example login events) or may be observed by dedicated monitors. For example, port scanning might be detected by an intrusion detection system (IDS) or intrusion prevention system (IPS).		
Example	The system provides the ability of generating security-related audit records that include, at a minimum: - Access control (e.g. success/failure of log in, log out) - Operating system events (e.g. reboot, shutdown) - Backup and recovery incidents - Configuration changes (e.g. permission changes, alarm value settings changes, system changes settings defined by the manufacturer) - Loss of communication (e.g. records when internal and external communication connection fails)		



[Figure 35] Example of security audit log

Objective	14. Audit storage capacity	Standard	IEC62443-3-3/SR2.9
Require-ments	The CBS shall provide the capability to allocate audit record storage capacity according to commonly recognized recommendations for log management. Auditing mechanisms shall be implemented to reduce the likelihood of such capacity being exceeded.		
Target	The requirement should be applied to all CBS. Where implementation is not feasible, a detailed explanation of compensation measures may be required.		
Explan-ation	The computer based system should provide sufficient audit storage capacity, taking into account retention policy, the auditing to be performed and the online audit processing requirements. The audit storage capacity should be sufficient to retain logs for a period of time required by applicable policies and regulations or business requirements.		
Example	This requirement provides the function to allocate storage space specifically security-related audit records.. This function monitors the usage of allocated space, triggering an alarm when it exceeds a predefined threshold, such as 80%, and 90%, thereby notifying the user. It also includes functions to manage space usage by deleting old records or preventing the saving of new records.		

Objective	15. Response to audit processing failures	Standard	IEC62443-3-3/SR2.10
Require-ments	The CBS shall provide the capability to prevent loss of essential services and functions in the event of an audit processing failure.		
Target	The requirement should be applied to all CBS. Where implementation is not feasible, a detailed explanation of compensation measures may be required		
Explan-ation	Audit generation typically occurs at the source of the event. Audit processing involves transmission, possible augmentation (such as the addition of a timestamp) and persistent storage of the audit records. Audit processing failures include, for example, software or hardware errors, failures in the audit capturing mechanisms and audit storage capacity being reached or exceeded. It should be noted that either overwriting the oldest audit records or halting audit log generation are possible responses to audit storage capacity being exceeded but imply the loss of potentially essential forensic information.		
Example	The systems provides a function to allocate space for security-related audit records. It monitors allocated space usage, triggers alarms when nearing predefined thresholds, such as. 80% and 90%, notifies users, and offers functions such as deleting old records or preventing the saving of new records when necessary.		

Objective	16. Timestamps	Standard	IEC62443-3-3/SR2.11
Require-ments	The CBS shall timestamp audit records.		
Target	The requirement should be applied to all CBS. Where implementation is not feasible, a detailed explanation of compensation measures may be required.		
Explan-ation	Timestamps (including date and time) of audit records should be generated using internal system clocks. If system-wide time synchronization is not present (which is typical in many installations), known offsets would be needed to support analysis of a sequence of events. In addition, synchronization of internally generated audit records with external events might require synchronization with a generally recognized external time source (such as the Global Positioning System (GPS), Global Navigation Satellite System (GLONASS) and Galileo). The time source should be protected from unauthorized alteration.		
Example	Include the time and timestamp for each event in security-related audit records.		

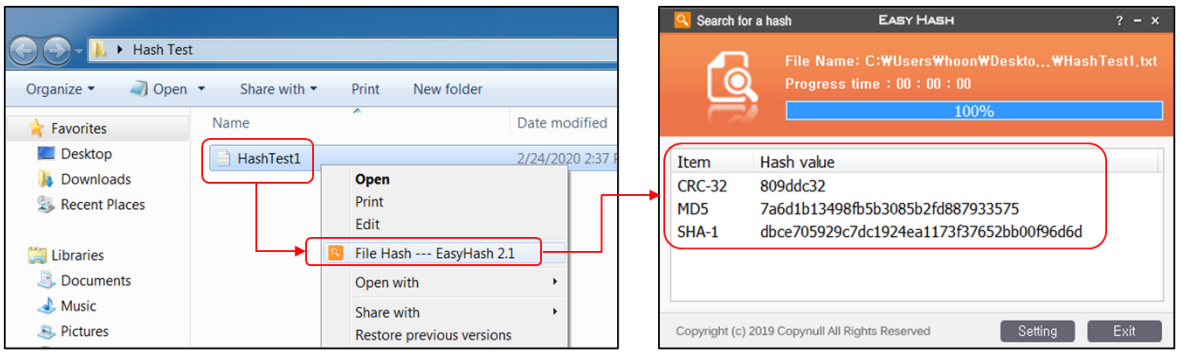
Objective	23. Audit log accessibility	Standard	IEC62443-3-3/SR6.1
Require-ments	The CBS shall provide the capability for accessing audit logs on read only basis by authorized humans and/or tools.		
Target	The requirement should be applied to all CBS. Where implementation is not feasible, a detailed explanation of compensation measures may be required.		
Explan-ation	The computer based system generates audit records about events occurring in the system. Access to these audit logs is necessary to support filtering audit logs, identifying and removing information that is redundant, reviewing and reporting activity during after-the-fact investigations of security incidents. This access should not alter the original audit records. In general, audit reduction and report generation should be performed on a separate information system. Manual access to the audit records (such as screen views or printouts) is sufficient for meeting the base requirement, but is insufficient for higher SLs. Programmatic access is commonly used to provide the audit log information to analysis mechanisms such as SIEM.		
Example	Users have read-only access to security-related audit records which are not allowed to modify and delete.		

3. Confidentiality and integrity

(1) Understanding security functional requirements

Security aims to protect information through three (3) essential elements: Confidentiality, Integrity, and Availability.

Confidentiality ensures that information is restricted from unauthorized access and disclosure. Encrypting a specific file with a password restricts access to authorized individuals who possess



[Figure 36] Example of hash value check with commercial tools

the correct password and decryption key. This method safeguards the confidentiality of the information within.

Integrity involves maintaining the accuracy and completeness of data and assets. If malicious code alters an executable file or physical damage corrupts a storage disk, the executable file's integrity is compromised. Tasks related to maintaining integrity often require understanding encryption techniques.

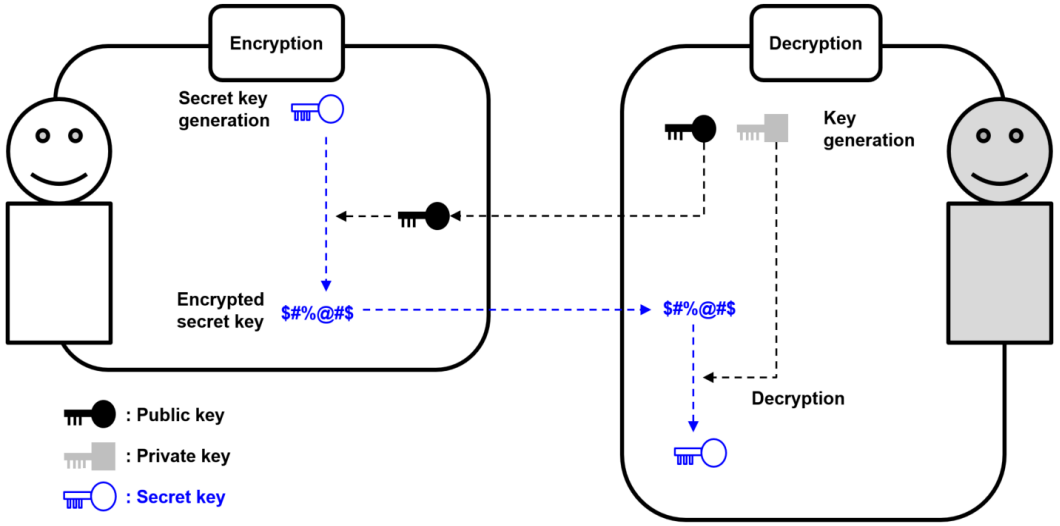
Hash functions are essential one-way encryption techniques that map data of arbitrary length, such as a file, to fixed-length bit string. The output of this mapping process is referred to as a hash value, which is generated using various encryption algorithms. [Figure 36] demonstrates obtaining the hash value of a sample text file using a commercial tool. Standard hash algorithms include CRC-32, MD5, and SHA-1.

The hash functions possess several primary characteristics:

1) They always produce a hash value of a fixed length[12]
2) The same input value consistently yields the same hash value.
3) The input value cannot be inferred from the output hash value(one-way)

Data integrity can be verified by ensuring that the same input consistently produces the same hash value. For instance, when transmitting and installing an update file, the sender includes a hash value to verify its integrity and confirming that it is undamaged. The recipient calculates the hash value of the received update file using the same encryption algorithm, compares it with the sender's hash value and validates the file's integrity if they match. This process ensures that the file has not been altered, thereby maintaining data integrity.

[12] The length of the hash value may vary depending on the encryption algorithm. However, when the same encryption algorithm is used, it consistently outputs a hash value of the same length.



[Figure 37] Example of symmetric key sharing method using asymmetric key encryption

Encryption is crucial for protecting confidentiality. Symmetric key and asymmetric key encryption are two-way encryption methods that enable both encryption and decryption of data. Unlike one-way encryption, which only allows for encryption and cannot be decrypted, two-way encryption supports both processes.

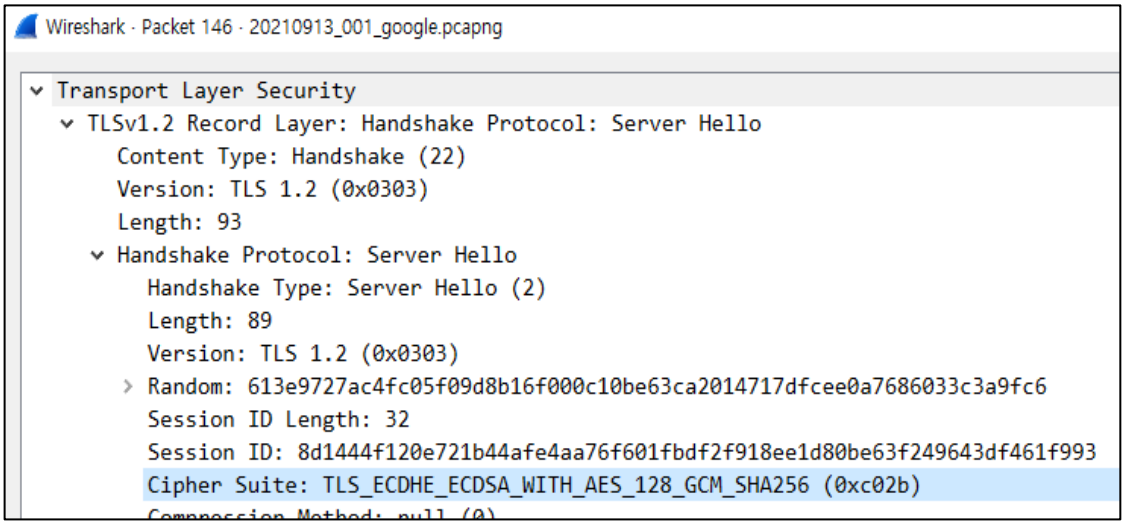
In symmetric key encryption, the same key, known as the secret key, is used for both encryption and decryption. Conversely, asymmetric key encryption uses a public key for encryption and a private key for decryption. Symmetric key encryption often uses shorter keys to provide the same level of security and operates faster. Consequently, symmetric key encryption is commonly employed to encrypt actual communication data. However, in this scenario, each user must possess a secret key for encryption and decryption.

When a user connects to a server for the first time, a secure method is needed to exchange the key generated by one party with the other. An asymmetric key encryption algorithm is implemented to share the symmetric key securely.

In asymmetric key system, which consists of a public key and a private key, different keys are used for encryption and decryption. The encryption key cannot decrypt data, and conversely, the decryption key cannot encrypt data. [Figure 37] demonstrates sharing the symmetric key, also known as the secret key, using asymmetric key encryption. To initiate key sharing, one party generates a pair of public and private keys

Security Strength		Through 2030	2031 and Beyond
< 112	Applying protection	Disallowed	
	Processing	Legacy-use*	
112	Applying protection	Acceptable	Disallowed
	Processing		Legacy use
128	Applying protection and processing information that is already protected	Acceptable	Acceptable
192		Acceptable	Acceptable
256		Acceptable	Acceptable

[Figure 38] NIST SP 800-57, Recommended security strength



[Figure 39] Example TLS communication packet

and shares the public key with the other party. The party intending to share the symmetric key then encrypts it with the recipient's public key and sends it over. Upon receipt, the encrypted symmetric key is decrypted using the recipient's private key, ensuring the secure exchange of the symmetric key, also known as the secret key. The data exposed externally in this process includes the public key and the encrypted data, while the private key remains protected and is not exposed. Due to the nature of asymmetric key encryption, the private key cannot be derived from the public key. Secure sharing necessitates strict protection of the private key from unauthorized access. Consequently, the Security Development Life Cycle (SDLC) document mandates procedures and technical controls to protect the private keys used in code signing.

The Transport Layer Security (TLS) protocol exemplifies secure communication using a combination of asymmetric and symmetric key encryption. TLS protocol ensures secure tranmission by encrypting data. [Figure 39] illustrates the usage of TLS for communication data packets. Within TLS, a cipher suite consists of several encryption algorithms. For instance, ECDHE facilitates asymmetric key encryption for secure key exchange, while AES 128 employs symmetric key encryption for encrypting the actual communication data. SHA 256 is used as the hash function encryption alogorithm to ensure integrity verification.

From a security perspective, new threats constantly emerge, and hacking techniques evolve alongside advancements in security technologies. NIST[13] outlines security strength in NIST SP 800-57, recommending security levels based on different time periods.

[13] NIST : National Institute of Standards and Technology

Security strength is measured in bit units, where n bits indicate that 2n operations are required to compromise the encryption algorithm. According to NIST, the recommended security strength is 112 bits or higher until 2030, increasing to 128 bits or higher thereafter.

Table 2: Comparable security strengths of symmetric block cipher and asymmetric-key algorithms

Security Strength	Symmetric Key Algorithms	FFC (DSA, DH, MQV)	IFC* (RSA)	ECC* (ECDSA, EdDSA, DH, MQV)
≤ 80	2TDEA	$L = 1024$ $N = 160$	$k = 1024$	$f = 160\text{-}223$
112	3TDEA[68]	$L = 2048$ $N = 224$	$k = 2048$	$f = 224\text{-}255$
128	AES-128	$L = 3072$ $N = 256$	$k = 3072$	$f = 256\text{-}383$
192	AES-192	$L = 7680$ $N = 384$	$k = 7680$	$f = 384\text{-}511$

[Figure 40] NIST SP 800-57, Security strength table

Given that security strength is a conceptual metric, verifying the actual strength of the encryption algorithm in use is necessary. NIST SP 800-57 provides a mapping of security strength to each algorithm's key length, as detailed in [Figure 40],comparing security strength across different encryption algorithm and key lengths. For instance, the RSA encryption algorithm with a 2048-bit key has a security strength of 128 bits.

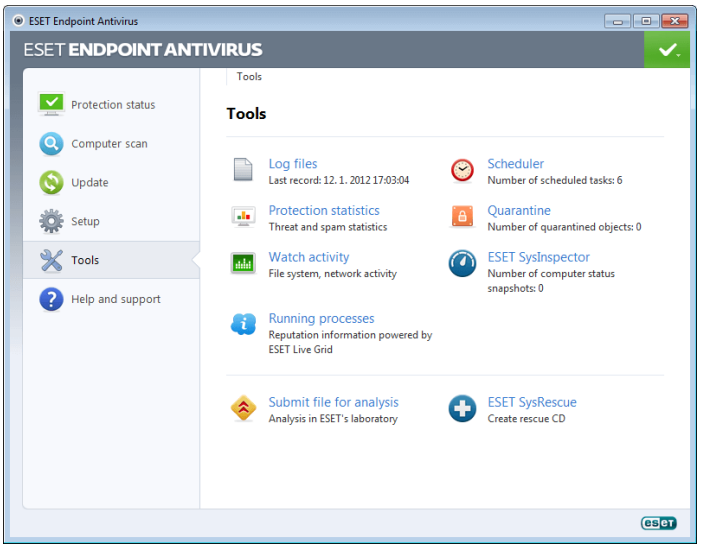
According to [Figure 38], the recommended security strength by 2030 is 112 bits. RSA 2048 can be considered a suitable choice for encryption algorithms according to this recommendation.

(2) Security functional requirements explanation and examples

Objective	17. Communication integrity	Standard	IEC62443-3-3/SR3.1
Require-ments	The CBS shall protect the integrity of transmitted information. Note: Cryptographic mechanisms shall be employed for wireless networks.		
Target	This requirement applies to all CBSs interconnected within a network, except for serial communication environments such as RS422/485.		
Explan-ation	Many common network attacks are based on the manipulation of data in transmission, for example manipulation of network packets. Switched or routed networks provide a greater opportunity for attackers to manipulate packets as undetected access to these networks is generally easier and the switching and routing mechanisms themselves can also be manipulated in order to get more access to transmitted information. Manipulation in the context of a computer based system could include the change of measurement values communicated from a sensor to a receiver or the alteration of command parameters sent from a control application to an actuator. Depending on the context (for example transmission within a local network segment versus transmission via untrusted networks) and the network type used in the transmission (for example transmission control protocol		

	(TCP) / internet protocol (IP) versus local serial links), feasible and appropriate mechanisms will vary. On a small network with direct links (point-to-point), physical access protection to all nodes may be sufficient on lower SLs if the endpoints' integrity is protected as well, while on a network distributed in areas with regular physical presence of staff or on a wide area network physical access is likely not enforceable. If a commercial service is used to provide communication services as a commodity item rather than a fully dedicated service (for example a leased line versus a T1 link), it may be more difficult to obtain the necessary assurances regarding the implementation of needed security controls for communication integrity. When it is infeasible or impractical to meet the necessary security requirements it may be appropriate to implement either appropriate compensating countermeasures or explicitly accept the additional risk. Industrial equipment is often subject to environmental conditions that can lead to integrity issues and/or false positive incidents. Many times the environment contains particulates, liquids, vibration, gases, radiation, and electromagnetic interference (EMI) that can cause conditions that affect the integrity of the communication wiring and signals. The network infrastructure should be designed to minimize these physical/environmental effects on communication integrity. For example, when particulate, liquids, and/or gases are an issue, it may be necessary to use a sealed registered jack 45 (RJ-45) or M12 connector instead of a commercial-grade RJ-45 connector on the wire. The cable itself may need to use a different jacket instead to handle the particulate, liquid, and/or gas as well. In cases where vibration is an issue, M12 connectors may be necessary to prevent the spring pins on an RJ-45 connector from disconnecting during use. In cases where radiation and/or EMI are an issue, it may be necessary to use shielded twisted pair or fiber cables to prevent any effect on the communication signals. It may also be necessary to perform a wireless spectrum analysis in these areas if wireless networking is planned to verify that it is a viable solution
Example	Implement communication protocols that incorporate integrity protection functions to ensure the integrity of transmitted data

Objective	18. Malicious code protection	Standard	IEC62443-3-3/SR3.2
Require-ments	The CBS shall provide capability to implement suitable protection measures to prevent, detect and mitigate the effects due to malicious code or unauthorized software. It shall have the feature for updating the protection mechanisms		
Target	The requirement applies to CBS using a general operating system (OS), such as Windows, Android.		
Explan-ation	The computer based system should use protection mechanisms to prevent, detect, mitigate and report instances of detected malicious code (for example, viruses, worms, Trojan horses and spyware) transported by electronic mail, electronic mail attachments, Internet access, removable media (for example, universal serial bus (USB) devices, diskettes or compact disks), PDF documents, web services, network connections and infected laptops or other common means.		

	Detection mechanisms should be able to detect integrity violations of application binaries and data files. Techniques may include, but are not limited to, binary integrity and attributes monitoring, hashing and signature techniques. Mitigation techniques may include, but are not limited to, file cleaning, quarantining, file deletion, host communication restriction and IPSs. Prevention techniques may include, but are not limited to, application blacklisting and whitelisting techniques, removable media control, sandbox techniques and specific computing platforms mechanisms such as restricted firmware update capabilities, No Execute (NX) bit, data execution prevention (DEP), address space layout randomization (ASLR), stack corruption detection and mandatory access controls.
Example	Install an anti-virus program or implement a solution to prevent malicious code.  [Figure 41] Example of antivirus program

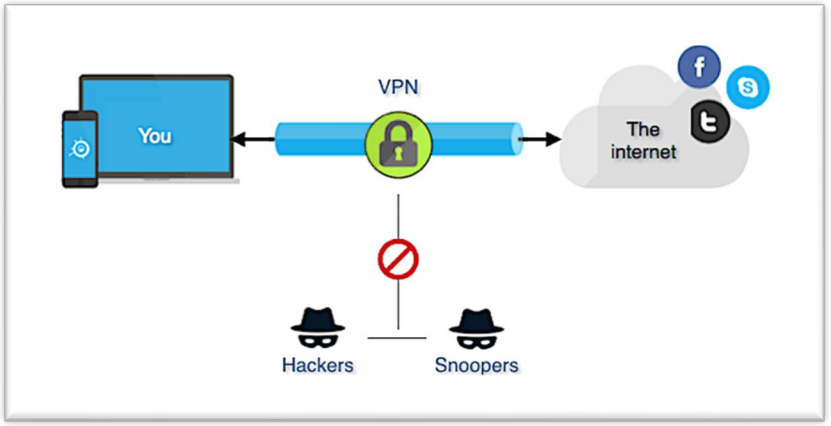
Objective	19. Security functionality verification	Standard	IEC62443-3-3/SR3.3
Require-ments	The CBS shall provide the capability to support verification of the intended operation of security functions and report when anomalies occur during maintenance		
Target	The requirement should be applied to all CBS. Where implementation is not feasible, a detailed explanation of compensation measures may be required.		
Explan-ation	The product supplier and/or system integrator should provide guidance on how to test the designed security controls. Asset owners need to be aware of the possible ramifications of running these verification tests during normal operations. Details of the execution of these verifications need to be specified with careful consideration of the requirements for continuous operations (for example, scheduling or prior notification). Examples of security verification functions include:		

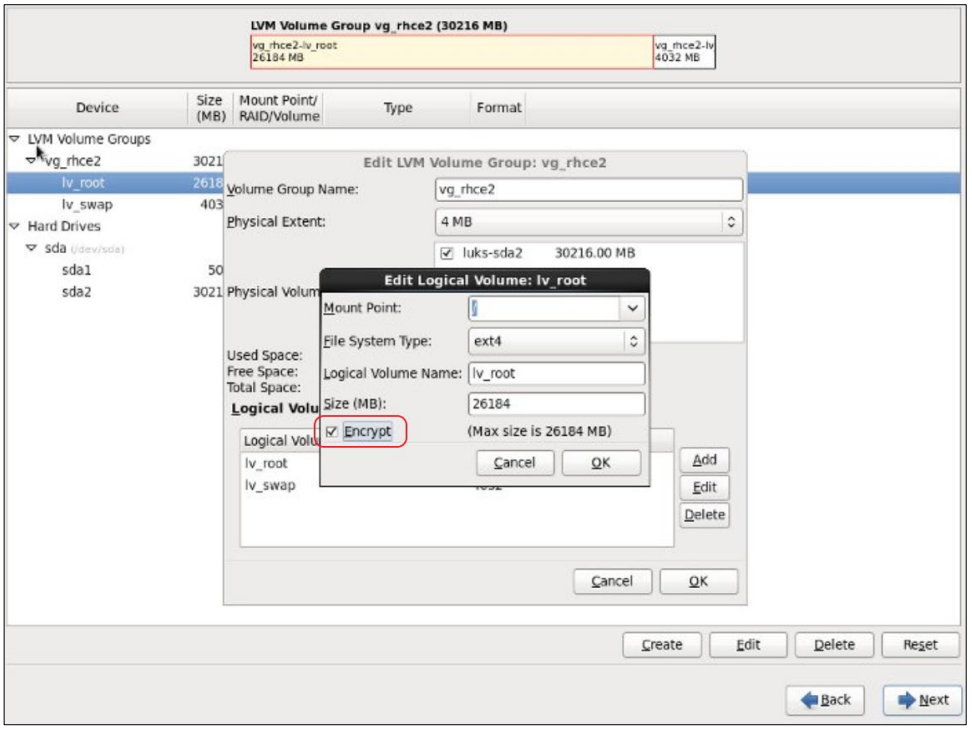
	- Verification of antivirus measures by European Institute for Computer Antivirus Research (EICAR) testing of the computer based system file system. Antivirus software should detect this and appropriate incident handling procedures should be triggered. - Verification of the identification, authentication and use control measures by attempting access with an unauthorized account (for some functionality this could be automated). - Verification of IDSs as a security control by including a rule in the IDS that triggers on irregular, but known non-malicious traffic. The test could then be performed by introducing traffic that triggers this rule and the appropriate IDS monitoring and incident handling procedures. - Confirmation that audit logging is occurring as required by security policies and procedures and has not been disabled by an internal or external entity.
Example	It provides a security function verification function. For instance, refer to the following. Create a document guiding how to do this and submit it as a reference document, 'CBS Maintenance and Verification Plan': - Verification of anti-virus vaccine function using EICAR test file - Record login failures due to unauthorized accounts and ensure audit logging. - If IPS/IDS is provided, generate abnormal traffic according to policy and verify detection. - Confirm audit records are generated as per manufacturer-defined conditions and are non-modified by the user.

Objective	20. Deterministic output	Standard	IEC62443-3-3/SR3.6
Require-ments	The CBS shall provide the capability to set outputs to a predetermined state if normal operation cannot be maintained as a result of an attack. The predetermined state could be: - Unpowered state, - Last-known value, or - Fixed value		
Target	The requirement should be applied to all CBS. Where implementation is not feasible, a detailed explanation of compensation measures may be required.		
Explan-ation	The deterministic behavior of computer based system outputs as a result of threat actions against the computer based system is an important characteristic to ensure the integrity of normal operations. Ideally, the computer based system continues to operate normally while under attack, but if the computer based system cannot maintain normal operation, then the computer based system outputs need to fail to a predetermined state. The appropriate predetermined state of computer based system outputs is application dependent and could be one of the following user configurable options: - Unpowered : the outputs fail to the unpowered state - Hold : the outputs fail to the last-known good value - Fixed : the outputs fail to a fixed value that is determined by the asset owner or an application		

Example	In the event of a system malfunction, a function is provided to set the operating state of a predefined output, minimizing the impact of system failure and ensure safety.

Objective	21. Information confidentiality	Standard	IEC62443-3-3/SR4.1
Require-ments	The CBS shall provide the capability to protect the confidentiality of information for which explicit read authorization is supported, whether at rest or in transit. Note: For wireless network, cryptographic mechanisms shall be employed to protect confidentiality of all information in transit.		
Target	The requirement applies to all CBSs connected within in a network, except for serial communication environments such as RS422/485.		
Explan-ation	Protection of information, at rest or in transit, can be maintained through physical means, compartmentalization or encryption, among other techniques. It is crucial that the technique chosen considers the potential ramifications on computer based system performance and the capability to recover from system failure or attack. The decision whether the confidentiality of a given piece of information should be protected or not depends on the context and cannot be made at product design. However, the fact that an organization limits access to information by configuring explicit read authorizations in the computer based system is an indicator that this information is considered confidential by the organization. Thus, all information for which the computer based system supports the capability to assign explicit read authorizations should be considered potentially confidential and thus the computer based system should also provide the capability to protect it. In some situations network configuration information stored and processed in switches and routers may be considered as confidential. Communications involving exposed information transfer may be vulnerable to eavesdropping or tampering. If the computer based system is depending upon an external communications service provider, it may be more difficult to obtain the necessary assurances regarding the implementation of needed security requirements for communication confidentiality. In such cases, it may be appropriate to implement compensating countermeasures or explicitly accept the additional risk. Entities should also be cognizant of information confidentiality when portable and mobile devices are utilized (for example, engineering laptops and USB sticks).		
Example	Provides encryption functions or tools to protect the confidentiality of stored data and communication data: - Examples of storage data encryption: BitLocker, Encrypting File System (EFS), LUKS (Linux Unified Key Setup-on-disk-format). - Examples of communication data encryptions: TLS protocol, VPN (Virtual Private Network).		





[Figure 42] Example of storage and communication data encryption

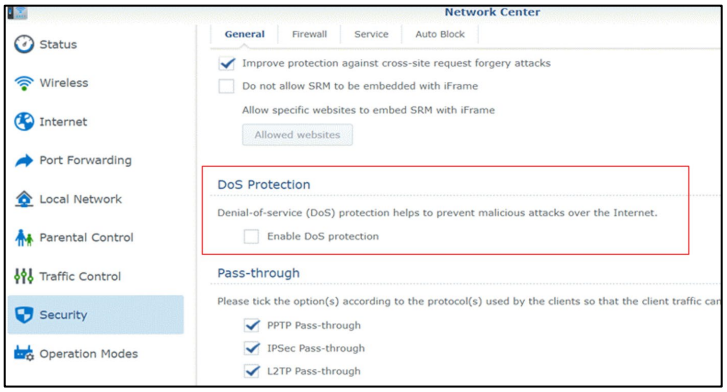
Objective	22. Use of cryptography	Standard	IEC62443-3-3/SR4.3
Require-ments	If cryptography is used, the CBS shall use cryptographic algorithms, key sizes and mechanisms according to commonly accepted security industry practices and recommendations.		
Target	The requirement applies to all CBSs interconnected within a network, except for serial communication environments such as RS422/485.		
Explan-ation	The selection of cryptographic protection should match the value of the information being protected, the consequences of the confidentiality of the information being breached, the		

	time period during which the information is confidential and computer based system operating constraints. This can involve either information at rest, in transit, or both. Note that backups are an example of information at rest, and should be considered as part of a data confidentiality assessment process. The computer based system product supplier should document the practices and procedures relating to cryptographic key establishment and management. The computer based system should utilize established and tested encryption and hash algorithms, such as the advanced encryption standard (AES) and the secure hash algorithm (SHA) series, and key sizes based on an assigned standard. Key generation needs to be performed using an effective random number generator. The security policies and procedures for key management need to address periodic key changes, key destruction, key distribution and encryption key backup in accordance with defined standards. Generally accepted practices and recommendations can be found in documents such as NIST SP800-57. Implementation requirements can be found for example in ISO/IEC 19790.
Example	Using encryption algorithms with a security strength of 112 bit or higher is recommended.

4. Availability

(1) Understanding security functional requirements

Availability refers to ensuring timely and reliable access to and use of system information and functions. This section explains the security function requirements from various perspectives, including network, power, and data, to ensure users can access system functions without issues when needed. A Denial of Service (DoS) attack generates excessive traffic that surpasses the capacity of devices like servers, preventing legitimate users from accessing services. Generally, users connect to a server and to receive various services. However, the data and its traffic a server can manage simultaneously is limited. Malicious users can send excessive data requests, hindering legitimate users from receiving proper services. System must incorporate DoS protection functions to guard against such attacks, which are generally provided by network devices. [Figure 43] illustrates an example of a DoS protection function screen provided by a network device.

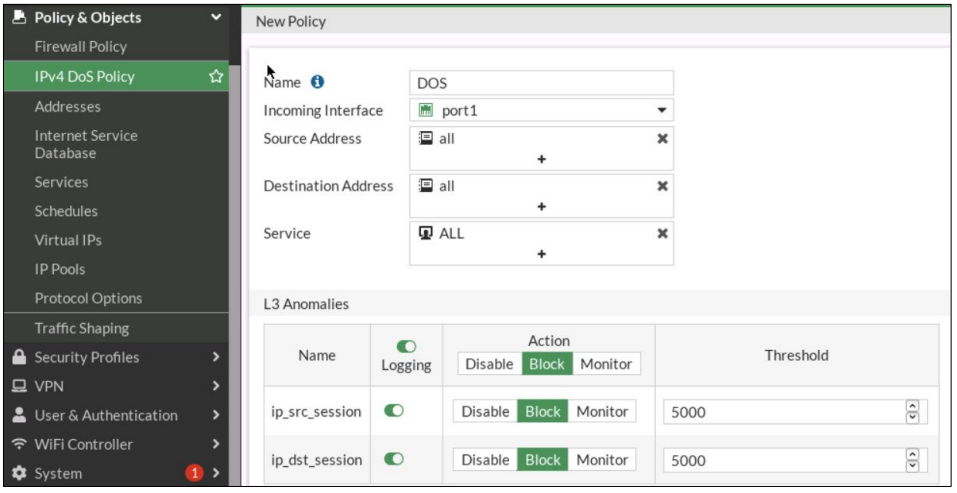


[Figure 43] Example of DoS protection function

Backup functions should enable recovery from system failures or incorrect settings without affecting the system's regular operation. The system should be capable of switching to or receiving power from an emergency power supply. Ensuring a reliable power source involves setting up an Uninterruptible Power Supply (UPS). If a UPS is not available, the system should automatically boot and become operational immediately when power is restored after an outage and blackout. All software applications required for system operation should run automatically upon reboot. Additionally, configuration functions for system security, including user accounts, permissions, passwords, recommended settings, and firewall policies, should be provided. These functions should be documented and be submitted as security setting instructions for reference.

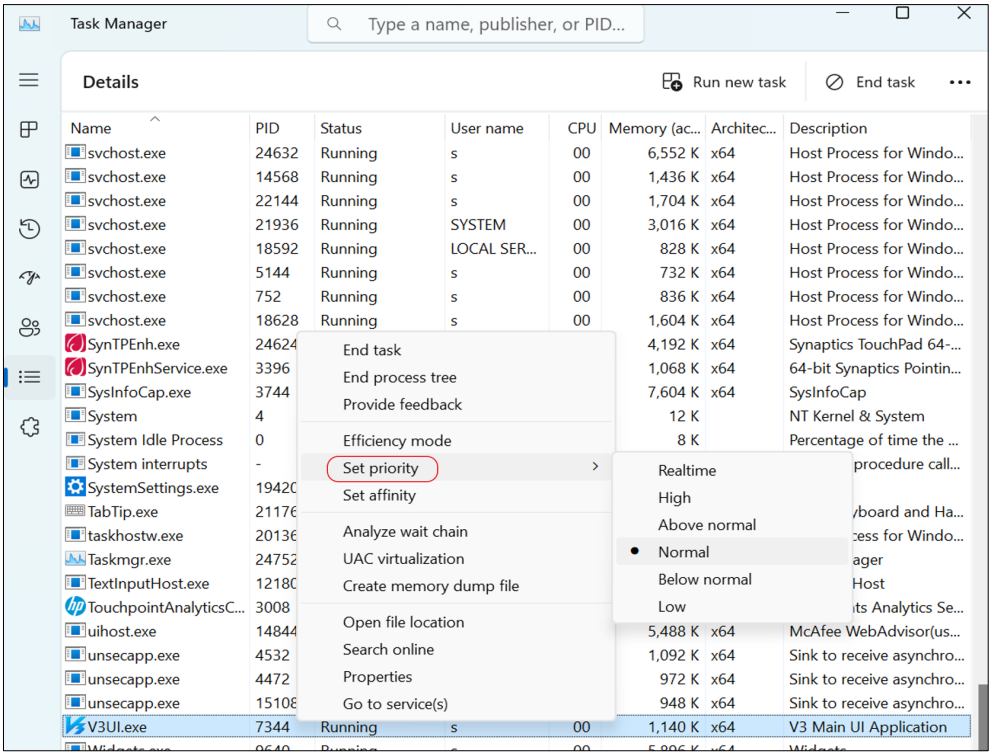
(2) Security functional requirements explanation and examples

Objective	24. Denial of service protection	Standard	IEC62443-3-3/SR7.1
Require-ments	The CBS shall provide the minimum capability to maintain essential functions during DoS events. Note: It is acceptable that the CBS may operate in a degraded mode upon DoS events, but it shall not fail in a manner which may cause hazardous situations. Overload-based DoS		

	events should be considered, i.e. where the networks capacity is attempted flooded, and where the resources of a computer is attempted consumed.
Target	The requirement should be applied to all CBS. Where implementation is not feasible, a detailed explanation of compensation measures may be required.
Explan-ation	A variety of technologies exist to limit, or in some cases, eliminate the effects of DoS situations. For example, boundary protection devices can filter certain types of packets to protect devices on an internal, trusted network from being directly affected by DoS events or restricting the information flow to be unidirectional outbound. Specifically, a DoS event on the computer-based system should not adversely impact any safety-related systems.
Example	A network device should provide functions to protect against DoS conditions, including network overload and DoS attacks.  [Figure 44] Example of firewall DoS protection policy settings screen <source : Fortinet>

Objective	25. Resource management	Standard	IEC62443-3-3/SR7.2
Require-ments	The CBS shall provide the capability to limit the use of resources by security functions to prevent resource exhaustion.		
Target	The requirements apply to CBS with security function software installed, for instance, when “18. Malicious code protection” requirement apply.		
Explan-ation	Resource management (for example, network segmentation or priority schemes) prevents a lower-priority software process from delaying or interfering with the computer based system servicing any higher-priority software process. For example, initiating network scans, patching and/or antivirus checks on an operating system can cause severe disruption to normal operations. Traffic rate limiting schemes should be considered as a mitigation technique.		
Example	The system should include a function that distinguishes between essential functions and security functions, ensuring that the resource use of essential functions takes precedence		

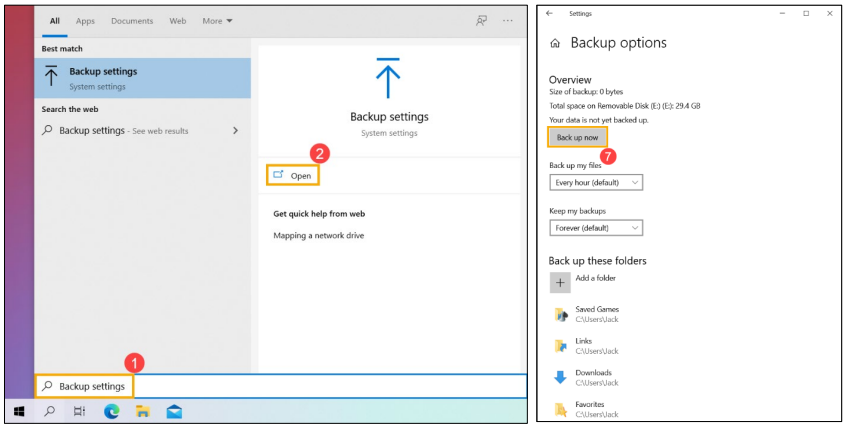
	over security functions. For instance, this can be achieved by providing a resource priority allocation function for each software in the operating system, and similar functions.



[Figure 45] Example of resource management

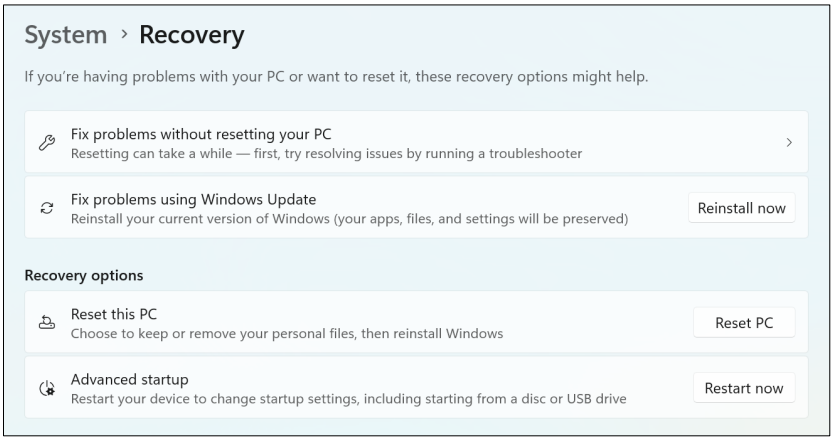
Objective	26. System backup	Standard	IEC62443-3-3/SR7.3
Require-ments	The identity and location of critical files and the ability to conduct backups of user-level and system-level information (including system state information) shall be supported by the CBS without affecting normal operations		
Target	The requirement should be applied to all CBS. Where implementation is not feasible, it may not apply to embedded systems composed of firmware and similar components.		
Explan-ation	The availability of up-to-date backups is essential for recovery from a computer based system failure and/or mis-configuration. Automating this function ensures that all required files are captured, reducing operator overhead. Although not usually required for computer based system recovery, information required for post-incident forensic activity should be specifically included in the backup. If the resulting backups contain confidential information, encryption should be considered.		

Example	Provides backup functionality for the system while ensuring that essential functions operate normally during the backup process.



[Figure 46] Example of backup

Objective	27. System recovery and reconstitution	Standard	IEC62443-3-3/SR7.4
Require-ments	The CBS shall provide the capability to be recovered and reconstituted to a known secure state after a disruption or failure.		
Target	The requirement should be applied to all CBS. Where implementation is not feasible, it may not apply to embedded systems composed of firmware or similar components.		
Explan-ation	Computer based system recovery and reconstitution to a known secure state means that all system parameters (either default or configurable) are set to secure values, security-critical patches are reinstalled, security-related configuration settings are reestablished, system documentation and operating procedures are available, application and system software is reinstalled and configured with secure settings, information from the most recent, known secure backups is loaded and the system is fully tested and functional.		
Example	Provides recovery functions for the system		



[Figure 47] Example of recovery

Objective	28. Alternative power source	Standard	IEC62443-3-3/SR7.5
Require-ments	The CBS shall provide the capability to switch to and from an alternative power source without affecting the existing security state or a documented degraded mode.		
Target	The requirement should be applied to all CBS. Where implementation is not feasible, a detailed explanation of compensation measures may be required.		
Explan-ation	There may be instances where compensating countermeasures such as physical door access control may be affected by loss of base power supply, in which case the emergency power supply should cover those associated systems. If this is not possible, other compensating countermeasures may be needed during such an emergency situation.		
Example	It does not affect external equipment that supplies UPS or is controlled during a blackout. It provides functions such as automatically restarting the system and making it usable by the user after blackout recovery.		

Objective	29. Network and security configuration settings	Standard	IEC62443-3-3/SR7.6
Require-ments	The CBS traffic shall provide the capability to be configured according to recommended network and security configurations as described in guidelines provided by the supplier. The CBS shall provide an interface to the currently deployed network and security configuration settings.		
Target	The requirement should be applied to all CBS. Where implementation is not feasible, a detailed explanation of compensation measures may be required.		
Explan-ation	These configuration settings are the adjustable parameters of the computer-based system components. In order to be able to detect and correct any deviations from the approved and/or recommended configuration settings, the computer-based system needs to support monitoring and control of changes to the configuration settings in accordance with security policies and procedures. For enhanced security, an automated check may be performed where the current settings are automatically collected by an agent and compared to approved settings.		
Example	Examples of security configuration settings include: - User accounts - Authorization - Password policies - Recommended product safety settings - Firewall policy, if available		

Objective	30. Least Functionality	Standard	IEC62443-3-3/SR7.7

Require-ments	The installation, the availability and the access rights of the following shall be limited to the strict needs of the functions provided by the CBS: - operating systems software components, processes and services - network services, ports, protocols, routes and hosts accesses and any software
Target	The requirement should be applied to all CBS. Where implementation is not feasible, a detailed explanation of compensation measures may be required.
Explan-ation	Computer based systems are capable of providing a wide variety of functions and services. Some of the functions and services provided may not be necessary to support essential functions. Therefore, by default, functions beyond a baseline configuration should be disabled. Additionally, it is sometimes convenient to provide multiple services from a single component of a computer-based system, but doing so increases risk over limiting the services provided by any one component. Many functions and services commonly provided by commercial-off-the-shelf (COTS) equipment may be candidates for elimination, for example, email, voice over internet protocol (VoIP), instant messaging (IM), file transfer protocol (FTP), hypertext transfer protocol (HTTP) and file sharing.FA
Example	Provides a function to restrict access to the operating system and other S/W applications provided by the system. Ensures that access is restricted to only authorized users and accounts.

Section 3 . Additional security capabilities explanation and example

1. Additional security capabilities

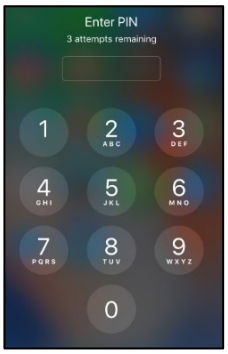
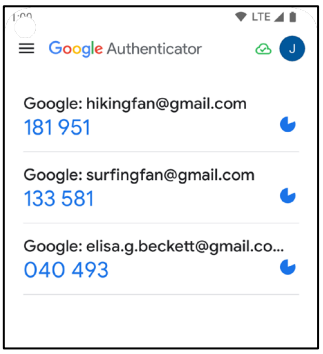
(1) Understanding additional security functional requirements

If the system has a remote connection to an untrusted network, it should implement the thirty (30) mandatory security capability requirements according to Chapter 3, Clause 401. of Guidance for Cyber Resilience, along with eleven (11) additional security capability requirements from Clause 402.

When connecting to an untrusted network, which refers to a network not covered by Guidance for Cyber Resilience, the system should also provide several functions. First, a multifactor authentication function is required. Multifactor authentication must use two or more authentication methods, with different factors for each method. The three (3) types of factors are knowledge-based, possession-based, and inherence-bases . Knowledge-based factors refer to information only the user knows, such as passwords or PIN codes. Possession-based factors involve physical items owned by the user, such as security cards and OTPs. Inherence-based factors refer to unique attributes of the user, such as fingerprint or iris recognition. Secondly, in addition to human users, software processes and devices should be identified and authenticated. Thirdly, the system should limit failed login attempts. For instance, if a user exceeds a predefined number of failed login attempts, they should be prevented from logging in for a specified period. Fourth, the system should display a notification message before user authentication. According to IEC 62443 3-3 SR 1.12, the message should include:.

1) Notification that the individual is accessing a specific computer-based system.
2) Information that system usage may be monitored, recorded and subject to audit.
3) A warning that unauthorized use is prohibited and subject to criminal and/or civil penalties
4) Notice that use of the system indicates consent to monitoring and recording.

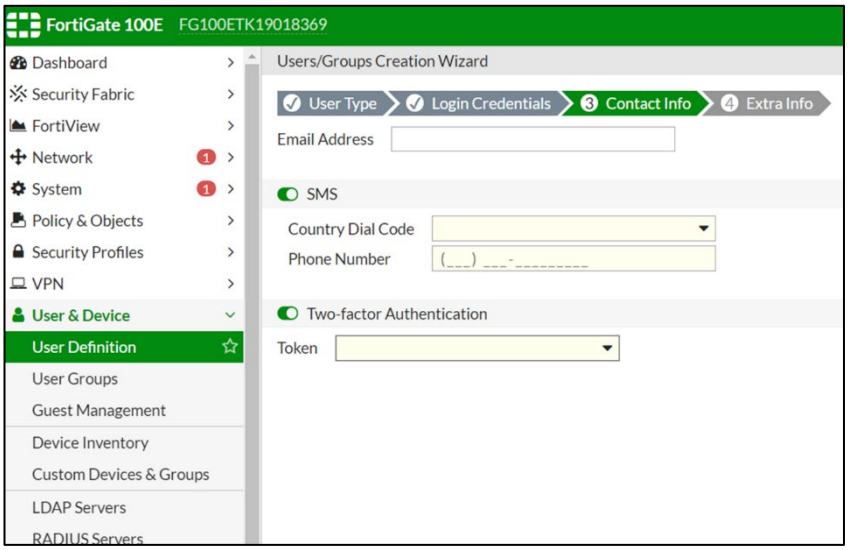
The user notification feature should also allow authorized personnel to modify settings, including relevant text. Lastly, when accessing from an untrusted network, system access should be allowed only after approval from authorized personnel on board.

		
Knowledge based factors	Possession based factors	Inherence based factors

[Figure 48] Example of multifactor authentication

(2) Explanation and examples of security functional requirements

Objective	31. Multifactor authentication for human users	Standard	IEC62443-3-3/SR1.1, RE2
Require-ments	Multifactor authentication is required for human users when accessing the CBS from or via an untrusted network.		
Example	Provides the ability to force multifactor authentication when connecting human users through an untrusted network. Multifactor authentication requires using at least two of the following three factors: - Knowledge based factor, such as password, or PIN code, - Possession based factor, such as security card, or OTP - Inherence based factor, such as fingerprint recognition, or iris recognition. 		



[Figure 49] Example of multifactor authentication <source : Fortinet>

Objective	32. Software process and device identification and authentication	Standard	IEC62443-3-3/SR1.2
Require-ments	The CBS shall identify and authenticate software processes and devices		
Explan-ation	The function of identification and authentication is to map an ID to an unknown software process or device (henceforth referred to an entity in this sub-clause) so as to make it known before allowing any data exchange. Allowing rogue entities to send and receive computer-based system specific data can result in detrimental behavior of the legitimate computer-based system. All entities need to be identified and authenticated for all access to the computer-based system. Authentication of the identity of such entities should be accomplished by using methods such as passwords, tokens or location (physical or logical). This requirement should be applied to both local and remote access to the computer-based system. However, in some scenarios where individual entities are used to connect to different target systems (for example, remote vendor support), it may be technically infeasible for an entity to have multiple identities. In these cases, compensating countermeasures would have to be applied. Identification and authentication mechanisms for all entities are needed to protect against attacks such as man-in-the-middle or message spoofing. In some cases, these mechanisms may involve multiple software processes running on the same physical server, each having their own identity. In other cases, the identity may be bound to the physical device, such as all processes running on a given PLC.		

	Special attention needs to be made when identifying and authenticating portable and mobile devices. These types of devices are a known method of introducing undesired network traffic, malware and/or information exposure to computer-based systems, including otherwise isolated networks. Where entities function as a single group, identification and authentication may be role-based, group-based or entity-based, it is essential that local emergency actions as well as computer-based system essential functions are not hampered by identification or authentication requirements (see Clause 4 for a more complete discussion). For example, in common protection and control schemes, a group of devices jointly execute the protection functions and communicate with multicast messages among the devices in the group. In these cases, group authentication based on shared accounts or shared symmetric keys are commonly used. In order to support identification and authentication control policies, the computer-based system verifies the identity of all entities as a first step. In a second step, the permissions assigned to the identified entity are enforced.
Example	Provides a function to identify and authenticate software processes and external devices connected to the system

Objective	33. Unsuccessful login attempts	Standard	IEC62443-3-3/SR1.11
Require-ments	The CBS shall enforce a limit of consecutive invalid login attempts from untrusted networks during a specified time period.		
Explan-ation	Due to the potential for denial of service, the number of consecutive invalid access attempts may be limited. If enabled, the computer-based system may automatically reset to zero the number of access attempts after a predetermined time period established by the applicable security policies and procedures. Resetting the access attempts to zero will allow users (human, software process or device) to gain access if they have the correct login identifier. Automatic denial of access for computer-based system operator workstations or nodes should not be used when immediate operator responses are required in emergency situations. All lockout mechanisms should consider functional requirements for continuous operations so as to mitigate adverse denial of service operating conditions which could result in total system failure or injury to personnel. Allowing interactive logins to an account used for critical services could provide a potential for denial of service or other abuse.		
Example	Provides a function that prevents a user from logging in for a specified period after exceeding a predefined number of failed login attempts.		

Objective	34. System use notification	Standard	IEC62443-3-3/SR1.12
Require-ments	The CBS shall provide the capability to display a system use notification message before authenticating. The system use notification message shall be configurable by authorized personnel.		
Explan-ation	Privacy and security policies and procedures need to be consistent with applicable laws, directives, policies, regulations, standards and guidance. Often the main justification for this requirement is legal prosecution of violators and proving intentional breach. This capability is thus necessary to support policy requirements, and does not improve CBS security. System use notification messages can be implemented in the form of warning banners displayed when individuals log in to the computer based system. A warning banner implemented as a posted physical notice in the computer based system facility does not protect against remote login issues. Examples of elements for inclusion in the system use notification message are: - that the individual is accessing a specific computer based system - that system usage may be monitored, recorded and subject to audit - that unauthorized use of the system is prohibited and subject to criminal and/or civil penalties - that use of the system indicates consent to monitoring and recording.		
Example	Provides a function to display guidance text before logging in, which can be modified by an authorized user(crew).		

Objective	35. Access via Untrusted Networks	Standard	IEC62443-3-3/SR1.13
Require-ments	Any access to the CBS from or via untrusted networks shall be monitored and controlled.		
Explan-ation	Examples of access to the computer based system via untrusted networks typically include remote access methods (such as dial-up, broadband and wireless) as well as connections from a company's office (non-computer based system) network. The computer based system should restrict access achieved through dial-up connections or protect against unauthorized connections or subversion of authorized connections. Access via untrusted networks to geographically remote computer based system component locations should only be enabled when necessary and authenticated. Security policies and procedures may require multifactor authentication for remote user access to the computer based system.		
Example	When accessing the system from an untrusted network, it provides a function that requires explicit approval from a crew member. For instance, the user can access after the crew member clicks a button on a specific screen or generates an access code using tools/programs. The user then receives the code from the crew member, enters it, and gains access.		

Objective	36. Explicit access request approval	Standard	IEC62443-3-3/SR1.13, RE1

Require-ments	The CBS shall deny access from or via untrusted networks unless explicitly approved by authorized personnel onboard.
Example	When accessing the system from an untrusted network, it provides a function that requires explicit approval from a crew member. For instance, the user can access after the crew member clicks a button on a specific screen or generates an access code using tools/programs. The user then receives the code from the crew member, enters it, and gains access.

Objective	37. Remote session termination	Standard	IEC62443-3-3/SR2.6
Require-ments	The CBS shall provide the capability to terminate a remote session either automatically after a configurable period of inactivity or manually by the user who initiated the session.		
Explan-ation	A remote session is initiated whenever a computer based system is accessed across the boundary of a zone defined by the asset owner based on their risk assessment. This requirement may be limited to sessions that are used for computer based system monitoring and maintenance activities (not critical operations) based on the risk assessment of the computer based system and security policies and procedures. Some computer based systems or components may not allow sessions to be terminated.		
Example	Provides system session locking function for remote access, which triggered by system inactivity for a preset period of manual action by the user.		

Objective	38. Cryptographic integrity protection	Standard	IEC62443-3-3/SR3.1, RE1
Require-ments	The CBS shall employ cryptographic mechanisms to recognize changes to information during communication with or via untrusted networks.		
Example	Uses encrypted communication protocols to protect integrity		

Objective	39. Input validation	Standard	IEC62443-3-3/SR3.5
Require-ments	The CBS shall validate the syntax, length and content of any input data via untrusted networks that is used as process control input or input that directly impacts the action of the CBS.		
Explan-ation	Rules for checking the valid syntax of computer based system inputs such as set points should be in place to verify that this information has not been tampered with and is compliant with the specification. Inputs passed to interpreters should be pre-screened to prevent the content from being unintentionally interpreted as commands. Note that this is a security SR, thus it does not address human error, for example supplying a legitimate integer number which is outside the expected range. Generally accepted industry practices for input data validation include out-of-range values for a defined field type, invalid characters in data fields, missing or incomplete data and buffer overflow. Additional		

	examples where invalid inputs lead to system security issues include SQL injection attacks, cross-site scripting or malformed packets (as commonly generated by protocol fuzzers).
Example	When entering a value outside the control input range, the system does not accept the input, prevents abnormal operation, and provides guidance to the user with a warning message.

Objective	40. Session integrity	Standard	IEC62443-3-3/SR3.8
Require-ments	The CBS shall protect the integrity of sessions. Invalid session IDs shall be rejected.		
Explan-ation	This control focuses on communications protection at the session, versus packet, level. The intent of this control is to establish grounds for confidence at each end of a communications session in the ongoing identity of the other party and in the validity of the information being transmitted. For example, this control addresses man-in-the-middle attacks including session hijacking, insertion of false information into a session or replay attacks. Use of session integrity mechanisms can have a significant overhead and therefore their use should be considered in light of requirements for real-time communications.		
Example	Provides a function that requires the establishment of a new session, such as log-in, when the session is invalidated due to system inactivity for a preset period or by manual action by the user.		

Objective	41. Invalidation of session IDs after session termination	Standard	IEC62443-3-3/SR3.8, RE1
Require-ments	The system shall invalidate session IDs upon user logout or other session termination (including browser sessions).		
Example	Provides a function that requires the establishment of a new session, such as log-in, when the session is invalidated due to system inactivity for a preset period or by manual action by the user.		

Marine and Ocean Equipment Team **Website : www.krs.co.kr**
36, Myeongji ocean city 9-ro, Gangseo-gu, Busan, 46762 Republic of Korea.