CHARTING THE FUTURE

ClassNK

Guidelines for Cyber resilience of on-board systems and equipment (Edition 1.0)

[English]





Copyright @ 2023 Nippon Kaiji Kyokai

Revision History

No.	Date	Revised part	Revision details
1.0	2023.11.29		First issue



Introduction

Traditional marine systems primarily relied on physical connections and controls without giving much consideration to threats such as unauthorized access or attacks from external sources. However, with rapid advancements in technology, marine systems have become digitally interconnected through computers and the Internet. As a result, such systems are now exposed to cyberspace and, thus, find themselves under the ever increasing the risks of cyber-attacks.

In April 2022, IACS (International Association of Classification Societies) issued two new URs (Unified Requirements) for cybersecurity (UR E26 and UR E27). These URs specify requirements related to the capability to reduce the occurrence and mitigate the effects of cyber incidents due to cyber-attacks (hereinafter referred to as "cyber resilience"). UR E26 covers ships and UR E27 covers on-board systems and equipment. The aim of the two URs is to ensure minimum cyber security of ships by providing a minimum set of requirements for cyber resilience of ships, on-board systems, and equipment. Following the publication of UR E26 and UR E27, the Nippon Kaiji Kyokai (hereinafter referred to as "the Society") has decided to incorporate these requirements in Part X of the *Rules for the Survey and Construction of Steel Ships* (hereinafter referred to as "Part X").

For the first time, cybersecurity measures have been incorporated into the Society's rules as mandatory requirements. As a result, many questions are expected to be raised by those concerned since cyber-attacks are always changing, and updating cybersecurity information is essential to respond to more complex and sophisticated evolving attacks. To address these concerns, we actively disseminate information as a third-party organisation that provides the highest quality classification services. As part of this information dissemination, we have decided to issue this Guidelines.

This Guidelines for cyber resilience of on-board systems and equipment (hereinafter referred to as "Guidelines") is a commentary on Chapter 4, Part X (UR E27). Specifically, this Guidelines explains the following.

Scope and approval process

This Guidelines describes procedures for approval by the Society including whether computer-based systems (hereinafter referred to as "CBS") are applicable. It also explains in detail requirements related to document reviews and surveys.

- Cyber resilience requirements

This Guidelines explains requirements related to the cyber resilience of on-board systems and equipment. These requirements are based on and incorporate parts of the International Electrotechnical Commission standard IEC 62443 and are described in detail.

Outline



Chapter 1 Application

This chapter describes the scope of application of Chapter 4, Part X (UR E27), and explains how to determine whether it applies to a particular CBS.

-

Chapter 2 Approval process

This chapter provides an overview of the two types of approval processes (individual product approval and type approval) specified for CBS in Chapter 4, Part X (UR E27). This chapter is intended to get an overview of the approval process.



Chapter 3 Explanation of Documentation

This chapter explains requirements related to the documentation to be submitted to the Society's Machinery Department for review and approval. This chapter is intended to <u>understand the details of documentation</u>.



Chapter 4 Explanation of Surveys

This chapter explains the requirements related to the surveys carried out by Society branch offices after documentation review. This chapter is intended to <u>understand the details of surveys</u>.



Chapter 5 Explanation of System requirements

This chapter explains "system requirements", which consist of security requirements for CBS related to security features that should be provided. This chapter is intended to <u>understand the details</u> of "System requirements".

20

Chapter 6 Explanation of Secure Development Lifecycle requirements

This chapter explains "secure development lifecycle requirements", which consist of security requirements for CBS related to lifecycle support for installation and maintenance. This chapter is intended to understand the details of "Secure Development Lifecycle requirements".

Contents

Chapter	1 Application	. 1
Chapter	2 Approval process	5
Overv	iew of Approval process	5
Indivi	dual product approval process	5
0 9	System is not type approved	. 7
2 9	System is type approved	9
B I	Previously approved system installed on sister vessel	11
Type a	approval process	14
	3 Explanation of Documentation	
	iew of Documentation	
Detail	of Documentation	19
1.	CBS asset inventory	20
2.	Topology diagrams	22
3.	Description of Security capabilities	24
4.	Test procedure of security capabilities	26
5.	Security configuration guidelines	
6.	Secure development lifecycle documents	30
7.	Plans for maintenance and verification of the CBS	32
8.	Information supporting the owner's incident response and recovery plan	
9.	Management of change plan	36
10.	Test reports	37
Chapter	4 Explanation of Surveys	39
Overv	iew of Surveys	39
	of Surveys	
	General survey items	
2.	Test of security capabilities	43
3.	Correct configuration of security capabilities	44
4.	Secure development lifecycle	46
Chapter	5 Explanation of System requirements	47
Overv	iew of System requirements	47
Detail	of System requirements	52
1.	Human user identification and authentication	53
2.	Account management	56
3.	Identifier management	59
	Authenticator management	
5.	Wireless access management	
6.	Strength of password-based authentication	38
7.	Authenticator feedback	71
8.	Authorization enforcement	73
9	Wireless use control	76

	10.	Use control for portable and mobile devices	79
	11.	Mobile code	82
	12.	Session lock	84
	13.	Auditable events	86
	14.	Audit storage capacity	89
	15.	Response to audit processing failures	92
	16.	Timestamps	94
	17.	Communication integrity	96
	18.	Malicious code protection	99
	19.	Security functionality verification	102
	20.	Deterministic output	105
	21.	Information confidentiality	
	22.	Use of cryptography	109
	23.	Audit log accessibility	. 111
	24.	Denial of service protection	.113
	25.	Resource management	.115
	26.	System backup	.118
	27.	System recovery and reconstitution	120
	28.	Alternative power source	123
	29.	Network and security configuration settings	125
	30.	Least Functionality	128
	31.	Multifactor authentication for human users	130
	32.	Software process and device identification and authentication	133
	33.	Unsuccessful login attempts	135
	34.	System use notification	138
	35.	Access via Untrusted Networks	141
	36.	Explicit access request approval	143
	37 .	Remote session termination	145
	38.	Cryptographic integrity protection	148
	39.	Input validation	150
	40.	Session integrity	152
	41.	Invalidation of session IDs after session termination	154
Cha	pter 6	Explanation of Secure Development Lifecycle requirements	156
0	vervie	w of Secure Development Lifecycle requirements	156
D	etail o	f Secure Development Lifecycle requirements	158
	1. C	ontrols for private keys	159
	2. S	ecurity update documentation	161
	3. D	ependent component and Operation system security update documentation	163
	4. S	ecurity update delivery	165
	5. P	roduct defence in depth	167
	6. D	Pefence in depth measures expected in the environment	169
	7. S	ecurity hardening guidelines	171

Reference	176
Appendix 1 Checklist of Document reviews	177
Appendix 2 Checklist of Surveys	197

Note: This Guidelines frequently refers to the rule number of Part X of the Society's rule, which has not yet been issued. Part X will be newly issued incorporating UR E26 and UR E27 by July 2024. We would appreciate your understanding in this matter.

Chapter 1 Application

This chapter describes those CBS to which Chapter 4, Part X (UR E27) is applicable, and the following flowchart (Figure 1) can be used to help determine this applicability.

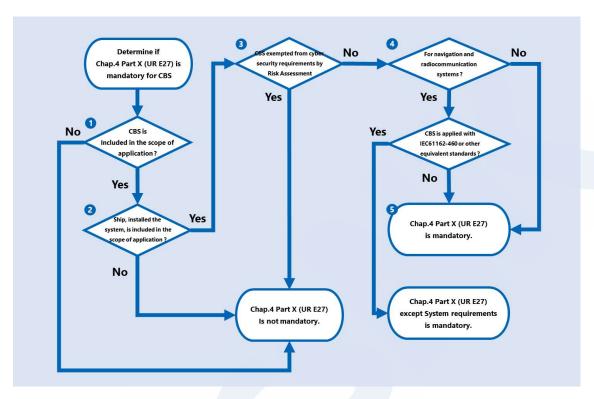


Figure 1 Flowchart of possibility of Application

1 CBS within the scope of Chapter 4, Part X (UR E27)

A CBS is a programmable electronic device or interoperable set of programmable electronic devices that are organised to achieve one or more specified purposes such as the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. A programmable electronic device is a physical component in which software is installed and includes a programmable logic controller (PLC).

Those systems subject to Chapter 4, Part X (UR E27) are ones that can <u>potentially lead to</u> dangerous situations for human safety and safety of the ship and/or threat to the environment.

The following are examples of computer systems that may be considered to fall within the scope of application of Chapter 4, Part X (UR E27). Please note that these are only examples, and systems may otherwise be deemed applicable or non-applicable regardless of the table below.



Propulsion

Engine control systems

Engine remote control systems

Main boiler control systems	CPP control systems
Electric propulsion control systems	FGSS control systems
Machinery alarm and monitoring systems (including data loggers)	Waterjet propulsion systems
Steering system control systems	Azimuth thruster control systems
Anchoring and mooring	

Generator engine control systems Electric power converters
(including power management systems) (for electric propulsion ship)

Battery management systems (consisting of lithium-ion batteries with total capacities of 20 kWh or more, and associated equipment)



Fire detection and extinguishing systems

Fire detection and alarm systems

Fixed CO₂ fire extinguishing systems

Fixed local application fire-fighting systems

Dry chemical fire-extinguishing equipment

Fixed foam fire extinguishing systems

Fixed foam fire extinguishing systems

Water-spraying systems



Bilge and ballast system, loading computer

Ballast transfer valve remote control systems

Loading computers



Watertight integrity and flooding detection

Watertight door power opening/closing Water level detection and alarm systems devices



Lighting (e.g. emergency lighting, low locations, navigation lights, etc.)

Navigation lighting control systems



Any required safety system whose disruption or functional impairing may pose risks to ship operations (e.g. emergency shutdown system, cargo safety system, pressure vessel safety system, gas detection system, etc.)

Inert gas systems	Cargo monitoring control systems
Liquefied gas emergency shutdown systems	Flammable gas detection systems
Reliquefication plants	Auxiliary boiler control systems
GCU control systems	Gas fuel tank monitoring and control systems



Navigational systems required by statutory regulations

Radar	Transmitting heading devices (THD)
Electronic plotting aids (EPA)	Automatic identification systems (AIS)
Automatic tracking aids (ATA)	Voyage date recorders (VDR)
Automatic radar plotting aids (ARPA)	Heading control systems (HCS)
Echo sounding devices	Track control systems (TCS)
Global navigation satellite systems (GPS)	Long range identification and tracking systems
	(LRIT)
Sound reception systems	Bridge navigational watch alarm systems
	(BNWAS)
Speed and distance measuring devices	Electronic chart display and information systems
	(ECDIS)



Internal and external communication systems required by class rules and

statutory regulations

General emergency alarm	Public addressor
NAVTEX receiver	VHF DSC device
EGC receiver	DSC device
VHF DSC continuous watch device	DSC continuous watch device
GMDSS radio installation	_



Others

Dynamic positioning systems (DPS)



2 Vessels within the scope of Chapter 4, Part X (UR E27)

Chapter 4, Part X (UR E27) applies to computer-based systems installed on board the following

vessels registered with ClassNK, whose contracts for construction are made on or after 1 July 2024...

- Passenger ships (including passenger high-speed craft) engaged in international voyages
- Cargo ships of 500 GT and upwards engaged in international voyages
- High speed craft of 500 GT and upwards engaged in international voyages
- Mobile offshore drilling units of 500 GT and upwards
- Self-propelled mobile offshore units engaged in construction (i.e., wind turbine installation maintenance and repair, crane units, drilling tenders, accommodation, etc.)

CBS installed on vessels other than those listed above are not applicable and do not require approval. Type approval, however, may still be obtained even if the CBS is not intended to be installed on a vessel. Please refer to "Type approval process" for more details.



Type approval process

P. 14

3 Risk assessment

CBS subject to the <u>risk assessments</u> required by Chapter 5, Part X (UR E26) and approved by the Society are exempt from Chapter 4, Part X (UR E27).

4 Navigational and radiocommunication systems

CBS conforming to <u>IEC 61162-460 or other equivalent standards</u> that are used for navigational and radiocommunication systems may be exempted from the "system requirements" specified in Chapter 4, Part X (UR E27) provided that they meet the requirements of Chapter 5, Part X (UR E26).

5 CBS subject to Chapter 4, Part X (UR E27)

Since CBS subject to Chapter 4, Part X (UR E27) must meet the requirements set forth in that chapter, document reviews and surveys should be conducted prior to shipment. Please refer to "Individual product approval process" for more details.



Individual product approval process

P. 5

Chapter 2 Approval process

This chapter describes the CBS approval process as defined in Chapter 4, Part X (UR E27) and GUIDANCE FOR THE APPROVAL AND TYPE APPROVAL OF MATERIALS AND EQUIPMENT FOR MARINE USE Part 7 Chapter 10. The purpose of this chapter is to provide an overview of our approval process in Chapter 4 Part X (UR E27).

Overview of Approval process

The first step is to determine whether the product is subject to Chapter 4, Part X (UR E27). This is explained in more detail in "Chapter 1 Application".



Chapter 1 Application

P.1

For CBS to which this chapter applies, there are two types of approval: individual product approval and type approval. A summary of each type of approval is as follows.

Approval type	Description
Individual product	This refers to product approval. Chapter 4, Part X (UR E27) applies to
approval	computer systems installed on applicable ships, and approval is required for
	each product.
Type approval	This refers to type approval. Part of the process required for individual
	product approval is eliminated by conducting the examinations and
	inspections of representative types specified in Chapter 4, Part X (UR E27)
	before it is prepared to be installed on board a ship.

Individual product approval process

The process for approving an individual product is divided into several processes depending on whether the system has type approval and on the approval records for sister vessels. The overview of processes is as follows:

Individual product approval process	Description
System is not type approved	In principle, all documentation and surveyor presence at surveys are required.
System is type approved	Some documentation may be omitted. In addition, surveyor presence at surveys may also be omitted in lieu of the submission of test reports.

Previously approved system installed on sister vessel

After comparing and examining any differences with the previously approved system, some or all documentation and survey presence at surveys may be omitted.

Figure 2 shows a flowchart for individual product approval.

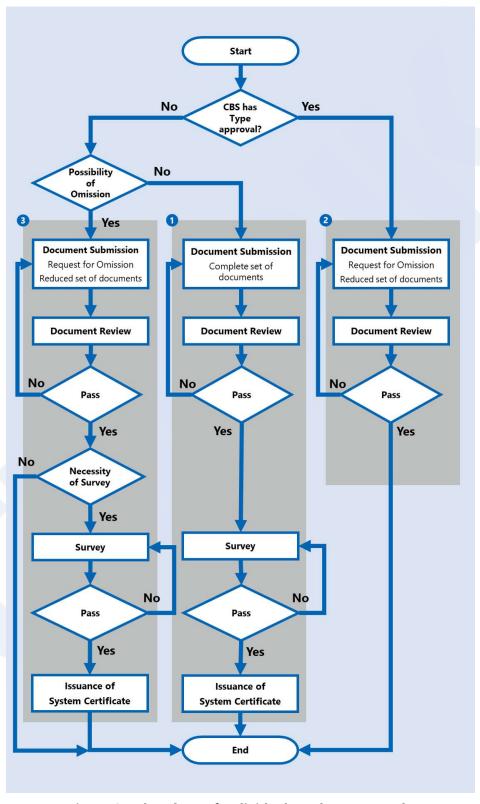


Figure 2 Flowchart of Individual product approval

1 System is not type approved

Figure 3 shows a flowchart for systems that are not type approved.

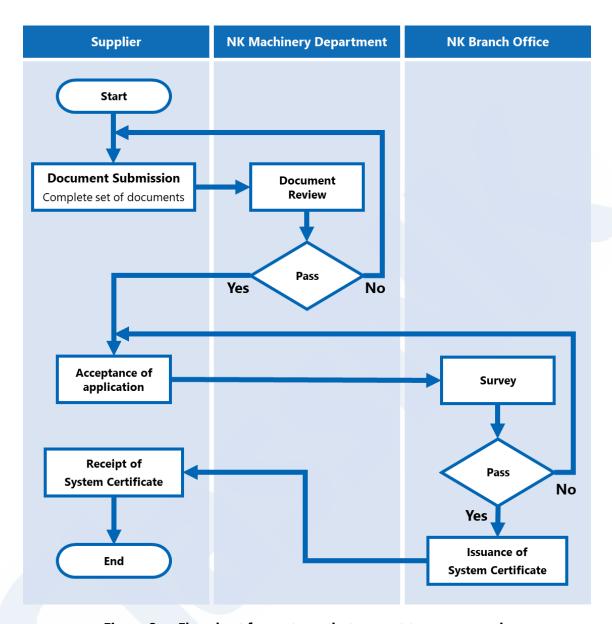


Figure 3 Flowchart for systems that are not type approved

Document submission and review

In principle, all documentation must be submitted on a ship-by-ship basis for systems that are not approved for use. Please use NK-PASS to submit relevant documentation. Please refer to the following URL for more information on NK-PASS.

URL: https://www.classnk.com/hp/en/activities/portal/nk-pass.html

The following documentation is to be submitted.

Documentation
CBS asset inventory
Topology diagrams
Description of Security capabilities
Test procedure of security capabilities
Security configuration guidelines
Secure development lifecycle documents
Plans for maintenance and verification of the CBS
Information supporting the owner's incident response and recovery plan
Management of change plan

Please refer to "Chapter 3 Document submission and review" in "Chapter 3 Documentation" for more information on the documentation required.

Chapter 3 Explanation of Documentation

P. 18

The Machinery Department reviews submitted documents upon receipt, and contacts applicants when it has any comments, requires any modifications or requires the submission of additional documents. Submitted documents which have been approved are returned to applicants stamped with the Society's official stamp.

Since surveys are optional for systems that are type approved, the Society's approval process is considered to be completed upon receipt of the approved documents by the applicant.

Surveys

Surveys in the presence of a Society surveyor are required after the document review process is completed. Please apply to the branch office nearest to your location for such surveys. Please refer to the following URL for a current list of NK branch offices.

URL: https://www.classnk.com/hp/en/directory/dir_top.aspx

The following are some of documents required for surveys.

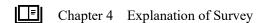
Documentation required for surveys
CBS asset inventory
Topology diagrams
Test procedure of security capabilities
Security configuration guidelines
Secure development lifecycle documents

Please ensure that the document review is completed and that any comments related to non-survey matters are resolved before applying for surveys. Once confirmed, please submit an application form and all required documents to the branch office in charge of the survey.

In principle, the following survey items are required for systems that are not type approved.

Survey items
General survey items
Test of security capabilities
Correct configuration of security capabilities
Secure development lifecycle

Please refer to "Chapter 4 Explanation of Surveys" for more information on surveys.



P. 39

The branch office in charge of the survey will issue a system certificate when the survey is completed, and the Society's approval process is considered to be completed upon receipt of the system certificate by the applicant.

System is type approved

Figure 4 shows a flowchart for systems that are type approved.

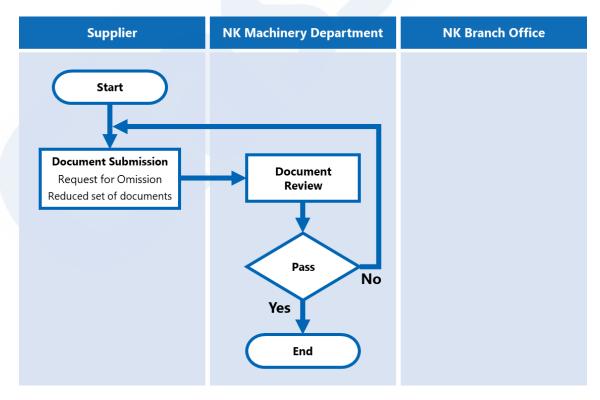


Figure 4 Flowchart for systems that are type approved

Document submission and review

The submission of some of the required documents may be exempted for systems that are type approved. Applications for exemptions from submission of documents are to include the following information.

Applications for exemption from submission of documents based on type		
approval		
Copy of the type approval certificate		
List of any differences from the type approved product, including software versions		

Please use NK-PASS to submit relevant documentation. Please refer to the following URL for more information on NK-PASS.

URL: https://www.classnk.com/hp/en/activities/portal/nk-pass.html

The following documentation is required for exemptions.

Documentation
CBS asset inventory
Topology diagrams
Test reports
Application for exemption from submission of documents based on the type approval

Please refer to "Chapter 3 Explanation of Documentation" for more information of the documentation required.



P. 18

The Machinery Department reviews submitted documents upon receipt and contacts applicants when it has any comments, requires any modifications or requires the submission of additional documents. Submitted documents that have been approved are returned to applicants stamped with the Society's official stamp.

Since surveys are optional for systems that are type approved, and the Society's approval process is considered to be completed upon receipt of the approved documents by the applicant.

3 Previously approved system installed on sister vessel

Figure 5 shows a flowchart for previously approved systems that are subsequently installed on sister vessels.

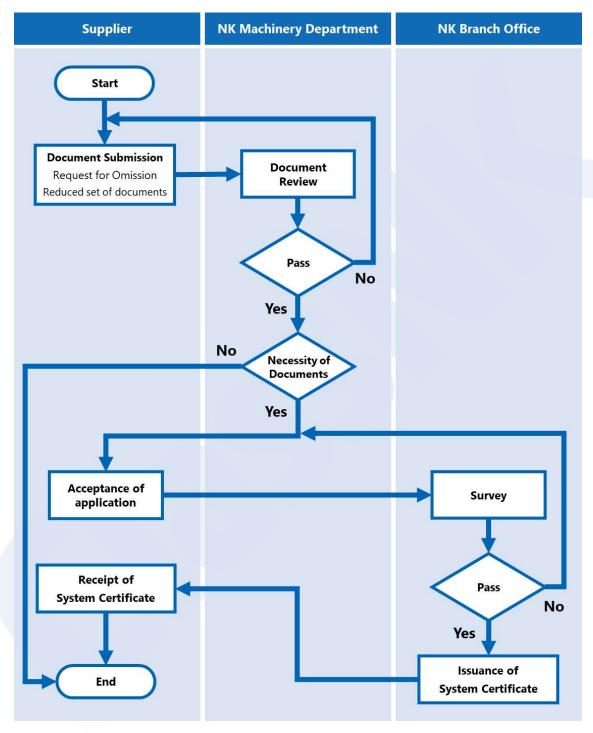


Figure 5 Flowchart for previously approved system installed on sister vessel

Document submission and review

The omitting of the submission of documents for second and subsequent ships for previously

approved systems installed on sister vessels is possible when there are no modifications made to such systems and there are no changes in the previously approved documents. Applications for exemptions from document submission are to include the following information.

Details of applications for exemption from submission of documents for previously approved systems installed on sister vessels
Information about the first vessel (reference vessel) for which relevant documents have been previously approved
Software version information of machinery and systems for the reference vessel and the subject vessel. If the software version for the subject vessel is an upgraded version of that used by the reference vessel, the version history is required.
List of all specification differences between the reference vessel and the subject vessel
Names of documents for which an exemption from submission is requested

In addition, when applicants submit documentation that proves that the system configuration, its functions and control specifications are the same as those of tests previously conducted in the presence of a Society surveyor and the test results are the same together with a request for omission of the survey, surveys may also be admitted on a case-by-case basis. Applications for exemptions from surveys are to include the following information.

Applications for exemption from surveys for previously approved systems	
installed on sister vessels	
Information about the first vessel (reference vessel) for which relevant documents have been	
previously approved	
Software version information of machinery and systems for the reference vessel and the subject	
vessel. If the software version for the subject vessel is an upgraded version of that used by the	
reference vessel, the version history is required.	
List of all specification differences between the reference vessel and the subject vessel	

In the above case, the documents that need to be submitted are as follows.

Documentation
CBS asset inventory
Topology diagrams
Test reports
Applications for exemption from document submission for previously approved systems
installed on sister vessels
Applications for exemption from surveys for previously approved systems installed on sister

Surveys

In principle, the individual product approval process is considered to be completed upon receipt of the approved documents by the applicant when applications for omission for all surveys are submitted and approved. However, partial or complete surveys may still be requested where desired by contacting the nearest branch office as described in "1 System is not type approved". Please refer to following URL for a current list of NK branch offices.

URL: https://www.classnk.com/hp/en/directory/dir top.aspx

The following documents are required for surveys.

Documents required for survey
CBS asset inventory
Topology diagrams
Test procedure of security capabilities
Security configuration guidelines
Secure development lifecycle documents

In principle, the following survey items are required for systems that are not type approved. However, some survey items may be omitted by applying for omission of survey. In such cases, the necessary survey from among the following survey items should be conducted in the presence of a Society surveyor.

Survey items		
General survey items		
Test of security capabilities		
Correct configuration of security capabilities		
Secure development lifecycle		

Please refer to "Chapter 4 Explanation of Surveys" for more information on surveys.

Chapter 4 Explanation of Survey

P. 39

Upon completion of surveys, system certificates are issued by the branch offices respectively in charge of the surveys. The individual product approval process for previously approved systems installed on sister vessels is considered to be completed upon receipt of the system certificate by the applicant.

Type approval process

This section provides an overview of the type approval process. Figure 6 shows a flowchart for this process.

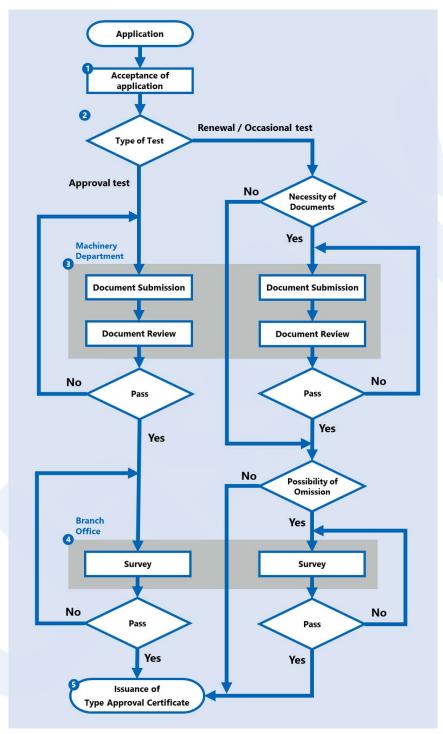


Figure 6 F Flowchart for the type approval process

1 Application

Applicants for type approval should submit application form "Form 7-10(E)" to the Machinery Department (email: mcd@classnk.or.jp) by NK-PASS or email after filling in the required items. The

application form can be downloaded from the "Class Survey (Manufacturers)" section of the Society's official website. Please use the following URL to download the form.

URL: https://www.classnk.com/hp/en/download/dl_appli.aspx

2 Type of test

The following three types of tests are available for type approval.

Survey	Description	
Approval Conducted when type approval is to be newly obtained for the CBS.		
Test		
Renewal	Conducted when renewing the expiration date of a CBS which is type approved.	
Test	The validity period of the type approval is five years, and this test is to be conducted	
	when renewal of the validity period is desired.	
Occasional	Conducted when a CBS which is type approved is changed or modified in some	
Test	way.	

3 Document Submission, Document Review

The documents required for type approval are to be submitted in one of the following ways.

- a) NK-PASS
- b) Email (mcd@classnk.or.jp)
- c) Regular mail (three copies of each document are to be submitted.)

It is acceptable to submit the documents at the time of application, and the following documents are to be submitted.

Documentation required for type approval
CBS asset inventory
Topology diagrams
Description of Security capabilities
Test procedure of security capabilities
Security configuration guidelines
Secure development lifecycle documents
Plans for maintenance and verification of the CBS
Information supporting the owner's incident response and recovery plan
Management of change plan

☐ Test reports

Please refer to "Chapter 3 Explanation of Documentation" for more information on the documents to be submitted.

Chapter 3 Explanation of Documentation

P. 18

The Machinery Department reviews submitted documents upon receipt, and contacts applicants when it has any comments, requires any modification or requires the submission of additional documents.

All documents are to be submitted for approval tests, but a document review will be conducted as necessary for renewal tests and some documents may not need to be submitted. Cases that require document review include those in which changes are made to the specifications of the type approved product since the date of approval (renewal date), or changes or additions needing to be made to previously submitted documents due to revisions of the Society's rules.

Only those documents that have been changed need be submitted for occasional tests. In such cases, a "history of changes" or another suitable document that clearly identifies the changes made should be sent to the Machinery Department along with the application for occasional test and documents required to be submitted.

4 Surveys

Surveys in the presence of a Society surveyor are required after the document review process is completed. Please apply to the branch office nearest to your location for such surveys. Please refer to the following URL for a current list of NK branch offices.

URL: https://www.classnk.com/hp/en/directory/dir_top.aspx

The following are some of the documents required for surveys.

Documents required for surveys
CBS asset inventory
Topology diagrams
Test procedure of security capabilities
Security configuration guidelines
Secure development lifecycle documents

Please ensure that the document review process is completed before applying for surveys. Once confirmed this, please apply form and all the required documents to the branch office in charge of

the survey.

Surveys may differ for approval tests, renewal tests, and occasional tests. In principle all survey items are required for approval tests, and all surveys must be conducted in the presence of a Society survey. Please consult with the branch office in charge of the survey regarding the survey schedule and details.

Only necessary survey items are required for renewal surveys; for example, surveys are required for changes in system specifications, or changes or additions to survey requirements due to revisions of the Society's rules.

Only those survey items related to system changes requiring the presence of a Society surveyor are required for occasional tests.

Please refer to "Chapter 4 Explanation of Survey" for more information on surveys.



Chapter 4 Explanation of Survey

P. 39

5 Issuance of Type Approval Certificate

The branch office in charge of the survey will inform the Machinery Department of the survey results, and a type approval certificate will be issued by the Machinery Department when such results are satisfactory.

In principle, the period of validity for type approval certificates is as follows: five years from the date of issue for those issued for approval tests, five years from the day after the expiration date of the previous certificate for those issued for renewal tests, and the period of validity of the previous certificate for those issued for occasional tests.

The type approval process is considered to be completed upon receipt of a new type approval certificate by the applicant.

Chapter 3 Explanation of Documentation

This chapter provides detailed information about the documentation described in Part X, Chapter 4 (UR E27).

Overview of Documentation

Documentation Requirements

Part X, Chapter 4 (UR E27), specifies the requirements for a total of 10 documentation related to computer system cybers resilience. Each documentation is as follows.

Documentation Requirements	
1. CBS asset inventory	P. 20
2. Topology diagrams	P. 22
3. Description of Security capabilities	P. 24
4. Test procedure of security capabilities	P. 26
5. Security configuration guidelines	P. 28
6. Secure development lifecycle documents	P. 30
7. Plans for maintenance and verification of the CBS	P. 32
8. Information supporting the owner's incident response and recovery plan	P. 33
9. Management of change plan	P. 36
10. Test reports	P. 37

Required documentation varies in approval process

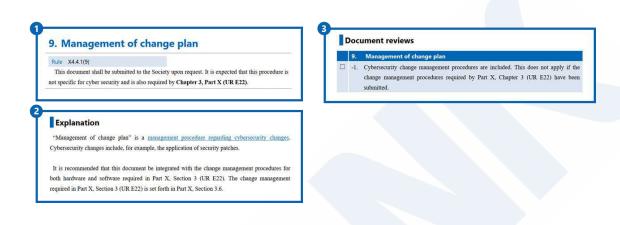
In the case of individual product approval, required documentation varies depending on whether approval for use has been granted or not, and the approval performance of the same type of ship. The required documentation for each approval process are described in detail in Chapter 2: Approval



Chapter 2 Approval process

Detail of Documentation

How to view the following pages



1 Requirement

The names and the details of the documentation requirements.

2 Explanation

An explanation of documentation.

3 Document reviews

A document reviews checklist for the requirements

1. CBS asset inventory

Reg. 4.4.1(1), Part X of the Rules

The CBS asset inventory shall include the information below.

- (a) List of hardware components (e.g., host devices, embedded devices, network devices)
- i) Name
- ii) Brand/manufacturer
- iii) Model/type
- iv) Short description of functionality/purpose
- v) Physical interfaces (e.g., network, serial)
- vi) Name/type of system software (e.g., operating system, firmware)
- vii) Version and patch level of system software
- viii) Supported communication protocols
- (b) List of software components (e.g., application software, utility software)
- i) The hardware component where it is installed
- ii) Brand/manufacturer
- iii) Model/type
- iv) Short description of functionality/purpose
- v) Version of software

Explanation

"CBS asset inventory" <u>provides a detailed list of assets owned by the computer system.</u> Here, assets refer to the components that make up the computer system. There are two types of components: hardware and software.

The details are as follows:

- Hardware Components

These are the physical components of a system, such as host devices, embedded devices, network devices.

- Software Components

These are the logical components of a system and refer to applications and operating systems. Unlike hardware components, software components are internal system programs and cannot be physically contacted.

The purpose here is to <u>identify the hardware and software that the system has</u>. This is important to grasp potential vulnerabilities in your system and to consider countermeasures.

Note: Confirm that your computer system is properly configured according to the computer system asset inventory by on-site inspection. Details are explained in detail in "General survey items".

General survey items

P. 41

Document reviews

1. C	1. CBS asset inventory		
-1.	The	following items are to be included.	
(1)	List	of hardware components	
	(a)	Name	
	(b)	Brand/manufacturer	
	(c)	Model/type	
	(d)	Short description of functionality/purpose	
	(e)	Physical interfaces (e.g., network, serial)	
	(f)	Name/type of system software (e.g., operating system, firmware)	
	(g)	Version and patch level of system software	
	(h)	Supported communication protocols	
(2)	List	of software components	
	(a)	The hardware component where it is installed	
	(b)	Brand/manufacturer	
	(c)	Model/type	
	(d)	Short description of functionality/purpose	
	(e)	Version of software	

2. Topology diagrams

Reg. 4.4.1(2), Part X of the Rules

- (a) The physical topology diagram shall illustrate the physical architecture of the system. It shall be possible to identify the hardware components in the CBS asset inventory. The diagram shall illustrate the following:
- i) All endpoints and network devices, including identification of redundant units
- ii) Communication cables (networks, serial links), including communication with I/O units
- iii) Communication cables to other networks or systems
- (b) The logical topology diagram shall illustrate the data flow between components in the system. The diagram shall illustrate the following:
- i) Communication endpoints (e.g., workstations, controllers, servers)
- ii) Network devices (switches, routers, firewalls)
- iii) Physical and virtual computers
- iv) Physical and virtual communication paths
- v) Communication protocol

One combined topology diagram may be acceptable if all requested information can be clearly illustrated.

Explanation

"Topology diagrams" is <u>a diagram showing the physical and logical configuration of the network</u>. There are two types of diagrams: physical and logical.

The details are as follows:

- Physical topology diagram

A physical network structure diagram. For example, information such as system configuration and connection cable route.

- Logical topology diagram

A logical network structure diagram. In addition to the flow of communication about physical components, this diagram also illustrates the flow in virtual spaces, such as virtual computers and virtual communication paths.

The purpose here is to grasp the physical and logical configuration of the system. This is important in determining and segmenting the security zones of the network during system integration.

Note: Confirm that the computer system is properly configured according to the topology diagram by on-site inspection. Details are explained in detail in "General survey items".



General survey items

P. 41

Document reviews

2. Topology diagrams			
-1.	The	following items are to be included.	
(1)	Phy	sical topology diagram	
	(a)	All endpoints and network equipment, including identification of redundant units	
	(b)	Communication cables, including communication with I/O units (Networks, serial	
		links, etc.)	
	(c)	Communication cables to other networks or systems	
(2)	Log	ical topology diagram	
	(a)	Communication endpoints (Workstations, controllers, servers, etc.)	
	(b)	Network devices (Switches, routers, firewalls, etc.)	
	(c)	Physical computer and virtual computers	
	(d)	Physical communication path and virtual communication paths	
	(e)	Communication protocols	

3. Description of Security capabilities

Reg. 4.4.1(3), Part X of the Rules

- (a) This document shall describe how the CBS with its hardware and software components meets the required security capabilities.
- (b) Any network interfaces to other CBS in the scope of applicability of Chapter 4, Part X (UR E26) shall be described. The description shall include destination CBS, data flows, and communication protocols. If the System integrator has allocated the destination CBS to another security zone, components providing protection of the security zone boundary shall be described in detail if delivered as part of the CBS.
- (c) Any network interfaces to other systems or networks outside the scope of applicability of UR E26 (untrusted networks) shall be described. The description shall specify compliance with the additional security capabilities, and include relevant procedures or instructions for the crew. Components providing protection of the security zone boundary shall be described in detail if delivered as part of the CBS.
- (d) A separate chapter shall be designated for each requirement. All hardware and software components in the system shall be addressed in the description, as relevant.
- (e) If any requirement is not fully met, this shall be specified in the description, and compensating countermeasures shall be proposed. The compensating countermeasures should:
- i) Protect against the same threats as the original requirement
- ii) Provide an equal level of protection as the original requirement
- iii) Not be a security control that is required by other requirements in this UR
- iv) Not introduce higher security risk

Any supporting documents (e.g. OEM¹ information) necessary to verify compliance with the requirements shall be referenced in the description and submitted.

Explanation

"Description of Security capabilities" is a <u>document that describes in detail the security functions</u> specified in X 4.4.2 and X 4.4.3.

Specifically, the following should be described:

· Security capabilities and compensating countermeasures

This document should describe security capabilities to meet system requirements. System requirements are requirements for security capabilities required for computer systems as part of cybersecurity measures.

Compensating countermeasures are measures adopted in place of the original security capabilities.

¹ **OEM**: Original Equipment Manufacturer. A company that manufactures products of other brands.

If the required security capabilities cannot be implemented in the system, compensating countermeasures are taken to replace those capabilities.

For details, see Chapter 5, "Explanation of System Requirements".

Chapter 5 Explanation of System requirements

P. 47

- Network interface

This refers to the point of contact (point of contact) for connecting to the network. For example, Ethernet NIC¹ and wireless LAN adapter are applicable. Network interfaces should be included in this document, along with information such as the computer system to which they communicate, data flows, and communication protocols. Network interfaces should be listed for each of the following networks:

- Networks within the scope of Part X, Chapter 4 (UR E27)

 This refers to networks configured by systems approved according to Part X, Chapter 4 (UR E27).
- Untrusted Networks

This refers to networks outside the scope of Part X, Chapter 4 (UR E27). For example, the Internet, etc. In this case, details must be provided on whether the components responsible for protecting the security zone boundaries are delivered as part of the system.

- Any supporting documents necessary to verify compliance with the requirements

Document reviews

3. Description of Security capabilities			
-1. The following items are to be included.			
(1) Security capabilities and compensating countermeasures			
See "Chapter 5 Explanation of System requirements" for more information.			
(2) Network interface			
(a) Networks within the scope of Part X, Chapter 4 (UR E27)			
(b) Untrusted Networks			
For the components responsible for protecting security zone boundaries, the detail	Ĺ		
whether they are delivered as a part of system should be described.			
(3) Any supporting documents necessary to verify compliance with the requirements			

_

¹ NIC: Network Interface Card. For example, LAN port.

4. Test procedure of security capabilities

Reg. 4.4.1(4), Part X of the Rules

- (a) This document shall describe how to demonstrate by testing that the system complies with the requirements of **the required security capabilities and the additional security capabilities**, including any compensating countermeasures. Demonstration of compliance by analytic evaluation may be specially considered. The procedure shall include a separate chapter for each applicable requirement and describe:
- i) Necessary test setup (i.e. to ensure the test can be repeated with the same expected result
- ii) Test equipment
- iii) Initial condition(s)
- iv) Test methodology, detailed test steps
- v) Expected results and acceptance criteria

The procedure shall also include means to update test results and record findings during the testing.

Explanation

"Test procedure of security capabilities" is the <u>test plan for the surveys of the security capability</u> <u>test as specified in Part X 2.2.3 (2)</u>. The survey demonstrates the required security capability in accordance with this document. Details of the required security features are described in detail in "Chapter 5 Explanation of system requirements".



Chapter 5 Explanation of System requirements

P. 47

When you take compensating countermeasures in place of security capabilities, Confirm the compensating countermeasures. These confirmation methods should also be included in this document.

This document should also include the necessary test setup, test equipment, initial conditions, test methodology, and expected results for the demonstration test for each requirement. It should also include a space to record test results and findings during the testing.

The details of the survey are explained in detail in "2. Test of security capabilities".



Test of security capabilities

P. 43

Document reviews

4. Test procedure of security capabilities

- \Box -1. The following items are to be included.
- (1) Demonstration tests of security capabilities and confirmation of compensating

countermeasures
See "Chapter 5 Explanation of System requirements" for more information.
(a) Necessary test setup
(b) Test equipment
(c) Initial condition(s)
(d) Test methodology, detailed test steps
(e) Expected results and acceptance criteria
(f) Entry column to update test results and record findings during the testing

5. Security configuration guidelines

Reg. X4.4.1(5), Part X of the Rules

- (a) This document shall describe recommended configuration settings of the security capabilities and specify default values. The objective is to ensure the security capabilities are implemented in accordance with **Chapter 5**, **Part X (UR E26)** and any specifications by the System integrator (e.g. user accounts, authorisation, password policies, safe state of machinery, firewall rules, etc.)
- (b) The document shall serve as basis for verification of item no. 29 "Network and security configuration settings" in System Requirements.

Explanation

"Security configuration guidelines" is a <u>document that explains recommended settings and default values for security capabilities provided to a computer system</u>. This document is the guideline to configurate in accordance with network and security structure recommended in guideline provided by a supplier. The purpose of this document is to ensure that the integrator's customers can properly set up and utilize the security capabilities of their products and systems according to their own specifications.

For more information, see the following:

- Description of the recommended configuration settings for security capabilities

Security configuration guidelines provide detailed descriptions on how to set up and use security capabilities. This includes, for example, how to configure user authentication, selection and configuration of encryption options, and configuration of network filtering.

- Specified default values

The guidelines also specify default values for each security setting. Default values typically indicate settings immediately after the system installation. However, because the default settings are often not the most secure settings, the integrator should review these settings and adjust them to meet the needs and policies of the owner.

In addition, the security configuration settings must be implemented in the system as a security feature, according to one of the system requirements, "29 Network and security configuration settings". For details, see "29 Network and security configuration settings".

Network and security configuration settings

P. 125

Document reviews

5. Security configuration guidelines		
-1. The following items are to be included.		
(1) Description of the recommended configuration settings for security capabilities		
(2) Specified default values		

6. Secure development lifecycle documents

Reg. 4.4.1(6), Part X of the Rules

This documentation shall be submitted to the Society upon request and shall describe the supplier's processes and controls in accordance with requirements for **Secure development lifecycle**. Software updates and patching shall be described. The document shall prepare **the Society for survey**.

Explanation

"Secure development lifecycle documents" is a <u>document that describes the processes and controls</u> for meeting the requirements of Secure development lifecycle. Secure development lifecycle is the lifecycle for the development and maintenance of a secure product.

For more information, see the following:

- Records how the security aspects have been addressed

According to Part X 4.5.1, system development is required to provide writing a record of how security aspects were handled at the following stages:

- (1) Requirement analysis phase
- (2) Design phase
- (3) Implementation phase
- (4) Verification phase
- (5) Release phase
- (6) Maintenance phase
- (7) End of life phase

- Processes and Controls for Secure development lifecycle

The Secure Product Development Lifecycle requirements stipulate a clear process for meeting each requirement. Therefore, the process for each requirement should be included in this document. You should also demonstrate that the system was designed and manufactured according to the process for each requirement. Therefore, the product of voucher documents such as records should also be mentioned in the process. The details of each requirement related to Secure development lifecycle are explained in detail in "Chapter 6 Explanation of Requirements for Secure development lifecycle".



Chapter 6 Explanation of Secure Development Lifecycle requirements

P. 156

- Software updates and patching

It is necessary to clarify whether software updates and adapting patches are supported. For adapting patches, it is necessary to clarify the risks of not patching. Software updates are described in detail in

"3. De	pendent component security update documentation". Adapting patches is descri	bed in detail in
"2. Sec	curity update documentation".	
	Dependent component and Operation system security update documentation	P. 163
	Security update documentation	P. 161

Document reviews

6. Secure development lifecycle documents		
-1. The following items are to be included.		
(1) Records how the security aspects have been addressed		
Recorded Documents should be prepared at the following stages:		
(a) Requirement analysis phase		
(b) Design phase		
(c) Implementation phase		
(d) Verification phase		
(e) Release phase		
(f) Maintenance phase		
(g) End of life phase		
(2) Processes and Controls for Secure development lifecycle		
See "Chapter 6 Explanation of requirements for Secure development lifecycle" for more		
information.		
(3) Software updates and patching		

7. Plans for maintenance and verification of the CBS

Reg. 4.4.1(7), Part X of the Rules

This document shall be submitted to the Society upon request and shall include procedures for security-related maintenance and testing of the system. The document shall include instructions for how the user can verify correct operation of the system's security functions as required by item No.19 "Security functionality verification" in System requirements.

Explanation

"Plans for maintenance and verification of the CBS" is a <u>document that describes the maintenance</u> and testing procedures necessary to maintain security capabilities. It provides information and instructions for system owners to maintain and test security capabilities after system operation. The clear provision of such information by the supplier enables the owner to do the appropriate work. Maintenance and testing after system operation are required to be carried out periodically in Part X, Chapter 5 (UR E26).

In addition, one of the system requirements, "19 Security functionality verification" stipulates that a function to verify the operation of security capabilities should be implemented. This function supports maintenance and testing of security capabilities. Therefore, details and usage of this function should be included in this document. More details are provided in "19 Security functionality verification".



Security functionality verification

P. 102

Document reviews

7. Plans for maintenance and verification of the CBS -1. The following items are to be included. (1) Description of recommended settings for security capabilities (2) Instructions for how the user can verify correct operation of the system's security functions The capabilities implemented by the system requirements "19 Security functionality verification" should be included.

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

Reg. 4.4.1(8), Part X of the Rules

This document shall be submitted to the Society upon request and shall include procedures or instructions allowing the user to accomplish the following:

- (1) Local independent control
- (2) Network isolation
- (3) Forensics by use of audit records
- (4) Deterministic output
- (5) Backup
- (6) Restore
- (7) Controlled shutdown, reset, roll-back and restart

Explanation

"Information supporting the owner's incident response and recovery plan" is a <u>document that</u> provides specific procedures for the system owner to respond to and recover from a cyber incident.

Details are as follows:

- Local independent control

Local independent control is control of the system directly at or near the installation site. This applies to computer systems used for remotely controlled primary or variable pitch propeller machine side controls. For applicable computer systems, procedures for moving from the network to the independent control state and operating procedures in the independent control state should be described.

- Network isolation

Network isolation is the separation of a computer system from a network. It helps prevent further growth and supports essential functions by isolating the system if security is breached. It should provide instructions for isolating the system from the network. For example, operating a physical ON/OFF switch on an embedded network device.

- Forensics by use of audit Records

This is a specific response to forensics. Forensics refers to activities that use audit records1 and

¹audit records: A single record of important security events.

audit logs¹ to investigate and analyse the causes and circumstances of important events. The purpose here is to support forensics against the system. Therefore, this document should include specific steps for forensics. For example, procedures for collecting information and analysing the cause of audit records and audit logs.

This response is supported by the ability to achieve "13. Auditable events" which is one of the requirements for security capabilities. Details are explained in detail in "13. Auditable events".

Auditable events

P. 86

- Deterministic output

Sets the output to a predetermined state when normal operation cannot be maintained due to an attack. This is supported by the ability to achieve "20. Deterministic output" which is one of the requirements for security features. The details are explained in detail in "20. Deterministic output"



Deterministic output

P. 105

- Backup

This action is used to back up important files. This action is implemented as a function that achieves one of the security function requirements, "26. System backup" The details are explained in detail in "26. System backup".



System backup

P. 118

- Restore

A known recovery and reconfiguration response after a system disruption or failure. A known protected state is one of the following:

- System parameters are set to default² or secure value.
- Security-critical patches³ are reinstalled.
- Security-related configuration are rechecked and re-established.
- System documentation and operating procedures are available.
- Application and system software is reinstalled with secure setting.
- Reconstitution from the backup data.

The purpose here is to restore and reconfigure the system to a known protected state after a disruption or failure. Therefore, this document should include procedures and instructions for restoring and reconfiguring to a known protected state.

¹ Audit log: A collection of audit records over time.

² **Default**: The standard values, conditions, and operating conditions that the system ships with.

³ Patch: A program that fixes system vulnerabilities and security defects.

Note that some of the requirements in this document may be implemented as the capability that achieves one of the security capability requirements, "27. System recovery and reconstitution" For details, see "27. System recovery and reconstitution".

System recovery and reconstitution

P. 120

- Controlled shutdown, reset, roll-back and restart

This section should describe the procedure for controlled shutdown, reset, rollback, and restart.

Controlled shutdown means to maintain in safe and known status by other connected systems performing /stopping or terminating to shut down when a computer system or network is turned off by a software function. This procedure is required because a forced shutdown can result in the loss of essential functions due to corruption of data, programs, and operating system files.

A reset is to erase the system's memory and restore it to its initial state.

A rollback is to restore the system to its previous safe state.

Rebooting is stopping the system and then restarting it immediately.

Document reviews

8. l	8. Information supporting the owner's incident response and recovery plan		
-1.	The following procedures or instructions are included.		
(1)	Local independent control		
(2)	Network isolation		
(3)	Forensics by use of audit records		
(4)	Deterministic output		
(5)	Backup		
(6)	Restore		
(7)	Controlled shutdown, reset, roll-back and restart		

9. Management of change plan

Reg. 4.4.1(9), Part X of the Rules

This document shall be submitted to the Society upon request. It is expected that this procedure is not specific for cyber security and is also required by **Chapter 3**, **Part X (UR E22)**.

Explanation

"Management of change plan" is a <u>management procedure regarding cybersecurity changes</u>. Cybersecurity changes include, for example, the application of security patches.

It is recommended that this document be integrated with the change management procedures for both hardware and software required in Part X, Chapter 3 (UR E22). The change management required in Part X, Chapter 3 (UR E22) is set forth in Part X, Chapter 3.6.

Document reviews

9. Management of change plan

-1. Cybersecurity change management procedures are included. This does not apply if the change management procedures required by Part X, Chapter 3 (UR E22) have been submitted.

10. Test reports

Reg. 4.4.1(10), Part X of the Rules

CBSs with Type approval certificate covering the security capabilities of Chapter 4, Part X (UR E27) may be exempted from survey by the Society. However, test reports signed by the supplier shall be submitted to the Society, demonstrating that the supplier has completed design, construction, testing, configuration, and hardening as would otherwise be verified by the Society in survey.

Explanation

"Test reports" is <u>documents that demonstrate that the supplier has completed the design, manufacture, testing, setup and enhancement of the product.</u> If a computer system has a certificate of approval for use, this document can be submitted to the Society, thereby omitting part of the materials submitted to the Society and the surveys. Refer to "Chapter 2 Approval Process" for the process of individual product approval when a certificate of approval for use is provided.



Chapter 2 Approval process

P. 5

Details are as follows:

4		
	r	
ч		,
	•	_

Test	Date	Result	Attachment	Date
General survey items				Company
Test of security capabilities				Department
Correct configuration of security				Name
capabilities				Name
Secure development lifecycle				Simmature.
Hardening at installation				Signature

1 Test report columns

(1) to (4) are the test items for the on-site inspection required by Part X 2.2.3 (Guideline 4). (5) is the hardening at the time of installation. Here, the hardening must be done according to the guidelines specified in the Enhanced Security Guidelines. The details of the Enhanced Security Guidelines are explained in detail below.



Security hardening guidelines

P. 171

Tests from (1) through (5) are recorded for test dates and results. In addition, please submit supporting documents that substantiate the test results. (Examples: test methods for security

capabilities, hardening practice records, etc.)

2 Signature from the supplier

Test results must be signed by the supplier. When all tests have been completed, please sign with the date, company name, department name and full name.

Document reviews

10. Test reports
-1. The following survey items are to be included.
(1) General survey items
(2) Test of security capabilities
(3) Correct configuration of security capabilities
(4) Secure development lifecycle
(5) Hardening at installation
-2. A signature from the supplier is to be included.

Chapter 4 Explanation of Surveys

This chapter describes the requirements related to surveys specified in Chapter 4, Part X (UR E27).

Overview of Surveys

Requirements

Chapter 4, Part X (UR E27) specifies requirements for four survey items as on-site surveys for computer system cybersecurity. Each item is as follows.

AA	Required survey items	
	1. General survey items	P. 41
	2. Test of security capabilities	P. 43
	3. Correct configuration of security capabilities	P. 44
	4. Secure development lifecycle	P. 46

Prepared documentation

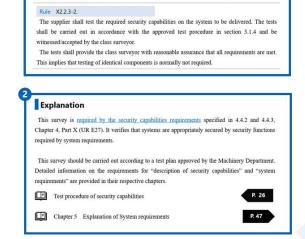
The following are some of the documents that are required to be approved for survey. Applicants should submit the following materials along with their survey applications.

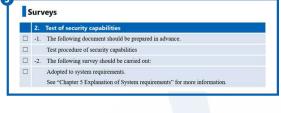
Documents required for surveys
CBS asset inventory
Topology diagrams
Description of security capabilities
Test procedure of security capabilities
Secure product development lifecycle documents

Detail of Surveys

2. Test of security capabilities

How to read the following pages





1 Requirement

The names and the details of the survey requirements.

2 Explanation

An explanation of surveys.

3 Surveys

A survey checklist for the requirements

1. General survey items

Reg. 2.2.3-1., Part X of the Rules

The supplier shall demonstrate that design, construction, and internal testing has been completed.

It shall also be demonstrated that the system to be delivered is correctly represented by the approved documentation. This shall be done by inspecting the system and comparing the components and arrangement/architecture with **CBS asset inventory** and **Topology diagrams**.

Explanation

This survey item <u>verifies that the system was correctly manufactured.</u> It involves document verification and visual inspections to confirm that systems are completed according to approved processes.

The details of this survey are as follows.

- Document Verification

Review records indicating that design, manufacture, and internal tests have been completed.

- Visual Inspection

Review system components and deployment/configuration using CBS asset inventory and topology diagrams.

See "Chapter 3 Documentation" for more information about CBS asset inventory and topology diagrams.

CBS asset inventory	P. 20
Topology diagrams	P. 22

Surveys

1. General survey items
-1. The following documents should be prepared in advance.
(1) CBS Asset Inventory
(2) Topology Diagrams
-2. The following inspections should be performed:
(1) Document Verification
(a) Record indicating completion of the design
(b) Record indicating completion of manufacturing

(c) Record indicating completion of internal testing
(2) Visual Inspection
(a) System configuration
Comparison with computer system asset inventory and topology diagram

2. Test of security capabilities

Reg. 2.2.3-2., Part X of the Rules

The supplier shall test the required security capabilities on the system to be delivered. The tests shall be carried out in accordance with the approved test procedure in section 3.1.4 and be witnessed/accepted by the class surveyor.

The tests shall provide the class surveyor with reasonable assurance that all requirements are met. This implies that testing of identical components is normally not required.

Explanation

This survey is <u>required by the security capabilities requirements</u> specified in 4.4.2 and 4.4.3, Chapter 4, Part X (UR E27). It verifies that systems are appropriately secured by security functions required by system requirements.

This survey should be carried out according to a test plan approved by the Machinery Department. Detailed information on the requirements for "description of security capabilities" and "system requirements" are provided in their respective chapters.

Test procedure of security capabilities

P. 26

Chapter 5 Explanation of System requirements

P. 47

Surveys

2. 1	2. Test of security capabilities	
-1.	The following document should be prepared in advance.	
	Test procedure of security capabilities	
-2.	The following survey should be carried out:	
	Adopted to system requirements.	
	See "Chapter 5 Explanation of System requirements" for more information.	

3. Correct configuration of security capabilities

Reg. 2.2.3-3., Part X of the Rules

The supplier shall test/demonstrate for the class surveyor that security settings in the system's components have been configured in accordance with the configuration guidelines in section 3.1.5. This demonstration may be carried out in conjunction with testing of the security capabilities.

The security settings shall be documented in a report, e.g. a ship-specific instance of the configuration guidelines.

Explanation

This survey <u>verifies that system components are configured according to security configuration</u> <u>guidelines.</u> A security configuration guideline is a document that describes recommended settings for the security features of a CBS. See "Security configuration guidelines" for more information.

Security configuration guidelines

P. 28

The details of this survey are as follows:

- Testing/Demonstration by Suppliers

Suppliers must demonstrate that system components are configured in accordance with established security configuration guidelines to ensure that recommended settings for security features are configured.

- Concurrent with Test of Security Capabilities

This security configuration validation is to be conducted as a Demonstration test for the functions of "Network and security configuration settings", which are shown in "Test of security capabilities". The test method is detailed in "Network and security configuration settings".

Network and security configuration settings

P. 125

- Documentation

Security settings and their validation results should be documented as reports. This is to explicitly indicate that the settings comply with guidelines so that they can be validated later. In addition, such reports should be submitted to the branch office in charge of the survey as soon as possible after the testing is completed.

Surveys

3. Correct configuration of security capabilities □ -1. The following document should be prepared in advance: □ Security Configuration Guidelines

-2.	The following survey should be carried out:
	Adopted to the requirements of network and security configuration settings.
	See "Network and security configuration settings" in the "Chapter 5 Explanation of
	System requirements" for more information.

4. Secure development lifecycle

Reg. 2.2.3-4., Part X of the Rules

The supplier shall, in accordance with documentation in section 3.1.6, demonstrate compliance with requirements for secure software development lifecycle in section 5.

Explanation

This survey is a <u>survey of the secure development lifecycle requirements</u> specified in 4.5, Chapter 4, Part X (UR E 27). It verifies that secure products are manufactured in accordance with secure development lifecycles.

This survey verifies that products are manufactured in accordance with the controlled processes specified in secure development lifecycle requirements and demonstrates that the handling of each requirement documented in management system documentation is implemented accordingly. Since management system documentation should make a record of how the requirement was met for each requirement, this survey verifies such records.

To grasp the details of each requirement, this survey refers to secure development lifecycle documents approved by the Machinery Department. See the following for more information about "secure development lifecycle documents".

Secure development lifecycle documents

P. 30

Chapter 6 Explanation of Secure Development Lifecycle requirements

P. 156

Surveys

4. Secure development lifecycle	
-1.	The following document should be prepared in advance.
	Secure product development lifecycle documents
-2.	The following survey should be carried out:
	Adopted Secure development lifecycle requirements.
	See "Chapter 6 Secure development lifecycle requirements" for more information.

Chapter 5 Explanation of System requirements

This chapter provides details on the system requirements required by Part X 4.4.2 and 4.4.3. System requirements are requirements for the security capabilities required of a CBS. Security capabilities provide a specific way to protect against threats and attacks on CBSs. By implementing security capabilities on CBSs that meet the minimum-security level requirements, cyber-attack risks for ships are reduced.

Overview of System requirements

■ What are required security capabilities

The system requirements set 6(six) foundational requirements as technical security requirements.



The foundational requirements define the system requirements to meet each objective. Each system requirement implements the <u>security functions required</u> by that requirement. In general, the required security capabilities apply to all CBSs. The required security capabilities are as follows:

Protect against casual or coincidental access by unauthenticated e	ntities
1. Human user identification and authentication	P. 53
2. Account management	P. 56
3. Identifier management	P. 59
4. Authenticator management	P. 62
5. Wireless access management	P. 65

	6. Strength of password-based authentication P. 68
	7. Authenticator feedback
	Protect against casual or coincidental misuse
	8. Authorization enforcement P. 73
	9. Wireless use control
	10. Use control for portable and mobile devices
	11. Mobile code P. 82
	12. Session lock P. 84
	13. Auditable events P. 86
	14. Audit storage capacity
	15. Response to audit processing failures P. 92
	16. Timestamps P. 94
Ĉ₽.	Protect the integrity of the CBS against casual or coincidental manipulation
	17. Communication integrity P. 96
	18. Malicious code protection
	19. Security functionality verification P. 102
	20. Deterministic output P. 105
	Prevent the unauthorized disclosure of information via eavesdropping or casual exposure
	21. Information confidentiality P. 107

	22. Use of cryptography P. 109
Q	Monitor the operation of the CBS and respond to incidents
	23. Audit log accessibility P. 111
(1)	Ensure that the control system operates reliably under normal production conditions
	24. Denial of service protection P. 113
	25. Resource management P. 115
	26. System backup P. 118
	27. System recovery and reconstitution P. 120
	28. Alternative power source P. 123
	29. Network and security configuration settings
	30. Least Functionality P. 128

■ Untrusted network Requires Additional Security capabilities

Networks that contain computer systems and that are not covered by Part X, Chapter 4 (UR E27) are called <u>untrusted networks</u>. This is a network that does not have minimum security measures in place. When network communication with untrusted networks is involved, security is to be more enhanced. Therefore, <u>additional security capabilities</u> requirements are applied.

The requirements for additional security capabilities are as follows:

Additional security capabilities	
31. Multifactor authentication for human users	P. 130
32. Software process and device identification and authentication	P. 133

33. Unsuccessful login attempts	P. 135
34. System use notification	P. 138
35. Access via Untrusted Networks	P. 141
36. Explicit access request approval	P. 143
37. Remote session termination	P. 145
38. Cryptographic integrity protection	P. 148
39. Input validation	P. 150
40. Session integrity	P. 152
41. Invalidation of session IDs after session termination	P. 154

■ If some security capabilities are not provided

If the required security capabilities cannot be provided for any reason, alternatives measures must be provided. This is called <u>compensating countermeasure</u> and may be accepted as an alternative if the following conditions are met:

- i) Protect against the same threats as the original requirement
- ii) Provide an equal level of protection as the original requirement
- iii) Not be a security control that is required by other requirements
- vi) Not introduce higher security risk

Compensating countermeasures may be exemplified in the details of each requirement. For example:

e.g., The account function cannot be implemented

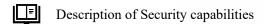
In this case, the user cannot be identified and there is a risk of being easily accessed by an attacker. Compensating countermeasures include placing them in a locked box. Locking the key allows access only to the person who owns the key and is therefore an acceptable alternative.



If the security capability is to be used as a compensating countermeasure, the countermeasure and the test procedure are to be described in the following documentation.

- Description of security capabilities

This document explains what capabilities are implemented for the requirements of each security capabilities. If the security capability is used as a compensating countermeasure, the details of this countermeasure are included. For details, see "Description of the security function".



P.24

- Test of security capabilities

This is a test procedure for demonstration tests required for each security capability. If the security capability is to be used as a compensating countermeasure, it is necessary to confirm by witness survey that this countermeasure satisfies the requirements of the security capability. Four details, see "Test of security capabilities".



Test of security capabilities

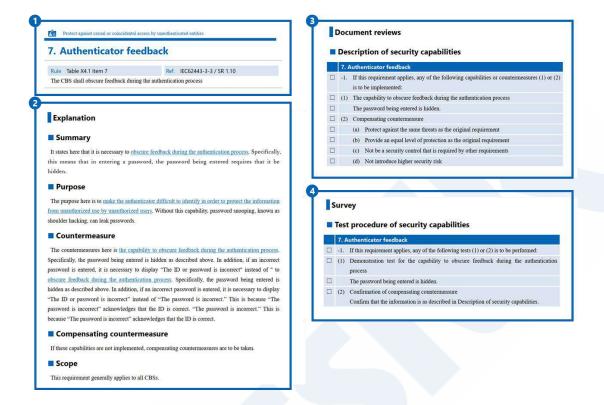
P. 43

Some security capabilities may not apply

Some system requirements may not apply to some CBSs. For example, the requirement "5. Wireless access management" is a required security capability for CBS that communicate wirelessly, so CBSs that do not communicate wirelessly are exempt. An example of the need for application is shown in the details of each requirement. If the specific system requirement is not applicable, the details are to be described in "Description of security capabilities".

Detail of System requirements

How to read the following pages



1 Requirement

The names and the details of the system requirements. The upper part of the titles indicates the basic requirements.

2 Explanation

The explanation of system requirements. It consists of the following:

- Summary: Overview of Requirements
- Purpose: Primary purpose of Requirements
- Countermeasures: Specific countermeasures of requirements
- Compensating countermeasures:
 Countermeasures taken in place of the original security capability to meet the requirement.
- Scope: Description of if the requirement applies or not

3 Document reviews

A document review checklist for system requirements

Description of security capabilities:
 Documentation required by 4.4.1 (3), Part X.

4 Surveys

A survey checklist for system requirements.

- Test procedure of security capabilities: Surveys required by 2.2.3-2., Part X.



1. Human user identification and authentication

Reg. Table X4.1 Item 1, Part X of the Rules

Ref. IEC62443-3-3 / SR 1.1

The CBS shall identify and authenticate all human users who can access the system directly or through interfaces.

Explanation

Summary

Item 1, Table X4.1, Part X states that it is necessary to <u>identify and authenticate all human users</u> who can access the system. The description for identification and authentication is as follows:

Term	Description
Identification This is to distinguish each user. This is done using an identifier that	
	who you are. In the case of identifying person, the identifier is typically the
	username.
Authentication This is to prove the identity of the user. This is done using an identifier as	
	information to prove the identity of the user called an authorization code. An
	authorization code is typically a password.

This means that you should use an identifier and an authorization code to log in to the system.

Purpose

The purpose is to <u>reduce the risk of being used by people who are not authorized to use the system.</u>
If the system does not identify and authenticate, an attacker can access without authorization. This could affect the operation of the vessel.

Countermeasures

These countermeasures here are <u>the capability that identify and authenticate all users (human user)</u>. Specifically, they are as follows:

- Account functions

A combination of an identifier and an authenticator is called an account and is used to identify and authenticate users. Users of the system must be able to log in to the system through this function. Identifiers, authenticators, and accounts are described in detail in the respective requirements.

Account management	P. 56	
Identifier management	P. 59	
Authenticator management	P. 62	

Compensating countermeasures

Compensating countermeasures should be adopted in cases where the aforementioned capabilities or countermeasures have not been implemented. The following is an example of a compensating countermeasure.

· Physical security measures

Instead of implementing identification and authentication as a function, you can complement this function by restricting physical access. For example, you might have a structure in which the system cannot be operated without a key controlled by predetermined personnel. In this case, it is important that the identification and authentication of each person is not necessary, and that the authority of each user is examined. The authority is explained in detail in "8. Authorization enforcement".

Authorization enforcement

P. 73

Scope

This requirement, in principle, applies to all CBSs.

Document reviews

Description of security capabilities

	1. Human user identification and authentication		
	-1.	this requirement applies, either of the following (1) or (2) is to be	implemented.
	(1)	apability to identify and authenticate users(person)	
) identifying by an identifier.	
		authenticating by an identifier and an authenticator.	
	(2)	ompensating countermeasure	
) Protect against the same threats as the original requirement	
) Provide an equal level of protection as the original requirement	
) Not be a security control that is required by other requirements	
) Not introduce higher security risk	

Surveys

■ Test procedure of security capabilities

1. F	1. Human user identification and authentication	
-1.	If this requirement applies, either of the following (1) or (2) is to be performed.	
(1)	Demonstration test for the capability of Human user identification and authentication	
	(a) Can log in with a valid identifier and authenticator	
	(b) Cannot log in with an invalid identifier and authenticator	
(2)	Confirmation of compensating countermeasure	
	Confirm that the information is as described in Description of security capabilities.	



2. Account management

Reg. Table X4.1 Item 2, Part X of the Rules

Ref. IEC62443-3-3 / SR 1.3

The CBS shall provide the capability to support the management of all accounts by authorized users, including adding, activating, modifying, disabling and removing account

Explanation

Summary

Item 2, Table X4.1, Part X states that it is necessary to <u>manage all accounts</u>. An account is used to identify and authenticate a user and consists of an identifier¹ and an authenticator². Identification and authentication are explained in detail in "1. Human user identification and authentication".



Human user identification and authentication

P. 53

In addition, the user subject to this requirement is basically only a person. However, in addition to People, Software Processes and Devices are also covered if the following conditions are met:

- Wireless communication
- Network communication with an untrusted network

Wireless communication is described in detail in "5. Wireless access management" and network communication with an untrusted network is described in "32. Software process and device identification and authentication".



Wireless access management

P. 76



Software process and device identification and authentication

P. 133

Purpose

The purpose is to <u>properly manage users of the system</u>. Improper management can result in unauthorized access by someone who does not have permission to use it.

Countermeasures

The countermeasure described here is to support the management of all accounts by authorized

^{1.} **Identifier** An indication what it is such as user ID, etc.

^{2.} Authenticator information used to prove the identity of the user itself such as password, etc.

users (Including adding, enabling, modifying, disabling and deleting accounts). This capability should be restricted to use only by people with administrative privileges (administrators).

Compensating countermeasures

Compensating countermeasures should be adopted in cases where the aforementioned capabilities or countermeasures have not been implemented. If account activation and deactivation is not implemented, it should be noted that it will be supplemented by additions and deletions.

Scope

This requirement does not apply to the following cases:

- In the case that the capability of "1. Human user identification and authentication" is as a compensating countermeasure or the requirement is not applicable.

If the capability to identify and authenticate the user is not implemented, there is no capability of the account. In this case, this requirement is not applicable.

Document reviews

Description of security capabilities

2. Account management		
-1.	If th	is requirement applies, either of the following (1) or (2) is to be implemented.
(1)	The	capability to support the management of all accounts by authorized users
	(a)	The following capabilities should be implemented.
		i) Adding, modifying and removing account
		ii) Activating and disabling account (In case compensating countermeasures are
		taken, the reasons shall be provided)
	(b)	Only authorized users can manage account.
(2)	Con	npensating countermeasure
	(a)	Protect against the same threats as the original requirement
	(b)	Provide an equal level of protection as the original requirement
	(c)	Not be a security control that is required by other requirements
	(d)	Not introduce higher security risk

Surveys

■ Test procedure of security capabilities

2. Account management

-1.	If this	s requirement applies, either of the following (1) or (2) is to be performed.	
(1)	Demonstration test for the capability to support the management of all accounts by		
	autho	orized users	
	(a)	The following capabilities should be implemented:	
		i) Adding, modifying and removing account	
		ii) Activating and disabling account	
	(b)	Account management permissions should be as follows:	
		i) Only authorized users can manage account.	
		ii) Unauthorized users cannot manage account.	
(2)	Conf	irmation of compensating countermeasure	
	Conf	irm that the information is as described in Description of security capabilities.	



3. Identifier management

Reg. Table X4.1 Item 3, Part X of the Rules

Ref. IEC62443-3-3 / SR 1.4

The CBS shall provide the capability to support the management of identifiers by user, group and role.

Explanation

Summary

Item 3, Table X4.1, Part X states that it is necessary to manage identifiers by user, group, and role. An identifier is a representation of who you are. In the identification of a person, a username is generally used.

In addition, the user subject to this requirement is basically only a human user. However, if the following conditions are met, a software process and a device are also targeted besides to a human user.

- Wireless communication
- Network communication with an untrusted network

Wireless communication is described in detail in "5. Wireless access management," and network communication with an untrusted network is described in "32. Software process and device identification and authentication"

Wireless access management

P. 76

Software process and device identification and authentication

P. 133

Purpose

The purpose is to manage identifiers by user, group, and role in accordance with the requirement.

Countermeasures

The countermeasure described here is to support the management of identifiers by user, group and role. Specifically, it is as follows.

Capability to create group accounts

A group account is a group of accounts organized by groups and roles. An example of an account might be following:

- Officer and Engineer
- System User and Maintenance Engineer
- System Administrator and User

Compensating countermeasures

Compensating countermeasures should be adopted in cases where the aforementioned capabilities or countermeasures have not been implemented.

Scope

This requirement does not apply to the following cases:

- In the case that the capability of "1. Human user identification and authentication" is as a compensating countermeasure or the requirement is not applicable.

If the capability to identify and authenticate the user is not implemented, there is no capability of the account. In this case, this requirement is not applicable.

Human user identification and authentication

P. 53

Document reviews

Description of security capabilities

3. Identifier management		
-1.	If this requirement applies, either of the following (1) or (2) is to be implemented.	
(1)	The capability to support the management of identifiers by user, group and role	
Add, modifying and remove identifiers		
(2)	Compensating countermeasure	
	(a) Protect against the same threats as the original requirement	
	(b) Provide an equal level of protection as the original requirement	
	(c) Not be a security control that is required by other requirements	
	(d) Not introduce higher security risk	

Surveys

■ Test procedure of security capabilities

3. Identifier management		
-1.	If this requirement applies, either of the following (1) or (2) is to be performed.	
(1)	Demonstration test for the capability to support the management of identifiers by user,	
	group and role	
	Add, modifying and remove identifiers	
(2)	Confirmation of compensating countermeasure	
	Confirm that the information is as described in Description of security capabilities.	



4. Authenticator management

Reg. Table X4.1 Item 4, Part X of the Rules

Ref. IEC62443-3-3 / SR 1.5

The CBS shall provide the capability to:

- Initialize authenticator content
- Change all default authenticators upon control system installation
- Change/refresh all authenticators
- Protect all authenticators from unauthorized disclosure and modification when stored and transmitted.

Explanation

Summary

Item 4, Table X4.1, Part X states that it is necessary to manage the authenticator. The authenticator is information that allows you to prove your identity. Authenticator mainly include passwords, PINs¹, tokens², public key authentication methods³, physical keys⁴, fingerprint authentication, and facial authentication. There are three types of authentication factors below, and you can use one (or a combination) of them to authenticate.

In addition, the user subject to this requirement is basically only a human user. However, if the following conditions are met, a software process and a device are also targeted besides to a human user.

- Wireless communication
- Network communication with an untrusted network

Wireless communication is described in detail in "5. Wireless access management," and network communication with an untrusted network is described in "32. Software process and device identification and authentication"

Wireless access management

P. 76

Software process and device identification and authentication

P. 133

¹ PIN It stands for Personal Identification Number. One of the authentication codes. Usually consists of 4 to 6 digits

² Security token One of the authorization codes. Generally, serves as a temporary certificate for users to access the system. For example, one-time password (OTP) generation device.

³ Public key authentication method: A method of authentication using a pair of public and private keys.

⁴ **Physical key** One of authentication codes. A key to unlock the physical lock such as safe and system.

Purpose

The purpose is to <u>ensure the confidentiality of the authenticator</u>. Leaking the authenticator could allow it to be misused by an attacker. This could affect the operation of the vessel.

Countermeasures

The countermeasure described here is the capability to manage authenticator. Using passwords as an example, specifically as follows:

- Initialize authenticator content

For example, initializing a password. If the authenticator is lost, a new authenticator can be set.

- Change all default authenticators upon control system installation

For example, changing from the initial password. This can mitigate potential security risks if the initial authenticator is predictable or widely available.

- Change/refresh all authenticators

For example, change of the password. It can change the code at any time.

- Protect all authenticators from unauthorized disclosure and modification when stored and transmitted.

For example, password encryption. It can protect sensitive information.

Note: If a password is used as the authenticator, requirements regarding its strength are stipulated in "6 Strength of password-based authentication".



6. Strength of password-based authentication

P. 68

Compensating countermeasures

Compensating countermeasures should be adopted in cases where the aforementioned capabilities or countermeasures have not been implemented.

Scope

This requirement does not apply to the following cases:

- In the case that the capability of "1. Human user identification and authentication" is as a compensating countermeasure or the requirement is not applicable.

If the capability to identify and authenticate the user is not implemented, there is no capability of the account. In this case, this requirement is not applicable.

Human user identification and authentication

P. 53

Document reviews

Description of security capabilities

4. Authenticator management		
-1.	If this requirement applies, either of the following (1) or (2) is to be implemented.	
(1)	The capability to manage authenticators	
	The following capabilities should be implemented.	
	(a) Initialize authenticator content (e.g., initializing a password)	
	(b) Change all default authenticators upon control system installation (e.g., changing	
	from the initial password)	
	(c) Change/refresh all authenticators (e.g., changing of the password)	
	(d) Protect all authenticators from unauthorized disclosure and modification when stored	
	and transmitted. (e.g., password encryption)	
(2)	Compensating countermeasure	
	(a) Protect against the same threats as the original requirement	
	(b) Provide an equal level of protection as the original requirement	
	(c) Not be a security control that is required by other requirements	
	(d) Not introduce higher security risk	

Surveys

■ Test procedure of security capabilities

4. Authenticator management		
-1.	If th	is requirement applies, either of the following (1) or (2) is to be performed.
(1)	(1) Demonstration test for the capability to manage authenticators	
	The	following capabilities should be implemented.
	(a)	Initialize authenticator content (e.g., initializing a password)
	(b)	Change all default authenticators upon control system installation (e.g., changing
		from the initial password)
	(c)	Change/refresh all authenticators (e.g., changing of the password)
	(d)	Protect all authenticators from unauthorized disclosure and modification when stored
		and transmitted. (e.g., password encryption)
(2)	Con	firmation of compensating countermeasure
	Con	firm that the information is as described in Description of security capabilities.



5. Wireless access management

Reg. Table X4.1 Item 5, Part X of the Rules

Ref. IEC62443-3-3 / SR 1.6

The CBS shall provide the capability to identify and authenticate all users (humans, software processes or devices) engaged in wireless communication

Explanation

Summary

Item 5, Table X4.1, Part X states that the user who communicates wirelessly is necessary to be identified and authenticated. In the case of wireless communications, the identification and authentication of the user is not only about the person, but also about the software process and device. Software processes and devices are described below.

Term	Description
Software Process	A program or application used by the system.
Device	A physical hardware or An equipment that uses the system.

Purpose

The purpose is to enhance security under wireless communications where there is a risk of cyber-attacks. The major difference between wireless and wired communications is that an attacker can easily access a network remotely within range of radio waves. In the case of wired communications, physical measures such as closing ports and managing entry and exit are also effective. However, these measures are not effective for wireless communications. Therefore, it is necessary to provide identification and authentication functions that can be used under wireless connections so that only authorized users can access them.

Countermeasures

The countermeasure described here is the capability to identify and authenticate a human user, software process, or device that engaged in wireless communication. Specifically, it is as follows.

- IEEE802.1X

This is a standard for authenticating network terminals. Ensure the security of wireless connections by identifying and authenticating users with an authentication server such as RADIUS.

Compensating countermeasures

Compensating countermeasures should be adopted in cases where the aforementioned capabilities or countermeasures have not been implemented.

Scope

This requirement does not apply to the following cases:

- CBS does not communicate wirelessly

If the CBS does not communicate wirelessly, this requirement does not apply.

Document reviews

Description of security capabilities

5. Wireless access management		
-1.	If th	nis requirement applies, either of the following (1) or (2) is to be implemented.
(1)	The	capability to identify and authenticate all users (humans, software processes or
	dev	ices) engaged in wireless communication
	(a)	Human user identification and authentication
		i) identifying by an identifier.
		ii) authenticating by an identifier and an authenticator.
	(b)	Software process identification and authentication
		i) identifying by an identifier.
		ii) authenticating by an identifier and an authenticator.
	(c)	Device identification and authentication
		i) identifying by an identifier.
		ii) authenticating by an identifier and an authenticator.
(2)	Con	npensating countermeasure
	(a)	Protect against the same threats as the original requirement
	(b)	Provide an equal level of protection as the original requirement
	(c)	Not be a security control that is required by other requirements
	(d)	Not introduce higher security risk

Surveys

■ Test procedure of security capabilities

5. Wireless access management

-1.	If th	is re	quirement applies, either of the following (1) or (2) is to be performed.
(1)	(1) Demonstration test for the capability to identify and authenticate all users (humans,		
	soft	ware	processes or devices) engaged in wireless communication
	(a)	Hu	man user identification and authentication
		i)	Can log in with a valid identifier and authenticator
		ii)	Cannot log in with an invalid identifier and authenticator
	(b)	Sof	tware process identification and authentication
		i)	Can log in with a valid identifier and authenticator
		ii)	Cannot log in with an invalid identifier and authenticator
	(c)	Dev	vice identification and authentication
		i)	Can log in with a valid identifier and authenticator
		ii)	Cannot log in with an invalid identifier and authenticator
(2)	Cor	ıfirm	ation of compensating countermeasure
	Cor	ıfirm	that the information is as described in Description of security capabilities.



6. Strength of password-based authentication

Reg. Table X4.1 Item 6, Part X of the Rules

Ref. IEC62443-3-3 / SR 1.7

The CBS shall provide the capability to enforce configurable password strength based on minimum length and variety of character types.

Explanation

Summary

Item 6, Table X4.1, Part X states that it is necessary to <u>enforce configurable password strength</u> <u>based on minimum length and variety of character types</u>. This means that passwords are not to be too short and to be configurable with a variety of characters.

Purpose

The purpose is to <u>make it harder for an attacker to guess the password.</u> For example, if a password consists of only 4(four) digits, it is less strong and more likely to be easily guessed.

Countermeasures

The countermeasure described here is the capability to enforce configurable password strength. Specifically, the minimum password length and character type should be strengthened to make them appropriate for the system. Some helpful guidelines are following:

- NIST1 SP800-63

Length: At least 8 characters (for user-created passwords)

Type: ASCII (REF 20) characters. Spaces. Unicode (ISO/OSC10646) characters, etc.

Compensating countermeasures

Compensating countermeasures should be adopted in cases where the aforementioned capabilities or countermeasures have not been implemented. The following is an example of a compensating countermeasure.

- Multi-factor authentication

Two or more authentication methods can complement the function of this requirement by increasing the strength of the authentication. Multi-factor authentication is described in detail in "31. Multifactor authentication for human users".

¹ **NIST** It stands for National Institute of Standards and Technology.



Scope

This requirement does not apply to the following cases:

- Password is not used for an authenticator.

When the password is not used for an authenticator, this requirement is not applicable.

Document reviews

Description of security capabilities

6. S	tren	gth of password-based authentication
-1.	If th	is requirement applies, either of the following (1) or (2) is to be implemented.
(1)	The	capability to enforce configurable password strength
	(a)	Minimum length
		The decision was made based on the guidelines set forth in the countermeasures.
	(b)	Variety of character types
		The decision was made based on the guidelines set forth in the countermeasures.
(2)	Con	npensating countermeasure
	(a)	Protect against the same threats as the original requirement
	(b)	Provide an equal level of protection as the original requirement
	(c)	Not be a security control that is required by other requirements
	(d)	Not introduce higher security risk

Surveys

6. Strength of password-based authentication	
-1. If this requirement applies, either of the following (1) or (2) is to be performed.	
(1) Demonstration test for the capability to enforce configurable password strength	
(a) Minimum length	
Adopted to the following items:	
i) A password can be set that is not less than the determined minimum length:	
ii) A password cannot be set that is less than the determined minimum length:	

(b) Variety of character types
A password can be set for the determined character types.
(2) Confirmation of compensating countermeasure
Confirm that the information is as described in Description of security capabilities.



7. Authenticator feedback

Reg. Table X4.1 Item 7, Part X of the Rules

Ref. IEC62443-3-3 / SR 1.10

The CBS shall obscure feedback during the authentication process

Explanation

Summary

Item 7, Table X4.1, Part X states that it is necessary to <u>obscure feedback during the authentication</u> <u>process</u>. Specifically, this means that in entering a password, the password being entered requires that it be hidden.

Purpose

The purpose is to <u>make the authenticator difficult to identify in order to protect the information</u> <u>from unauthorized use by unauthorized users</u>. Without this capability, password snooping, known as shoulder hacking, can leak passwords.

Countermeasures

The countermeasure described here is the capability to obscure feedback during the authentication process. Specifically, the password being entered is hidden as described above. In addition, if an incorrect password is entered, it is necessary to display "The ID or password is incorrect" instead of "The password is incorrect." This is because "The password is incorrect" acknowledges that the ID is correct.

Compensating countermeasures

Compensating countermeasures should be adopted in cases where the aforementioned capabilities or countermeasures have not been implemented.

Scope

This requirement, in principle, applies to all CBSs.

Document reviews

Description of security capabilities

7. A	7. Authenticator feedback		
-1.	If this requirement applies, either of the following (1) or (2) is to be implemented.		
(1)	The capability to obscure feedback during the authentication process		
	The password being entered is hidden.		
(2)	Compensating countermeasure		
	(a) Protect against the same threats as the original requirement		
	(b) Provide an equal level of protection as the original requirement		
	(c) Not be a security control that is required by other requirements		
	(d) Not introduce higher security risk		

Surveys

7. <i>A</i>	7. Authenticator feedback		
-1.	If this requirement applies, either of the following (1) or (2) is to be performed.		
(1)	Demonstration test for the capability to obscure feedback during the authentication		
	process		
	The password being entered is hidden.		
(2)	Confirmation of compensating countermeasure		
	Confirm that the information is as described in Description of security capabilities.		



8. Authorization enforcement

Reg. Table X4.1 Item 8, Part X of the Rules

Ref. IEC62443-3-3 / SR 2.1

On all interfaces, human users shall be assigned authorizations in accordance with the principles of segregation of duties and least privilege.

Explanation

Summary

Item 8, Table X4.1, Part X states that it is to <u>be assigned authorizations in accordance with two important principles of "segregation of duties" and "least privilege"</u>. Separation of duties and least privilege are described below.

Term	Description
Separation of duties	The principle of separating one important task into two or more people and
	preventing one person from having all the power. This can be separated by
	roles and groups as well as individuals. For example, separating the person
	responsible for the work from the approver.
Least Privilege	The principle that an employer (person) has only the minimum authority
	necessary to perform his/her duties. Specifically, an administrator can
	configure the system, add users, and so on, while a general user is only
	allowed to operate the system.

Therefore, it is necessary to clearly define the role of the human user or the human user, assign appropriate permissions, and restrict the human user to allow only authorized operations.

Purpose

The purpose is to properly assign privileges to users.

Countermeasures

The countermeasure described here is the capability to support the assignment of privileges according to the separation of duties and the principle of least privilege. Specifically, it is as follows.

- Managing Permissions with Access Control Lists

Access control lists control access to system resources (such as files and databases). An access control list consists of the following elements:

Elements	Description
Subject	The human user who has been granted access. This applies to all human users,
	including group-based users.
Object	The resource that has been granted access. Examples include files, databases, and
	network resources.
Permission	The operation for which access was granted. For example, read, write, and
	execute.

Compensating countermeasures

Compensating countermeasures should be adopted in cases where the aforementioned capabilities or countermeasures have not been implemented. The following is an example of a compensating countermeasure.

- Physical security

If compensating countermeasure is taken for the capability of "1. Identification and authentication of user (person)", this capability cannot be implemented in the system. In such cases, it is necessary to supplement this capability through physical security or other means. For example, in the case of authorization of system users and maintenance users, maintenance can be performed by the key held only by the maintenance users.



Human user identification and authentication

P. 53

Scope

This requirement, in principle, applies to all CBSs.

Document reviews

Description of security capabilities

8. Authorization enforcement		
-1. If this requirement applies, either of the following (1) or (2) is to be implemented.		
(1) The capability to support the assignment of privileges according to the separation of duties		
and the principle of least privilege		
The following elements are to be controlled by access control lists or other means.		
(a) Subject (e.g., all users, including groups)		
(b) Object (e.g., files, databases, network resources)		

	(c)	Permissions (e.g., read, write, execute)
(2)	Con	npensating countermeasure
	(a)	Protect against the same threats as the original requirement
	(b)	Provide an equal level of protection as the original requirement
	(c)	Not be a security control that is required by other requirements
	(d)	Not introduce higher security risk

Surveys

8. Authorization enforcement		
-1.	If this requirement applies, either of the following (1) or (2) is to be performed.	
(1)	The Demonstration test for the capability to support the assignment of privileges	
	according to the separation of duties and the principle of least privilege	
	The following elements are to be managed in accordance with the principles of	
	segregation of duties and least privilege by means of access control lists, etc.	
	(a) Subject (e.g., all users, including groups)	
	(b) Object (e.g., files, databases, network resources)	
	(c) Permissions (e.g., read, write, execute)	
(2)	Confirmation of compensating countermeasure	
	Confirm that the information is as described in Description of security capabilities.	



9. Wireless use control

Reg. Table X4.1 Item 9, Part X of the Rules

Ref. IEC62443-3-3 / SR 2.2

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

Explanation

Summary

Item 9, Table X4.1, Part X states that it is to <u>authorize</u>, <u>monitor</u> and <u>enforce usage restrictions for</u> <u>wireless connectivity to the system according to commonly accepted security industry practices</u>. "Commonly accepted security industry practices" is generally used wireless communication technologies. Examples include Wi-Fi and Bluetooth. Authorization, monitoring, and restrictions on the use of wireless connections are as follows.

Capability	Description
Authorization	The process of granting or denying access to a specific resource or feature. This
	typically occurs after authentication and controls what users can access or perform.
Monitoring	Monitoring devices that are connected wirelessly.
Usage	Usage restrictions on devices that can be connected wirelessly.
restrictions	

Purpose

The purpose is to <u>provide greater security for use under wireless communications</u>, where the <u>risk of cyberattacks is high.</u> Without adequate security measures in place, an attacker could connect to the affected access point and be attacked.

Countermeasures

The countermeasure described here is that the capability to authorize, monitor and enforce usage restrictions for wireless connectivity to the system. The example below describes the case of WPA2-PSK authentication¹.

- Authorization

¹ WPA2-PSK Authentication: An authentication method that secures access under wireless communication using a pre-shared key.

This allows or denies access to a specific resource for each user. Control access to the network by authenticating with SSID (Service Set Identifier) and encryption key.

- Monitoring

This monitors wirelessly connected devices. You can check the list of connected devices by using the Windows PC screen, etc. Note that the connected devices are identified by their MAC addresses. A MAC address is a physical address that is unique to a device.

- Usage Restrictions

This restricts usage of devices that can be connected wirelessly. A function called MAC address filtering restricts access to the network for devices with a specific MAC address.

Compensating countermeasures

Compensating countermeasures should be adopted in cases where the aforementioned capabilities or countermeasures have not been implemented.

Scope

This requirement does not apply to the following cases:

- Without wireless communication

This requirement does not apply if the CBS does not have wireless communication technology and is not an access point.

Document reviews

Description of security capabilities

9. V	9. Wireless use control	
-1.	If this requirement applies, either of the following (1) or (2) is to be implemented.	
(1)	The capability to authorize, monitor and enforce usage restrictions for wireless	
	connectivity to the system	
	(a) The following functions are implemented in accordance with generally accepted	
	industry security practices	
	i) Authorization	
	ii) Monitoring	
	iii) Usage restrictions	
(2)	Compensating countermeasure	
	(a) Protect against the same threats as the original requirement	
	(b) Provide an equal level of protection as the original requirement	
	(c) Not be a security control that is required by other requirements	
	(d) Not introduce higher security risk	

Surveys

9. Wireless use control	
-1. If this requirement applies, either of the following (1) or (2) is to be performed.	
(1) Demonstration test for the capabilities to authorize, monitor, and usage restrict of wireless	
connections to the system	
The following items are to be satisfied.	
(a) The SSID and encryption key setting status can be checked on the configuration	
screen, etc.	
(b) SSID and encryption key settings for testing are available.	
(c) The list of connected devices is available on the connected Windows PC's screen, etc.	
And the MAC addresses are available.	
(d) If there is a usage restriction function (e.g., MAC address), only authorized devices	
can be connected.	
(2) Confirmation of compensating countermeasure	
Confirm that the information is as described in Description of security capabilities.	



10. Use control for portable and mobile devices

Reg. Table X4.1 Item 10, Part X of the Rules

Ref. IEC62443-3-3 / SR 2.3

When the CBS supports use of portable and mobile devices, the system shall include the capability

- 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

Explanation

Summary

Item 10, Table X4.1, Part X states that it is necessary to <u>control for portable and mobile devices</u> when the CBS connects to <u>devices</u>. Portable and mobile devices are devices that can be carried around. Examples include USB flash drives, smartphones, tablets, and laptops.

Purpose

The purpose is to <u>reduce the risk of malware infection through portable or mobile devices</u>. Malware infection from devices should be protected as a security feature of the system, not just the device itself.

Countermeasures

The countermeasure described here is that the capability to restrict the usage and transfer of portable and mobile devices. The details are as follows.

- Usage Restrictions

Limits the connection to only authorized devices.

- Transfer Restrictions

Restricts the transfer of code and data between a system and a device.

Compensating countermeasures

Compensating countermeasures should be adopted in cases where the aforementioned capabilities or countermeasures have not been implemented. The following is an example of a compensating countermeasure.

- Block a port with a blocker

A blocker is a physical security tool that physically blocks a computer's USB port or LAN port by plugging it into the computer. Blocking a port with a blocker complements this feature to prevent the

use of portable and mobile devices.

- Clean up of portable and mobile devices

Before using portable and mobile devices, you can complement this function by using specialized hardware to scan and clean up malware.

Scope

This requirement does not apply to the following cases:

- Not Supporting the Use of portable and mobile devices

If the use of portable and mobile devices is not supported, this requirement does not apply.

Document reviews

Description of security capabilities

10.	10. Use control for portable and mobile devices	
-1.	-1. If this requirement applies, either of the following (1) or (2) is to be implemented.	
(1)	Cap	abilities for restricting the use of portable and mobile devices and restricting data
	tran	smission
	(a)	Restrictions on the use of portable and handheld devices
		Only authorized devices are permitted to be used
	(b)	Restrictions on data transfer for portable and mobile devices
		The transfer of device codes and data are to be restricted
(2)	Con	npensating countermeasure
	(a)	Protect against the same threats as the original requirement
	(b)	Provide an equal level of protection as the original requirement
	(c)	Not be a security control that is required by other requirements
	(d)	Not introduce higher security risk

Surveys

10. Use control for portable and mobile devices	
-1. If this requirement applies, either of the following (1) or (2) is to be performed.	
(1) Demonstration test for the capabilities of use limitation and data transfer limitation for	
portable and handheld devices	
(a) Restriction of use of portable and mobile devices.	

The following shall be complied with
i) Authorized devices can be used.
ii) Unauthorized devices cannot be used.
(b) Unauthorized devices cannot be used.
The transfer of device codes and data are to be restricted
(2) Confirmation of compensating countermeasure
Confirm that the information is as described in Description of security capabilities.



11. Mobile code

Reg. Table X4.1 Item 11, Part X of the Rules

Ref. IEC62443-3-3 / SR 2.4

The CBS shall control the use of mobile code such as java scripts, ActiveX and PDF.

Explanation

Summary

Item 11, Table X4.1, Part X states that the use of mobile code is to be controlled. Mobile code is a program that is downloaded from another computer system via a network and automatically executed without the user having to explicitly download, install or otherwise operate it.

Purpose

The purpose is to <u>prevent security risks from the automatic execution of mobile code</u>. This section aims to prevent security risks from the automatic execution of mobile code. Some malwares can exploit the mechanism of mobile code and apply it to infect viruses, unauthorized operations or tampering. To prevent them, mobile codes are to be restricted.

Countermeasures

The countermeasure described here is the ability to control the use of mobile code. For example, removing the browser or prohibiting the operation of mobile code by setting a policy.

Compensating countermeasures

Compensating countermeasures should be adopted in cases where the aforementioned capabilities or countermeasures have not been implemented.

Scope

This requirement does not apply to the following cases:

- No web access (client) functionality

If a generic operating system (generic OS) such as Windows is not used, there is generally no web access (client) function. If there is no web access, the mobile code is not automatically downloaded. In such cases, this requirement does not apply.

Document reviews

Description of security capabilities

11. Mobile code	
-1. If this requirement applies, either of the following (1) or (2)	is to be implemented.
(1) The capability to control the use of mobile codes	
(a) Capability to control the use of mobile codes (e.g., rem	nove browsers, prohibit mobile
code behaviour in policy settings).	
(2) Compensating countermeasure	
(a) Protect against the same threats as the original requirer	nent
(b) Provide an equal level of protection as the original requ	uirement
(c) Not be a security control that is required by other requi	rements
(d) Not introduce higher security risk	

Surveys

11. Mobile code		
-1.	If this requirement applies, either of the following (1) or (2) is to be implemented.	
(1)	The Demonstration test for the capability to control the use of mobile codes	
	(a) Control the use of mobile codes (e.g., remove browsers, prohibit mobile code	
	behaviour in policy settings).	
(2)	Confirmation of compensating countermeasure	
	Confirm that the information is as described in Description of security capabilities.	



12. Session lock

Reg. Table X4.1 Item 12, Part X of the Rules

Ref. IEC62443-3-3 / SR 2.5

The CBS shall be able to prevent further access after a configurable time of inactivity or following activation of manual session lock.

Explanation

Summary

Item 12, Table X4.1, Part X states that <u>a capability of session lock</u>, <u>either automatic or manual</u>, is to be provided. **Session** is the series of operations from the time users log into the system until they log out. Locking a session when the system has not been operated for a certain period is called session lock. **Session lock** is the locking of a session when the system is inactive for a certain period.

Purpose

The purpose is to <u>reduce the risk of session abuse during periods of inactivity</u>. If a session cannot be locked, an attacker can hijack the session. As a result, system availability may be lost due to unauthorized manipulation of the system.

Countermeasures

The countermeasure described here is the capability of session lock, either automatically or manually.

- Automatic session lock.

The inactivity period is configurable. On the other hand, the application of this function to systems that directly affect ship navigation is not recommended, as it may compromise availability.

· Manual session lock

Compensating countermeasures

Compensating countermeasures should be adopted in cases where the aforementioned capabilities or countermeasures have not been implemented.

Scope

This requirement does not apply to the following cases:

- If the session is not used

This requirement does not apply if the system does not use sessions, e.g., if the system, does not

Document reviews

Description of security capabilities

12.	12. Session lock	
-1.	If th	is requirement applies, either of the following (1) or (2) is to be implemented.
(1)	Sess	sion lock functionality, either automatic or manual
	(a)	For automatic session locks, the following is to be checked:
		i) The session locks after a period of inactivity
		ii) The inactivity period is configurable.
	(b)	For manual session locks, the following is to be checked:
		i) Session lock is manually enabled.
(2)	Con	npensating countermeasure
	(a)	Protect against the same threats as the original requirement
	(b)	Provide an equal level of protection as the original requirement
	(c)	Not be a security control that is required by other requirements
	(d)	Not introduce higher security risk

Surveys

12. Session lock	
-1. If this requirement applies, either of the following (1) or (2) is to be performed.	
(1) For automatic session locks, the following is to be checked:	
(a) The session locks after a period of inactivity	
i) The inactivity period is configurable.	
ii) For manual session locks, the following is to be checked:	
(b) Session lock is manually enabled.	
i) For automatic session locks, the following is to be checked:	
(2) Confirmation of compensating countermeasure	
Confirm that the information is as described in Description of security capabilities.	



13. Auditable events

Reg. Table X4.1 Item 13, Part X of the Rules

Ref. IEC62443-3-3 / SR 2.8

The CBS shall generate audit records relevant to security for at least the following events: access control, operating system¹ events, backup and restore events, configuration changes, loss of communication.

Explanation

Summary

Item 13, Table X4.1, Part X states that the requirement to generate audit records of important events relevant to security. "Audit records" are records of important events relevant to security.

Purpose

The purpose is to <u>record important events that need audits</u>. If an essential record is lacking, the audit will not be proper, making it difficult to analyse the cause of the incident.

Countermeasures

The countermeasure described here is to generate audit records of important events. Specifically, audit records of the following events are necessary:

- Access control

This is the means to restrict who can access a computer or network. Successful and failed login attempts, changes in access privileges, etc. are examples. By recording these events, unauthorized access and abuse of privileges can be traced.

- Operating system events

This refers to all OS-related activities such as system startup and shutdown, system errors, software updates and installations, etc.

- Backup and restore events

Records activities related to data backup and restoration, including backups and restores, successful and failed backups, attempts to tamper with backup data, etc.

- Configuration changes

It means timestamp, procedure, and account of the system setting changes. The settings include security settings, network settings, and user permission settings.

¹ **Operating System:** The software that serves as the foundation for running a computer system, or OS for short. A commonly used OS, such as Windows, is called a general-purpose OS.

- Loss of communication

Records interruptions and loss of network connectivity, interruptions in communication between services, and events that prevent the system from connecting to the network. This record enables the identification of network attacks and connectivity problems.

Compensating countermeasures

If these capabilities are not implemented, compensating countermeasures are to be taken an example of a compensating countermeasure:

- Audit records are produced by an external monitoring system.

External monitoring systems can complement this requirement by recording the events. An external monitoring system could be, for example, an engine control console (ECC).

Scope

This requirement, in principle, applies to all CBSs.

Document reviews

Description of security capabilities

13.	uditable events
-1.	f this requirement applies, either of the following (1) or (2) is to be implemented.
(1)	The function to generate audit records of important events
	a) The audit records of the following events are necessary
	i) Access control
	ii) Operating system events
	iii) Backup and restore events
	iv) Configuration changes
	v) Loss of communication
(2)	Compensating countermeasure
	a) Protect against the same threats as the original requirement
	b) Provide an equal level of protection as the original requirement
	c) Not be a security control that is required by other requirements
	d) Not introduce higher security risk

Surveys

13. Auditable events					
-1. If this requirement applies, either of the following (1) or (2) is to be performed.					
(1) The tests of the function to generate audit records of important events					
(a) It is to be confirmed the audit records of the following events can be generated.					
i) Access control					
ii) Operating system events					
iii) Backup and restore events					
iv) Configuration changes					
v) Loss of communication					
(2) Confirmation of compensating countermeasure					
Confirm that the information is as described in Description of security capabilities.					



14. Audit storage capacity

Reg. Table X4.1 Item 14, Part X of the Rules

Ref. IEC62443-3-3 / SR 2.9

The CBS shall generate audit records¹ relevant to security for at least the following events: access control, operating system events, backup and restore events, configuration changes, loss of communication.

Explanation

Summary

Item 14, Table X4.1, Part X states that the requirement to allocate sufficient audit record¹ storage capacity according to commonly recognized recommendations for log management and system configuration. The NIST² Special Publication (SP) 800-92 is an example of them.

It also states that the audit function should be implemented in such a way as to reduce the <u>likelihood of exceeding the capacity</u>. The function ensures the capacity to supplement audit records over the required period.

Purpose

The purpose is to <u>store audit records needed for audits</u>. If storage for records is insufficient, the audit record will be lacking, making it difficult to analyse the threat of the incident.

Countermeasures

The countermeasure described here is the capability allocating sufficient audit record storage capacity according to commonly recognized recommendations for log management and system configuration and an audit mechanism reducing the likelihood of exceeding the capacity. Specifically, they will be the following:

- Ensuring sufficient audit record storage capacity based on general recommendations
 Needs to allocate sufficient audit record storage capacity considering guidelines and policies stating general recommendations like NIST SP 800-92.
- Ensuring the capacity to supplement audit records over the required period

 In designing the capacity of audit records, the amount of audit logs in a certain period and the period sufficient capacity is available are to be considered.

Compensating countermeasures

Compensating countermeasures should be adopted in cases where the aforementioned capabilities

¹ Audit record Single record of significant security events

or countermeasures have not been implemented. The following is an example of a compensating countermeasure.

- Output function of the records to external storage devices.

In designing the capacity of audit records, the amount of audit logs in a certain period and the period sufficient capacity is available are to be considered.

If storing the records needed for audits is impossible, complement this function by putting out the records to external storage. In this case, the specification of export functions needs is to be clearly stated, such as the need for export in a certain period.

Scope

This requirement does not apply to the following cases.

- In "13. Auditable events", compensating countermeasures are either to be adopted or the requirements do not apply.

If the capability to generate audit records is not implemented, there is no identifier. In such cases, this requirement is not applicable.

∐≣

Auditable events

P. 86

Document reviews

Description of security capabilities

14. Audit storage capacity					
-1.	. If this requirement applies, either of the following (1) or (2) is to be implemented.				
(1)	The	The capabilities allocating sufficient audit record storage capacity according to commonly			
	reco	ognized recommendations for log management			
	(a)	Based on commonly recognized recommendations for log management (e.g. NIST			
		SP800-92)。			
	(b)	Ensuring the capacity to supplement audit records over the required period.			
(2)	Compensating countermeasure				
	(a) Protect against the same threats as the original requirement				
	(b)	Provide an equal level of protection as the original requirement			
	(c)	Not be a security control that is required by other requirements			
	(d)	Not introduce higher security risk			

Surveys

14. Audit storage capacity			
-1.	If this requirement applies, either of the following (1) or (2) is to be performed.		
(1)	The Demonstration test for the capability allocating sufficient audit record storage		
	capacity according to commonly recognized recommendations for log management		
	(a) Based on commonly recognized recommendations for log management (e.g. NIST		
	SP800-92)。		
	(b) Ensuring the capacity to supplement audit records over the required period.		
(2)	Confirmation of compensating countermeasure		
	Confirm that the information is as described in Description of security capabilities.		



15. Response to audit processing failures

Reg. Table X4.1 Item 15, Part X of the Rules

Ref. IEC62443-3-3 / SR 2.10

The CBS shall provide the capability to prevent loss of essential services and functions in the event of an audit processing failure.

Explanation

Summary

Item 15, Table X4.1, Part X states that the need to prevent the loss of essential services and functions when the audit process fails. The audit process is the process that involves the audit record. The audit process is related to the audit record, including to generate the audit record. Typical possible failures are software or hardware errors in the system, a failure of the audit process, or an excess of storage capacity. In addition, essential services and functions mean those whose failure will be fatal to vessel operation. Therefore, the essential functions must not fail in the event of an error in the processing involved in the audit record.

Purpose

The purpose is to prevent the risk of loss of essential services and functions due to the audit process. If the audit process and essential services and functions are part of the same process, the failure of the record function can cause an outage of essential functions.

Countermeasures

The countermeasure described here is the capability to prevent the loss of essential services and functions in the event of a failure of the audit process. Separating audit functions from essential functions is one of the examples.

Compensating countermeasures

Compensating countermeasures should be adopted in cases where the aforementioned capabilities or countermeasures have not been implemented.

Scope

This requirement does not apply to the following cases.

- In "13. Auditable events", compensating countermeasures are either to be adopted or the requirements do not apply.

¹ Audit record Single record of significant security events

If the capability to generate audit records is not implemented, there is no identifier. In such cases, this requirement is not applicable.

Auditable events

P. 86

Document reviews

Description of security capabilities

15. Response to audit processing failures				
-1.	-1. If this requirement applies, either of the following (1) or (2) is to be implemented.			
(1)	1) Capabilities to prevent the loss of essential services and functions when the audit process			
	fails			
	(a)	Prevent the loss of essential services and functions in the event of a failure of the		
		audit process. (e.g., Separating audit functions from essential functions)		
(2)	Compensating countermeasure			
	(a)	Protect against the same threats as the original requirement		
	(b)	Provide an equal level of protection as the original requirement		
	(c)	Not be a security control that is required by other requirements		
	(d)	Not introduce higher security risk		

Surveys

15.	15. Response to audit processing failures			
-1.	If this requirement applies, either of the following (1) or (2) is to be performed.			
(1)	Demonstration test for Capabilities to prevent the loss of essential services and functions			
	when the audit process fails			
	(a) Prevent the loss of essential services and functions in the event of a failure of the			
	audit process. (e.g., Separating audit functions from essential functions)			
(2)	Confirmation of compensating countermeasure			
	Confirm that the information is as described in Description of security capabilities.			



16. Timestamps

Reg. Table X4.1 Item 16, Part X of the Rules

Ref. IEC62443-3-3 / SR 2.11

The CBS shall timestamp audit records.

Explanation

Summary

Item 16, Table X4.1, Part X states that the audit record must include the date and time of the events.

Purpose

The purpose is to create a timeline of when the events requiring audit occurred. Without the timeline, analysis of the cause will be difficult.

Countermeasures

The timestamp does not need to synchronize with other systems.

The countermeasure described here is the capability to record the date and time. Specifically, it is a time stamp. A timestamp is the date and time when a specific event is generated as a log.

For reliability, it is recommended to use dedicated clock hardware (e.g., real-time clock IC¹) or a system internal clock (system clock²) to generate timestamps. When using a system clock, it is possible to record the date and time by reading the counted value of the operation time after startup as the date and time.

Compensating countermeasures

Compensating countermeasures should be adopted in cases where the aforementioned capabilities or countermeasures have not been implemented.

Scope

This requirement does not apply to the following cases.

 In "13. Auditable events", compensating countermeasures are either to be adopted or the requirements do not apply.

If the capability to generate audit records is not implemented, there is no identifier. In such cases,

¹ **Real-time clock IC:** An integrated circuit maintains the current date and time. It has a backup battery and maintains the time even if the system is off.

² System clock: A clock on the system. It is based on the number of operations of hardware at a fixed period (e.g., arithmetic unit).

Document reviews

Description of security capabilities

16. Timestamps					
-1.	If th	If this requirement applies, either of the following (1) or (2) is to be implemented.			
(1)	The	The capability to include the date and time in the audit record			
	(a)	To include the timestamp in the audit record (e.g., Real-time clock IC, System clock)			
(2)	Compensating countermeasure				
	(a)	Protect against the same threats as the original requirement			
	(b)	Provide an equal level of protection as the original requirement			
	(c)	Not be a security control that is required by other requirements			
	(d)	Not introduce higher security risk			

Surveys

16. Timestamps			
-1.	If this requirement applies, either of the following (1) or (2) is to be performed.		
(1)	Demonstration test for the capability to include the date and time in the audit record		
	(a) To include the timestamp in the audit record (e.g., Real-time clock IC, System clock)		
(2)	Confirmation of compensating countermeasure		
	Confirm that the information is as described in Description of security capabilities.		



17. Communication integrity

Reg. Table X4.1 Item 17, Part X of the Rules

Ref. IEC62443-3-3 / SR 3.1

The CBS shall protect the integrity of transmitted information.

Note: Cryptographic mechanisms shall be employed for wireless networks.

Explanation

Summary

Item 17, Table X4.1, Part X states that the integrity of the information transmitted is to be protected. Integrity means that the information is accurate and complete. This means that there needs to be a mechanism to ensure that information is not tampered with and that the information is transmitted as it is.

Purpose

The purpose is to prevent the risk of information that is transmitted being improperly altered, deleted and destroyed. If the information transmitted is tampered with, this could lead to a loss of confidence in the information and threaten the safety of the navigation.

Countermeasures

The countermeasure described here is the capability of the receiver of the information to verify that the information has been tampered with. The specific functions are as follows.

- When there is a discrepancy between the received data and the transmitted data, the function requests the sender to retransmit the data.
- When the received data continues to differ from the transmitted data, an alarm is triggered.

<u>If wireless communication is used, a high-strength encryption algorithm is to be used.</u> Because, under wireless communication, signals in transmission can easily be intercepted from outside the CBS. Encryption is explained in more detail in Item No.22. Use of cryptography.



Use of cryptography

P. 109

Compensating countermeasures

Compensating countermeasures should be adopted in cases where the aforementioned capabilities or countermeasures have not been implemented.

Scope

This requirement does not apply to the following cases:

- No connection to a network or other CBS

If no connection to a network or other computer system is used, this requirement does not apply.

Document reviews

■ Description of security capabilities

17. Communication integrity			
-1.	If this requirement applies, either of the following (1) or (2) is to be implemented.		
(1)	The capability to protect the integrity of transmitted information		
	(a) The following functions are to be provided		
	i) When there is a discrepancy between the received and transmitted data, a		
	function to request the sender to retransmit the data.		
	ii) A function to issue an alarm when discrepancies between the received and		
	transmitted data continue to be detected.		
	(b) Where wireless communications are used, the information transmitted is to be		
	encrypted.		
(2)	(2) Compensating countermeasure		
	(a) Protect against the same threats as the original requirement		
	(b) Provide an equal level of protection as the original requirement		
	(c) Not be a security control that is required by other requirements		
	(d) Not introduce higher security risk		

Surveys

17. Communication integrity				
-1. If this requirement applies, either of the following (1) or (2) is to be performed.				
(1) Demonstration test for capability to protect the integrity of transmitted information				
(a) The following functions are to be provided				
i) When there is a discrepancy between the received and transmitted data, a				
function to request the sender to retransmit the data.				
ii) A function to issue an alarm when discrepancies between the received and				
transmitted data continue to be detected.				
(b) Where wireless communications are used, the information transmitted is to be				
encrypted.				

☐ (2) Confirmation of compensating countermeasure

Confirm that the information is as described in Description of security capabilities.



18. Malicious code protection

Reg. Table X4.1 Item 18, Part X of the Rules

Ref. IEC62443-3-3 / SR 5

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 mechanism.

Explanation

Summary

Item 18, Table X4.1, Part X states that it is necessary to <u>implement suitable protection measures to</u> <u>prevent</u>, <u>detect and mitigate the effects due to malicious code or unauthorized software</u>. Malicious code or unauthorized software is any program or software that is designed to intentionally cause a system to behave in an unauthorized and harmful manner, commonly referred to as **malware**.

Purpose

The purpose is to minimize the risk from malware.

Countermeasures

The countermeasure described here is the capability to implement suitable protection measures to prevent, detect and mitigate the effects due to malware.

- Capability to prevent the effects of malware

This is a means to prevent malware from entering the system. These include application whitelist restrictions, removable media execution restrictions, and sandbox functionality.

- Capability to detect the effects of malware

A means of checking whether malware has entered the system. These include intrusion detection systems (IDS) and anti-malware scans.

- Capability to mitigate the effects of malware

A means of minimizing the impact of malware when it occurs. This includes deleting files and isolating infected terminals.

In addition, these countermeasures are required to <u>be regularly updated</u> so that the mechanisms in place can function effectively.

Compensating countermeasures

Compensating countermeasures should be adopted in cases where the aforementioned capabilities

or countermeasures have not been implemented. The following is an example of a compensating countermeasure.

- External security devices

External security devices, such as firewalls, can complement this capability by preventing, detecting, and reducing malware.

Scope

This requirement does not apply to the following cases:

- Not to use a general-purpose OS1

Malware is usually targeted at general-purpose operating systems such as Windows. Therefore, CBSs with proprietary operating systems that do not use general-purpose operating systems are likely to be free of malware, and this requirement does not apply.

Document reviews

Description of security capabilities

18. Malicious code protection			
-1.	If this requ	direment applies, either of the following (1) or (2) is to be implemented.	
(1)	(1) The capability to implement suitable protection measures to prevent, detect and mitigate		
	the effects	due to malware	
	(a) The fe	following capabilities are to be implemented:	
	i) (Capability to prevent the effects of malware (e.g., Application whitelist	
	1	restrictions, removable media execution restrictions, Sandbox capabilities)	
	ii) (Capability to detect the effects of malware (e.g., intrusion detection system	
	((IDS), anti-malware scan)	
	iii) (Capability to mitigate the effects of malware (e.g., delete files, quarantine	
	i	infected terminals)	
(2)	Compensat	ting countermeasure	
	(a) Protect	ct against the same threats as the original requirement	
	(b) Provid	de an equal level of protection as the original requirement	
	(c) Not b	e a security control that is required by other requirements	
	(d) Not in	ntroduce higher security risk	

Surveys

 $^{1}\,$ General-purpose OS: A general operating system. For example, Windows.

18. Malicious code protection
-1. If this requirement applies, either of the following (1) or (2) is to be performed.
(1) Demonstration test for the capability to implement suitable protection measures to
prevent, detect and mitigate the effects due to malware;
(a) The following capabilities are implemented:
i) Capability to prevent the effects of malware (e.g., Application whitelist
restrictions, removable media execution restrictions, Sandbox capabilities)
ii) Capability to detect the effects of malware (e.g., intrusion detection system
(IDS), anti-malware scan)
iii) Capability to mitigate the effects of malware (e.g., delete files, quarantine
infected terminals)
(2) Confirmation of compensating countermeasure
Confirm that the information is as described in Description of security capabilities.



19. Security functionality verification

Reg. Table X4.1 Item 19, Part X of the Rules

Ref. IEC62443-3-3 / SR 3.3

The CBS shall provide the capability to support verification of the intended operation of security functions and report when anomalies occur during maintenance.

Explanation

Summary

Item 19, Table X4.1, Part X states that it is necessary to <u>support verification of the intended operation of security functions</u>. In this section, security functions are all of the security capabilities required by Chapter 4 of Part X (UR E27) that are implemented. This means it is necessary to ensure the implemented security functions work correctly.

In addition, it is necessary to report when anomalies occur during maintenance.

Purpose

The purpose is to implement the security capabilities required by Part X, Chapter 4 (UR E27) in the CBS and to verify that the capabilities are performing the operation successfully to satisfy the requirements. If proper testing is not implemented, the security capabilities may not function when needed. Furthermore, if an anomaly occurs during maintenance, it can be reported, thereby increasing confidence in maintenance.

Countermeasures

The countermeasures are the capability to support verification of the intended operation of security functions, and the capability to report when anomalies occur during maintenance. Specifically, they are as follows:

· Capability to support verification of the intended operation of security functions

The capability verifies the operation of implemented security capabilities. For example, in the capability for authenticating people, if a login is attempted by an invalid account, the login is denied.

Capability to report when anomalies occur during maintenance

The capability for reporting problems that may occur during maintenance. For example, when antivirus software is installed, a message is output when an update of an identification code or pattern of a virus or malware fails.

Note: These capabilities are used by the owner to maintain the system. To support their use, the supplier should include instructions on how to verify these capabilities in "Plans for maintenance and verification of the CBS".

Plans for maintenance and verification of the CBS

P. 32

Compensating countermeasures

Compensating countermeasures should be adopted in cases where the aforementioned capabilities or countermeasures have not been implemented.

Scope

This requirement, in principle, applies to all CBSs.

Document reviews

Description of security capabilities

19.	Secu	rity functionality verification
-1.	If th	is requirement applies, either of the following (1) or (2) is to be implemented.
(1)	The	capability to support verification of the intended operation of security functions and
	repo	ort when anomalies occur during maintenance
	(a)	Capability to support verification of the intended operation of security functions
		Verify the intended operation of security functions
	(b)	Capability to report when anomalies occur during maintenance
		Report when anomalies occur during maintenance (e.g., if antivirus software is
		installed, a message is output when virus or malware identification codes or patterns
		fail to update, etc.)
(2)	Con	npensating countermeasure
	(a)	Protect against the same threats as the original requirement
	(b)	Provide an equal level of protection as the original requirement
	(c)	Not be a security control that is required by other requirements
	(d)	Not introduce higher security risk

Surveys

■ Test procedure of security capabilities

19. Security functionality verification

-1. If this requirement applies, either of the following (1) or (2) is to be performed.

(1) The demonstration test for the capability to support verification of the intended operation
of security functions and report when anomalies occur during maintenance
(a) Capability to support verification of the intended operation of security functions
i) Verify the intended operation of security functions
(b) Capability to report when anomalies occur during maintenance
 Report when anomalies occur during maintenance (e.g., if antivirus software is installed, a message is output when virus or malware identification codes or patterns fail to update.)
(2) Confirmation of compensating countermeasure
Confirm that the information is as described in Description of security capabilities.



20. Deterministic output

Reg. Table X4.1 Item 20, Part X of the Rules

Ref. IEC62443-3-3 / SR 3.6

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

Explanation

Summary

Item 20, Table X4.1, Part X states that it is necessary to <u>set outputs to a predetermined state if</u> normal operation cannot be maintained as a result of an attack. "Predetermined state" is as follows.

Term	Description
Unpowered state	The system is turned off.
Last-known value	The value that the system was outputting just before the system was attacked.
Fixed value	The specific value that has been pre-set by the system. This value is determined by the owner or other parties.

Purpose

The purpose is to make the entire system more secure and easier to resolve by maintaining a specific state, even if the system is incompetent by an attack. As an example, suppose a system controlling a marine plant is attacked. If the system experiences an unexpected output due to an attack, it may cause equipment to malfunction and prevent normal operation. In such a case, safety can be ensured by moving to a predetermined state, such as shutting down the system or returning it to a safe operating range.

Countermeasures

The countermeasure described here is the capability to set outputs to a predetermined state. This capability is necessary to change to the specified state described above.

Compensating countermeasures

Compensating countermeasures should be adopted in cases where the aforementioned capabilities or countermeasures have not been implemented.

Scope

This requirement, in principle, applies to all CBSs.

Document reviews

Description of security capabilities

20.	eterministic outp	out
-1.	f this requirement a	pplies, either of the following (1) or (2) is to be implemented.
(1)	The capability to set	outputs to a predetermined state
	The output can be cl	nanged to at least one of the following states
	a) Unpowered sta	te
	b) Last-known va	lue, or Fixed value
(2)	Compensating coun	termeasure
	a) Protect against	the same threats as the original requirement
	b) Provide an equ	al level of protection as the original requirement
	c) Not be a securi	ty control that is required by other requirements
	d) Not introduce l	nigher security risk

Surveys

20.	20. Deterministic output		
-1.	If this requirement applies, either of the following (1) or (2) is to be performed.		
(1)	The Demonstration test for the capability to set outputs to a predetermined state		
	The output can be changed to at least one of the following states		
	(a) Unpowered state		
	(b) Last-known value, or Fixed value		
(2)	Confirmation of compensating countermeasure		
	Confirm that the information is as described in Description of security capabilities.		



21. Information confidentiality

Reg. Table X4.1 Item 21, Part X of the Rules

Ref. IEC62443-3-3 / SR 4.1

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.

Explanation

Summary

Item 21, Table X4.1, Part X states that <u>confidentiality protection of information for which explicit</u> <u>authorization is required with respect to reading, whether in storage or in transmission.</u>

Reading means retrieving information from a database or file. For example, when viewing a web page on the Internet, the browser reads data from the web server to display the page.

In addition, information that requires explicit authorization is only to be accessed by authorized persons. In other words, information that requires authorization to obtain must be kept confidential.

Purpose

The purpose is to ensure the confidentiality of information that can only be accessed by authorized persons. If the confidentiality of information is compromised, it may lead to information leaks or unauthorized information use.

Countermeasures

The countermeasures here are capabilities to protect the confidentiality of information that requires explicit authorization for reading. Specifically, the measures are as follows:

- Capability to protect the confidentiality of information in storage.

Capability to protect the confidentiality of information in storage, including functions related to access rights such as user authentication and authorization, and functions to encrypt information.

- Capability to protect the confidentiality of information during transmission

Capability to protect the confidentiality of information during transmission, such as encryption. One-to-one wired connections also ensure confidentiality during transmission.

In addition, when wireless communication is used, encryption mechanisms must be employed because of the possibility that data in transmission may be accessed. For encryption mechanisms, please refer to "22. Use of cryptography".

Compensating countermeasures

Compensating countermeasures should be adopted in cases where the aforementioned capabilities or countermeasures have not been implemented.

Scope

This requirement, in principle, applies to all CBSs. If the information is not transmitted, the confidentiality of the information during transmission is not applicable.

Document reviews

Description of security capabilities

21.	Information confidentiality
-1.	If this requirement applies, either of the following (1) or (2) is to be implemented.
(1)	Confidentiality protection capabilities of information for which explicit authorization is
	required with respect to reading, whether in storage or in transmission
	(a) The following capabilities are to be confirmed.
	i) Capabilities to protect the confidentiality of information in storage.
	ii) Capabilities to protect the confidentiality of information during transmission.
	(b) When wireless communication is used, encryption mechanisms are to be employed.
(2)	Compensating countermeasure
	(a) Protect against the same threats as the original requirement
	(b) Provide an equal level of protection as the original requirement
	(c) Not be a security control that is required by other requirements
	(d) Not introduce higher security risk

Surveys

This requirement will be verified through the document reviews. Therefore, the surveys are not required.



22. Use of cryptography

Reg. Table X4.1 Item 22, Part X of the Rules

Ref. IEC62443-3-3 / SR 4.3

If cryptography is used, the CBS shall use cryptographic algorithms, key sizes and mechanisms according to commonly accepted security industry practices and recommendations.

Explanation

Summary

Item 22, Table X4.1, Part X states that <u>the recommended cryptographic algorithms</u>, <u>key sizes</u>, and <u>mechanisms are needed</u>. Descriptions of the encryption algorithms, key lengths, and mechanisms are following.

Terms	Descriptions
Cryptographic	The procedures and rules for encrypting and decrypting (restoring) data.
algorithm	
Key size	The number of bits that make up a key. The greater the number of bits, the
	more combinations of keys, and the stronger the encryption.
Key mechanism	How keys are generated and managed. Management includes, for example,
	periodic changes, destruction, key distribution, and encryption key backup.

Purpose

The purpose is to ensure the integrity and confidentiality of the encrypted information.

Countermeasures

The countermeasure described here is to employ encryption schemes in accordance with generally accepted security industry practices and recommendations. "Generally accepted security industry practices and recommendations" include followings:

- · ISO/IEC 19790
- · NIST1 SP800-57
- · NIST FIPS14

Compensating countermeasures

¹ NIST: National Institute of Standards and Technology

Compensating countermeasures should be adopted in cases where the aforementioned capabilities or countermeasures have not been implemented.

Scope

This requirement does not apply to the following cases:

- In case of no use of encryption.

If cryptography is not used, this requirement does not apply.

Document reviews

■ Description of security capabilities

22.	Use of cryptography
-1.	If this requirement applies, any of the following mechanisms or countermeasures (1) or (2)
	is to be implemented:
(1)	Encryption algorithm, key length, and mechanism according to generally accepted
	security industry practices and recommendations
	Generally accepted security industry practices and recommendations are employed for the
	following items
	(a) Cryptographic algorithm
	(b) Key size
	(c) Key mechanism
(2)	Compensating countermeasure
	(a) Protect against the same threats as the original requirement
	(b) Provide an equal level of protection as the original requirement
	(c) Not be a security control that is required by other requirements
	(d) Not introduce higher security risk

Surveys

This requirement will be verified through the document reviews. Therefore, the surveys are not required.



23. Audit log accessibility

Reg. Table X4.1 Item 23, Part X of the Rules

Ref. IEC62443-3-3 / SR 6.1

The CBS shall provide the capability for accessing audit logs on read only basis by authorized humans and/or tools.

Explanation

Summary

Item 23, Table X4.1, Part X states that <u>authorized persons and/or tools must have read-only access</u> to the <u>audit log.</u> An authorized human user is a person authorized to use this function, primarily an administrator. Authorized tools, on the other hand, are programs authorized to use this functionality. An example would be software for monitoring and analysing security-related events and alerts, called SIEM¹. An audit log is a chronological collection of audit records². It can be viewed as a compilation of multiple audit logs.

Purpose

The purpose is to reduce the risk of audit logs being altered.

Countermeasures

The countermeasure here will be the function of <u>read-only access to the audit log by authorized</u> human users and/or tools.

Compensating countermeasures

Compensating countermeasures should be adopted in cases where the aforementioned capabilities or countermeasures have not been implemented.

Scope

- In "13. Auditable events", compensating countermeasures are either to be adopted or the requirements do not apply.

If the capability to generate audit records is not implemented, there is no identifier. In such cases, this requirement is not applicable.



Auditable events

P. 111

Document reviews

¹ SIEM: Security Information and Event Management

² Audit record: Single record of significant security events

Description of security capabilities

23.	Audit log accessibility
-1.	If this requirement applies, either of the following (1) or (2) is to be implemented.
(1)	The function of read-only access to the audit log by authorized human users and/or tools.
	(a) The function of access to the audit log by authorized human users and/or tools.
	(b) The access to the audit log is read-only.
(2)	Compensating countermeasure
	(a) Protect against the same threats as the original requirement
	(b) Provide an equal level of protection as the original requirement
	(c) Not be a security control that is required by other requirements
	(d) Not introduce higher security risk

Surveys

23.	Audit log accessibility
-1.	If this requirement applies, either of the following (1) or (2) is to be performed.
(1)	Capability to set output to a predefined state
	(a) Conform to the following items.
	i) Access to the audit log by authorized human users and/or tools is available.
	ii) Access to the audit log by unauthorized human users and/or tools is not
	available.
	(b) The access to the audit log is read-only.
(2)	Confirmation of compensating countermeasure
	Confirm that the information is as described in Description of security capabilities.



24. Denial of service protection

Reg. Table X4.1 Item 24, Part X of the Rules

Ref. IEC62443-3-3 / SR 7.1

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 DoS1 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.

Explanation

Summary

Item 24, Table X4.1, Part X states that <u>essential functions are to be maintained during DoS events</u>. DoS, which stands for "Denial of Service", is an attack technique that causes systems to fail by sending large amounts of information to servers or other devices in an attempt to cause them to overload.

Purpose

The purpose is <u>to prevent the risk of DoS attacks shutting down essential functions</u> since such attacks can compromise availability and even cause total system outages. Therefore, measures are required to maintain essential functionality.

Countermeasures

The following countermeasures provide <u>minimal functionality to maintain essential functions</u> during DoS events.

- Reduce the priority of communication processing processes
- Limit the IP addresses that can be accessed

Compensating countermeasures

Compensating countermeasures should be adopted in cases where the aforementioned capabilities or countermeasures have not been implemented. The following is an example of a compensating countermeasure.

¹**DoS**: Denial of Service. DDoS (Distributed Denial of Service) attacks, among others, use multiple computers and devices to disrupt systems on a larger scale by sending massive amounts of traffic to websites and servers.

- External security devices restrict the IP addresses that can be accessed.

External perimeter protection devices (firewalls, intrusion detection systems (IDS), etc.) can complement this capability by restricting the IP addresses that can be accessed.

Scope

This requirement, in principle, applies to all CBSs.

Document reviews

Description of security capabilities

24.	Denial of service protection	
-1.	If this requirement applies, either of the following (1) or (2) is to be implemented.	
(1)	Minimum capability to maintain essential functions during DoS events	
	Maintenance of essential functions during DoS events (e.g., deprioritising communication	
	processes)	
(2)	Compensating countermeasures	
	(a) Protect against the same threats as the original requirement	
	(b) Provide an equal level of protection as the original requirement	
	(c) Not be a security control that is required by other requirements	
	(d) Not introduce higher security risk	

Surveys

24.	Denial of service protection
-1.	If this requirement applies, either of the following (1) or (2) is to be performed.
(1)	Demonstration test for Minimum capability to maintain essential functions during DoS
	events
	Maintenance of essential functions during DoS event (e.g., confirming the results of DoS
	event simulation tests)
(2)	Confirmation of compensating countermeasure
	Confirm that the information is as described in Description of security capabilities.



25. Resource management

Reg. Table X4.1 Item 25, Part X of the Rules Ref. IEC624

Ref. IEC62443-3-3 / SR 7.2

The CBS shall provide the capability to limit the use of resources by security functions to prevent resource exhaustion.

Explanation

Summary

Item 25, Table X4.1, Part X states that the use of resources by security features should be restricted, in which "resources" refer to the physical or logical resources available to a system such as CPU processing time, process memory, storage capacity, and network bandwidth.

Purpose

The purpose is to prevent security functions from running out of resources. The following are some examples of security functions affected by a resource shortage and the corresponding expected events.

Cause security functions	Expected events
Virus scanning by antivirus software	Slow down the CPU
	Run out of free memory
Long-term security log storage	Run out of hard disk memory

Countermeasures

The countermeasures described here <u>restrict the use of resources by security functions</u>. It is necessary to implement functions that prevent a shortage of resources in response to security functions or expected events that cause a shortage of resources. For example, the following countermeasures can be adopted.

Cause security functions	Countermeasure
or Expected events	
Virus scanning by antivirus	Scan outside system operating hours.
software	Stops scanning when the free space of a resource falls
	below a certain value.
Long-term security log storage	When the log is written, the remaining capacity is

	checked, and an alarm is raised if it is running out.
	Change to the ring buffer method ¹ .
Network bandwidth compression	The communication amount is controlled by a rate
	limiting.

Compensating countermeasures

Compensating countermeasures should be adopted in cases where the aforementioned capabilities or countermeasures have not been implemented. The following is an example of a compensating countermeasure.

- Ensure sufficient resources

This function ensures that sufficient resources are available to prevent security functions from running out of resources. In such cases, a rationale for sufficient resources is to be provided.

Scope

This requirement, in principle, applies to all CBSs.

Document reviews

Description of security capabilities

25. Resource management			
-1.	If this requirement applies, either of the following (1) or (2) is to be implemented.		
(1)	Capability to restrict the use of resources by security functions to avoid exhausting		
	resources		
(2)	Compensating countermeasure		
	(a) Protect against the same threats as the original requirement		
	(b) Provide an equal level of protection as the original requirement		
	(c) Not be a security control that is required by other requirements		
	(d) Not introduce higher security risk		

Surveys

■ Test procedure of security capabilities

25. Resource management

¹ Ring buffer method: A data storage system used cyclically in buffer areas for temporarily storing data in which old data is overwritten in the order added to free up additional space for new data.

-1.	If this requirement applies, either of the following (1) or (2) is to be performed.
(1)	Demonstration test for the capability to restrict the use of resources by security functions
	so that resources are not exhausted
(2)	Confirmation of compensating countermeasure
	Confirm that the information is as described in the security capability descriptions.



26. System backup

Reg. Table X4.1 Item 26, Part X of the Rules

Ref. IEC62443-3-3 / SR 7.3

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

Explanation

Summary

Item 26, Table X4.1, Part X states that two things about backup the system are required.

- Backup critical files
- Backup does not affect normal operations

Purpose

The purpose is to ensure that important files are backed up.

Countermeasures

The countermeasures described here <u>backup critical files that may need to be recovered at some</u> <u>point</u>. The files to be backed up are determined by the system and are backed up in a manner they does not affect normal system operations.

Compensating countermeasures

Compensating countermeasures should be adopted in cases where the aforementioned capabilities or countermeasures have not been implemented. The following is an example of a compensating countermeasure.

- Replacing with a spare system

Replacing original systems with spares can compensate for said systems' functions. In such cases, however, it is important that the spares have the same settings as the original system. In addition to the system itself, spares may include portable media such as CDs and DVDs.

Scope

This requirement does not apply to the following cases:

· When there is no need to back up

The purpose of a backup is to allow recovery of critical files and other information in cases where

systems go down due to reprogramming by attackers. Therefore, backups are not required for programs that are written directly to the hardware, such as embedded systems using firmware, that cannot be over written.

Document reviews

Description of security capabilities

26.	26. System backup			
-1.	If this requirement applies, either of the following (1) or (2) is to be implemented.			
(1)	Capability to back up critical files to be recovered			
	(a) Backup of data needed to recover the system			
	(b) Does not affect normal operation			
(2)	Compensating countermeasure			
	(a) Protect against the same threats as the original requirement			
	(b) Provide an equal level of protection as the original requirement			
	(c) Not be a security control that is required by other requirements			
	(d) Not introduce higher security risk			

Surveys

■ Test procedure of security capabilities

26. System Backup -1. If this requirement applies, either of the following (1) or (2) is to be performed. (1) Demonstrated capability to back up critical files to be recovered Backup of data needed to recover the system (2) Confirmation of compensating countermeasure Confirm that the information is as described in the security capability descriptions.



27. System recovery and reconstitution

Reg. Table X4.1 Item 27, Part X of the Rules

Ref. IEC62443-3-3 / SR 7.4

The CBS shall provide the capability to be recovered and reconstituted to a known secure state after a disruption or failure.

Explanation

Summary

Item 27, Table X4.1, Part X states that systems should be capable of being recovered and reconstituted to a known secure state after any disruption or failure.

Purpose

The purpose is to quickly recover and reconfigure a system back to a previous state after an incident has occurred.

Countermeasures

The countermeasures described here <u>help recover and reconfigure a system to a known secure</u> <u>state after any disruption or failure</u>. More specifically, the following are examples of such countermeasures.

- Recovery capability

Recovery capability refers to the overall process by which a system or application recovers from a failure or failure. A known secure state means following:

- System parameters are set to default¹ or secure value
- Security-critical patches² are reinstalled
- Security-related configuration are rechecked and re-established
- System documentation and operating procedures are available
- Application and system software is reinstalled with secure setting
- Reconstitution from the backup data

Note: Recovery and reconfiguration to known secure state may be difficult to achieve with security capability alone, such as reinstalling patches or applications, or reconfiguring security settings. Therefore, it is needed to specify how to do this in the instructions for restoring to

Default: The standard values, conditions, and operating conditions that the system ships with.

² Patch: A program that fixes system vulnerabilities and security defects.

known secure states. These instructions will serve as reference documents required to be submitted to the Society as "Information supporting the owner's incident response and recovery plan". Surveys carried out in the presence of a Society surveyor verify that the system can be restored and reconfigured to a known secure state in accordance with the methods specified in this document. The following links provide more information about this document.

Information supporting the owner's incident response and recovery plan

P. 33

Compensating countermeasures

Compensating countermeasures should be adopted in cases where the aforementioned capabilities or countermeasures have not been implemented. The following is an example of a compensating countermeasure.

- Restoring and reconfiguring to a known secure state immediately after an incident by replacing the original system with a spare

System access is complemented by controlling ports with external network devices, such as firewalls. In such cases, the aforementioned "Information supporting the owner's incident response and recovery plan" is to include instructions for replacing original systems with spares.

Scope

This requirement generally applies to all CBSs

Document reviews

Description of security capabilities

/	27.	27. System recovery and reconstitution				
	-1.	If thi	is requirement applies, either of the following (1) or (2) is to be implemented.			
	(1)	Capa	ability to be recovery and reconstitution to a known secure state after a disruption or			
		failu	re			
		Capability to achieve the following events: It is not necessary to achieve all events by this				
		capability.				
		(a)	System parameters are set to default or secure value			
		(b)	Security-critical patches are reinstalled			
		(c)	Security-related configuration are rechecked and re-established			
		(d)	System documentation and operating procedures are available			
		(e)	Application and system software is reinstalled with secure setting			
		(f)	Reconstitution from the backup data			

(2)	Con	npensating countermeasure
	(a)	Protect against the same threats as the original requirement
	(b)	Provide an equal level of protection as the original requirement
	(c)	Not be a security control that is required by other requirements
	(d)	Not introduce higher security risk

Surveys

■ Test procedure of security capabilities

27. System recovery and reconstitution □ -1. If this requirement applies, either of the following (1) or (2) is to be performed. □ (1) Demonstrated ability to conduct back up critical files to be recovered. The system can be recovered and reconstituted to a known secure state in accordance with the methods specified in "Information supporting the owner's incident response and recovery plan". □ (2) Confirmation of compensating countermeasure Confirm that the information is as described in the security capability descriptions.



28. Alternative power source

Reg. Table X4.1 Item 28, Part X of the Rules

Ref. IEC62443-3-3 / SR 7.5

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.

Explanation

Summary

Item 28, Table X4.1, Part X states that the following two points are required for the alternative power source.

- Switch to and from an alternate power source
- Security capability does not affect existing security states or documented degraded modes

A "degraded mode" is a mode that allows the system to continue its original functions, albeit imperfectly, either by limiting the system's performance or functions, or by isolating abnormal areas when a system malfunction occurs.

Purpose

The purpose is to <u>ensure system security even in the event of a temporary loss of power</u>. Power loss occurs for a period of time when switching to or from an alternate power source. In this case, the impact of the power loss is not to be reached the security status or functionality of the system.

Countermeasures

The countermeasure described here is the capability to switch to and from an alternate power source without affecting the existing security state or the documented degraded mode. Specifically, to prevent loss of security in the event of a power loss, the power supply is to be uninterrupted by an internal battery or storage battery.

Compensating countermeasures

Compensating countermeasures should be adopted in cases where the aforementioned capabilities or countermeasures have not been implemented. The following is an example of a compensating countermeasure.

Redundant CBS, one of which is supplied by an alternate power source
 Duplicating CBS can complement this capability.

Scope

This requirement generally applies to all CBSs

Document reviews

Description of security capabilities

28.	Alternative power source
-1.	If this requirement applies, either of the following (1) or (2) is to be implemented.
(1)	Capability to switch to and from alternate power sources without affecting existing
	security state or documented degraded mode
	Switching to and from an alternative power source without affecting the following
	conditions:
	(a) Existing security state
	(b) Documented degraded mode
(2)	Compensating countermeasure
	(a) Protect against the same threats as the original requirement
	(b) Provide an equal level of protection as the original requirement
	(c) Not be a security control that is required by other requirements
	(d) Not introduce higher security risk

Surveys

28.	28. Alternative power source			
-1.	If this requirement applies, either of the following (1) or (2) is to be performed.			
(1)	Demonstration test for the capability to switch to and from alternative power sources			
	without affecting existing security conditions or documented degraded modes			
	Switching to and from an alternative power source without affecting the following			
	conditions:			
	(a) Existing security state			
	(b) Documented degraded mode			
(2)	Confirmation of compensating countermeasure			
	Confirm that the information is as described in the security capability descriptions.			



29. Network and security configuration settings

Reg. Table X4.1 Item 29, Part X of the Rules

Ref. IEC62443-3-3 / SR 7.6

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.

Explanation

Summary

Item 29, Table X4.1, Part X states that CBSs are to <u>implement features that are set according to</u> the network and security configuration recommended in the guidelines provided by the supplier. The guidelines provided by the supplier refer to "Security configuration guidelines" as part of the submission.

Purpose

The purpose is to <u>set the network and security configuration as recommended by the supplier</u>. System availability can be hindered by misconfiguration or DoS attacks. In this case, the network and security configuration intended by the supplier are to be corrected.

Countermeasures

The countermeasures taken here are <u>capabilities</u> (<u>such as setting parameters</u>) that can be <u>set according to the network and security configuration recommended in the guidelines provided by the supplier. Specifically, they are as follows.</u>

· Capability to set network configuration

Set IP address¹ and subnet mask².

· Capability to set security configuration

Security configuration includes the capability to configure firewalls.

Note: This capability is also used to enhance security during system maintenance. In doing so, "Security hardening guidelines" created by the Secure Product Development Lifecycle support enhanced security. "Security hardening guidelines" are described in detail below.

¹ **IP address:** An address on the network. A value that is expressed as four decimal digits (for example, "223.255.255") and is used to identify the object of communication on the network.

² Subnet mask: A value indicating which of the IP addresses refers to the network and host sections. Change this value when the network is to be subdivided (subnetting).

Security hardening guidelines	P. 171
In addition, "Survey carried out with attendance by a surveyor" confirms the	nat the security
capability is the recommended setting and the default value for the function	n that sets the
security configuration. The recommended setting and the default value is to	be included in

P. 26

Compensating countermeasures

Security configuration guidelines

Compensating countermeasures should be adopted in cases where the aforementioned capabilities or countermeasures have not been implemented.

"Security configuration guidelines". The guidelines are explained in detail below.

Scope

This requirement generally applies to all CBSs

Document reviews

Description of security capabilities

29.	Network and security configuration settings
-1.	If this requirement applies, either of the following (1) or (2) is to be implemented.
(1)	Capability set according to the network and security configuration recommended in the
	guidelines provided by the supplier
	The following items can be established:
	(a) Network configuration
	(b) Security configuration
(2)	Compensating countermeasure
	(a) Protect against the same threats as the original requirement
	(b) Provide an equal level of protection as the original requirement
	(c) Not be a security control that is required by other requirements
	(d) Not introduce higher security risk

Surveys

Test procedure of security capabilities

29. Network and security configuration settings

-1.	If this requirement applies, either of the following (1) or (2) is to be performed.		
(1)	Demonstration test for the capability set according to the network and security		
	configuration recommended in the guidelines provided by the supplier		
	The following items can be established:		
	(a) Network configuration		
	(b) Security configuration		
(2)	Confirmation of compensating countermeasure		
	Confirm that the information is as described in the security capability descriptions.		



30. Least Functionality

Reg. Table X4.1 Item 30, Part X of the Rules

Ref. IEC62443-3-3 / SR 7.7

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 systems¹ software components², processes and services
- network services, ports³, protocols⁴, routes⁵ and hosts⁶ accesses and any software

Explanation

Summary

Item 30, Table X4.1, Part X states that <u>anything that is not essential to the functionality of the system is not to be installed, available or accessible.</u>

Purpose

The purpose here is <u>to prevent security holes</u> by disabling unnecessary functions and minimising system functionality. The more features that are implemented into a system, the more likely the system is to have security holes and be subject to cyber-attacks.

Countermeasures

The countermeasure described here is to <u>minimise system functionality and configuration</u> information. More specifically, the following services and functions should be minimised.

- Operating systems software components, processes and services.
- Network services, ports, protocols, route and host accesses, and all software.

Compensating countermeasures

Compensating countermeasures should be adopted in cases where the aforementioned capabilities or countermeasures have not been implemented.

Scope

¹ **Operating system:** The underlying software that powers a computer system and is often referred to simply as "OS". For example, Microsoft Windows is a type of operating system.

² **Component:** A piece of equipment, a system, software, etc.

³ **Port:** The terminal part where equipment, systems, software, etc. connect or communicate with other external entities. This also includes physical communication ports such as USB ports and LAN ports.

⁴ **Protocol:** The rules and procedures that allow multiple systems to communicate without any problems. It is not possible to communicate using protocols that are not supported.

Route: The paths through which data travels, along with the associated network addresses.

⁶ **Host:** A computer body containing a processing device, storage device, or the like that provides some function to other equipment.

Document reviews

■ Description of security capabilities

30. Least Functionality			
-1.	f this requirement applies, either of the following (1) or (2) is to be implemented.		
(1)	east Functionality		
	To minimise the "Installation, availability, and access rights" of the following items to the		
	ninimum levels necessary.		
	a) Operating systems software components, processes and services.		
	b) Network services, ports, protocols, route and host accesses, and all software.		
(2)	Compensating countermeasure		
	a) Protect against the same threats as the original requirement		
	b) Provide an equal level of protection as the original requirement		
	c) Not be a security control that is required by other requirements		
	d) Not introduce higher security risk		
	-1. If (1) I I I I I I I I I I I I I I I I I I I		

Surveys

30.	30. Least Functionality		
-1.	If this requirement applies, either of the following (1) or (2) is to be performed.		
(1)	Demonstration test for least functionality		
	Unnecessary features and services, if implemented, have been disabled.		
(2)	Confirmation of compensating countermeasure		
	Confirm that the information is as described in the security capability descriptions.		



31. Multifactor authentication for human users

Reg. Table X4.1 Item 31, Part X of the Rules

Ref. IEC62443-3-3 / SR 1.1, RE 2

Multifactor authentication is required for human users when accessing the CBS from or via an untrusted network.

Explanation

Summary

Item 31, Table X4.1, Part X states that <u>Multifactor authentication is required for human users</u> when accessing the CBS from or via an untrusted network. Multifactor authentication means combining two or more different factors and authenticating a human user. According to NIST-SP 800-63¹, authentication factors are classified into following 3(three) types:

Authentication factors	Example
Something you know	It's something only the person knows. For example, password, PIN^2 , etc.
Something you have	It's something only the person has. For example, security tokens ³ , public key authentication method ⁴ , and physical keys ⁵ .
Something you are	It's part of individual body. For example, fingerprints and faces.

Purpose

The purpose is to <u>strengthen the capability to authenticate human users</u>. An untrusted network is a network that is unreliable in terms of security. Therefore, cybersecurity needs to be enhanced by strengthening the authentication process. For detail of the capability to authenticate human users, see "1. Human user identification and authentication".



Human user identification and authentication

P. 53

Countermeasures

NIST: It stands for National Institute of Standards and Technology

² PIN: It stands for Personal Identification Number. One of the authentication codes. Usually consists of 4 to 6 digits.

³ **Security token**: One of the authorization codes. Generally, serves as a temporary certificate for users to access the system. For example, one-time password (OTP) generation device.

⁴ Public key authentication method: A method of authentication using a pair of public and private keys.

⁵ **Physical key**: One of authentication codes. A key to unlock the physical lock such as safe and system.

The countermeasure described here is the capability of multi-factor authentication when authenticating human users. This capability requires that human users be authenticated by two or more authentication factors.

Compensating countermeasures

Compensating countermeasures should be adopted in cases where the aforementioned capabilities or countermeasures have not been implemented.

Scope

This requirement does not apply to the following cases:

- CBS without network communication to untrusted networks

This requirement is not applied with the CBS, because additional security capabilities are not required to the CBS.

Document reviews

Description of security capabilities

31.	Mul	tifactor authentication for human users
-1.	If th	is requirement applies, either of the following (1) or (2) is to be implemented.
(1)	The	capability of multi-factor authentication when authenticating human users
	(a)	Being authenticated by two or more different authentication factors
	(b)	Being able to log in when a valid authenticator is used
(2)	Con	npensating countermeasure
	(a)	Protect against the same threats as the original requirement
	(b)	Provide an equal level of protection as the original requirement
	(c)	Not be a security control that is required by other requirements
	(d)	Not introduce higher security risk

Surveys

31. Multifactor authentication for human users		
-1. If this requirement applies, either of the following (1) or (2) is to be performed.		
(1) Demonstration test for the capability of multi-factor authentication when authenticating		
human users		
(a) Can log in with a valid identifier and authenticator		

	(b) Cannot log in with an invalid authenticator
(2)	Confirmation of compensating countermeasure
	Confirm that the information is as described in Description of security capabilities.



32. Software process and device identification and authentication

Reg. Table X4.1 Item 32, Part X of the Rules

Ref. IEC62443-3-3 / SR 1.2

The CBS shall identify and authenticate software processes and devices

Explanation

Summary

Item 32, Table X4.1, Part X states that it is necessary to <u>identify and authenticate software</u> processes and devices. The software processes and devices are as follows:

Term	Description
Software Process	A program or application used for the CBS.
Device	A physical hardware or machinery used for the CBS.

Purpose

The purpose is to reduce the risk of unauthorized access by allowing the system to authenticate software processes and devices when communicating with untrusted networks. Untrusted networks increase the likelihood of unauthorized access. Therefore, identification and authentication are not only for humans, but also for software processes and devices to provide greater security for communications.

Countermeasures

The countermeasure described here is the capability to identify and authenticate software processes and devices used for the CBS. These are necessary to be identified and authenticated by an identifier and an authenticator, as is the case with human users.

Compensating countermeasures

Compensating countermeasures should be adopted in cases where the aforementioned capabilities or countermeasures have not been implemented.

Scope

This requirement does not apply to the following cases:

- No network communication with untrusted networks

Additional security capabilities are not applied, this requirement is out of scope.

Document reviews

Description of security capabilities

32.	Software process and device identification and authentication
-1.	If this requirement applies, either of the following (1) or (2) is to be implemented.
(1)	The capability to identify and authenticate software processes and devices
	(a) Software process identification and authentication
	i) identifying by an identifier.
	ii) authenticating by an identifier and an authenticator.
	(b) Device identification and authentication
	i) identifying by an identifier.
	ii) authenticating by an identifier and an authenticator.
(2)	Compensating countermeasure
	(a) Protect against the same threats as the original requirement
	(b) Provide an equal level of protection as the original requirement
	(c) Not be a security control that is required by other requirements
	(d) Not introduce higher security risk

Surveys

32.	Softw	vare process and device identification and authentication
-1.	If this	s requirement applies, either of the following (1) or (2) is to be performed.
(1)	Demo	onstration test for the capability to identify and authenticate software processes and
	device	es
	(a) S	Software process identification and authentication
	i	i) Can log in with a valid identifier and authenticator
	i	ii) Cannot log in with an invalid identifier and authenticator
	(b) l	Device identification and authentication
	i	i) Can log in with a valid identifier and authenticator
	i	ii) Cannot log in with an invalid identifier and authenticator
(2)	Confi	irmation of compensating countermeasure
	Confi	irm that the information is as described in Description of security capabilities.



33. Unsuccessful login attempts

Reg. Table X4.1 Item 33, Part X of the Rules

Ref. IEC62443-3-3 / SR 1.11

The CBS shall enforce a limit of consecutive invalid login attempts from untrusted networks during a specified time period.

Explanation

Summary

Item 33, Table X4.1, Part X states that logins over untrusted networks are to be <u>prevented for a specified period of time from repeatedly logging in with the wrong password.</u>

Purpose

The purpose is to <u>defend against continuous cyber-attacks such as brute force attacks¹ or DoS² attacks. Failing to defend against attacks can result in compromised passwords, network outages or system outages.</u>

Countermeasures

The countermeasures described here <u>limit consecutive invalid login attempts within a certain period</u> of time. This capability requires that access be denied if the configured number of attempts is exceeded. In addition, denied access is to continue either for a specified period of time or until unlocked by an administrator.

Compensating countermeasures

Compensating countermeasures should be adopted in cases where the aforementioned capabilities or countermeasures have not been implemented.

Scope

This requirement does not apply to the following cases:

- In 「1. Human user identification and authentication」, compensating countermeasure are to be taken or the requirements do not apply

If user identification and authentication functionality is not implemented, there is no identifier. In

¹ **Brute force attack:** A cyberattack technique that tries every possible combination to crack a password. In some cases, thousands of login attempts may be made using automated tools over a short period of time.

² DoS: Means "denial of service" and includes "distributed denial of service (DDoS) attacks among others. DoS attacks use multiple computers and devices to disrupt systems on a large scale by sending massive amounts of traffic to websites and servers.

Human user identification and authentication

P. 53

- No network communication with untrusted networks

Since additional security capabilities do not apply, this requirement also does not apply.

Document reviews

Description of security capabilities

33.	Unsu	ccessful login attempts			
-1.	If thi	is requirement applies, any of the following capability or countermeasures (1) or (2) is			
	to be	e implemented:			
(1)	Capa	Capability to limit consecutive invalid login attempts			
	The	following items are met:			
	(a)	Access is denied when the number of consecutive invalid login attempts exceeds the			
		configured number of attempts.			
	(b)	Denied access lasts either for a specified period of time or until unlocked by an			
		administrator.			
(2)	Com	pensating countermeasure			
	(a)	Protect against the same threats as the original requirement			
	(b)	Provide an equal level of protection as the original requirement			
	(c)	Not be a security control that is required by other requirements			
	(d)	Not introduce higher security risk			

Surveys

33.	nsuccessful login attempts	
-1.	f this requirement applies, either of the following (1) or (2) is to be performed.	
(1)	Demonstration test for the capability to identify and authenticate software processes and	
	evices	
	The following items are met:	
	a) Deny access if the number of consecutive invalid login attempts exceeds the	
	configured number of attempts	
	b) Denied access is to be last for a specified period of time or until unlocked by an	
	administrator	
(2)	Confirmation of compensating countermeasure	



34. System use notification

Reg. Table X4.1 Item 34, Part X of the Rules

Ref. IEC62443-3-3 / SR 1.12

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.

Explanation

Summary

Item 34, Table X4.1, Part X states that <u>a system use notification message is required to be displayed</u>. A system use notification message is a message that is displayed before a person is logged into the system.

Purpose

The purpose is to require the user to agree to the terms and conditions of use of the system, including the system's terms of use and security policy, before using the system. Such an agreement clarifies to the user his/her responsibilities in relation to the use of the system.

Countermeasures

This requires that the message is displayed before human users can be authorised. It also requires the capability to configurate the message. The reason for this is so that if the system's terms of use or security policy changes, they can be properly reflected. The edit function must only be able to be edited by authorised persons, e.g., administrators, to ensure that the appropriate messages are displayed.

Note The following is an example of what is typically included in a system usage notification message. These are for reference and are not necessarily limited to them.

- that the individual is accessing a specific CBS.
- that system usage may be monitored, recorded and subject to audit.
- That unauthorized use of the system is prohibited.
- That use of the system indicates consent to monitoring and recording.

Compensating countermeasures

Compensating countermeasures should be adopted in cases where the aforementioned capabilities or countermeasures have not been implemented.

Scope

This requirement does not apply to the following cases:

- No network communication with untrusted networks

Additional security capabilities are not applied, this requirement is out of scope.

- No HMI is implemented.

If the system does not have an HMI, such as a monitor for displaying system usage notification messages, this requirement does not apply.

Document reviews

■ Description of security capabilities

34.	34. System use notification		
-1.	If th	is requirement applies, either of the following (1) or (2) is to be implemented.	
(1)	The	capability to display and configurate a system use notification message	
	The	following capabilities should be implemented.	
	(a)	The capability to display a system use notification message	
		Displaying a system use notification message before authenticating.	
	(b)	The capability to configurate a system use notification message	
		Can be configurable by authorized personnel.	
(2)	Con	npensating countermeasure	
	(a)	Protect against the same threats as the original requirement	
	(b)	Provide an equal level of protection as the original requirement	
	(c)	Not be a security control that is required by other requirements	
	(d)	Not introduce higher security risk	

Surveys

■ Test procedure of security capabilities

34.	34. System use notification		
-1.	If this requirement applies, either of the following (1) or (2) is to be performed.		
(1)	The capability to display and configurate a system use notification message		
	The following capabilities should be implemented.		
	(a) The capability to display a system use notification message		
	Displaying a system use notification message before authenticating.		
	(b) The capability to configurate a system use notification message		
	The following items are to be satisfied.		

i) Can be configurable by authorized personnel.
ii) Cannot be configurable by unauthorized personnel.
(2) Confirmation of compensating countermeasure
Confirm that the information is as described in Description of security capabilities.



35. Access via Untrusted Networks

Reg. Table X4.1 Item 35, Part X of the Rules

Ref. IEC62443-3-3 / SR 1.13

Any access to the CBS from or via untrusted networks shall be monitored and controlled.

Explanation

Summary

Item 35, Table X4.1, Part X states that access via untrusted networks is to be monitored and controlled.

Purpose

The purpose is to monitor access from untrusted networks and restrict or block specific access as necessary. This prevents unauthorized access by attackers.

Countermeasures

The countermeasure described here is the capability to monitor and control access. For example, incorporating intrusion detection systems (IDS).

Compensating countermeasures

Compensating countermeasures should be adopted in cases where the aforementioned capabilities or countermeasures have not been implemented. The following is an example of a compensating countermeasure.

- Monitoring and controlling access by external security instruments

If this capability is not provided to the system, this function is complemented by external security instruments.

Scope

This requirement does not apply to the following cases:

- No network communication with untrusted networks

Additional security capabilities are not applied, this requirement is out of scope.

Document reviews

Description of security capabilities

35.	35. Access via Untrusted Networks	
-1.	If this requirement applies, either of the following (1) or (2) is to be implemented.	
(1)	The capability to monitor and control access via untrusted networks	
(2)	Compensating countermeasure	
	(a) Protect against the same threats as the original requirement	
	(b) Provide an equal level of protection as the original requirement	
	(c) Not be a security control that is required by other requirements	
	(d) Not introduce higher security risk	

Surveys

■ Test procedure of security capabilities

35. Access via Untrusted Networks □ -1. If this requirement applies, either of the following (1) or (2) is to be performed. □ (1) Demonstration test for the capability to monitor and control access via untrusted networks □ (2) Confirmation of compensating countermeasure Confirm that the information is as described in Description of security capabilities.



36. Explicit access request approval

Reg. Table X4.1 Item 36, Part X of the Rules

Ref. IEC62443-3-3 / SR 1.13, RE 1

The CBS shall deny access from or via untrusted networks unless explicitly approved by authorized personnel on board.

Explanation

Summary

Item 36, Table X4.1, Part X states that it is necessary to <u>deny access from or via untrusted networks</u> unless explicitly approved by authorized personnel on board.

Purpose

The purpose is to deny unauthorized access requests from untrusted networks. This prevents unauthorized access by attackers.

Countermeasures

The countermeasure described here is the capability to deny access from or via untrusted networks unless explicitly approved by authorized personnel on board. Specifically, the following two capabilities apply.

- The capability to assign access approval permissions to human users
- The capability to deny unapproved access

Compensating countermeasures

Compensating countermeasures should be adopted in cases where the aforementioned capabilities or countermeasures have not been implemented.

Scope

This requirement does not apply to the following cases:

- No network communication with untrusted networks

Additional security capabilities are not applied, this requirement is out of scope.

Document reviews

Description of security capabilities

36.	Explicit access request approval	
-1.	If this requirement applies, either of the following (1) or (2) is to be implemented.	
(1)	The capability to deny access from or via untrusted networks unless explicitly approved	
	by authorized personnel on board	
	(a) The capability to assign access approval permissions to human users	
	(b) The capability to deny unapproved access	
(2)	(2) Compensating countermeasure	
	(a) Protect against the same threats as the original requirement	
	(b) Provide an equal level of protection as the original requirement	
	(c) Not be a security control that is required by other requirements	
	(d) Not introduce higher security risk	

Surveys

■ Test procedure of security capabilities

36.	Explicit access request approval
-1.	If this requirement applies, either of the following (1) or (2) is to be performed.
(1)	The Demonstration test for the capability to deny access from or via untrusted networks
	unless explicitly approved by authorized personnel on board
	(a) The capability to assign access approval permissions to human users
	(b) The capability to deny unapproved access
(2)	Confirmation of compensating countermeasure
	Confirm that the information is as described in Description of security capabilities.



37. Remote session termination

Reg. Table X4.1 Item 37, Part X of the Rules

Ref. IEC62443-3-3 / SR 2.6

The CBS shall provide the capability to terminate a remote session either automatically after a configurable time period of inactivity or manually by the user who initiated the session.

Explanation

Summary

Item 37, Table X4.1, Part X states that <u>the remote session is to be terminated manually or automatically</u>. **Remote session** is a remotely accessed session to a CBS from a remote location, e.g., via the internet.

Purpose

The purpose is to terminate a session as soon as the required remote session has ended. This prevents unnecessary sessions remaining connected and prevents unauthorized access.

Countermeasures

The countermeasure described here is the function to terminate the remote access session. Specifically, the function to log out of the remote session, either automatically or manually.

Countermeasure	Description
Automatic	This function automatically logs out the user after a set period of inactivity.
termination	
Manual	Capabilities should be provided on the side receiving remote access (local
termination	side) and on the side accessing remotely (remote side), so that the session can
	be terminated by an operation of the user who initiated the session.
	Functionality on the local side includes the function to block session ID
	connections, e.g., on the administrator's screen. The local side functions are
	such as the function to block session ID connections on the administrator's
	screen. On the remote side, functions such as a logout function.

Compensating countermeasures

Compensating countermeasures should be adopted in cases where the aforementioned capabilities or countermeasures have not been implemented.

Scope

This requirement does not apply to the following cases:

- No network communication with untrusted networks

Additional security capabilities are not applied, this requirement is out of scope.

- No remote access functionality

This requirement does not apply if there is only local network communication.

Document reviews

Description of security capabilities

37.	37. Remote session termination		
-1.	If th	is requirement applies, either of the following (1) or (2) is to be implemented.	
(1)	Cap	ability to terminate a remote session	
	Eith	er of the following functions is to be implemented.	
	(a)	Capability to terminate a remote session automatically	
		The following items are to be complied with.	
		i) The inactivity time until the end of the session is to be configurable.	
		ii) The session is to be terminated after a configurable period of inactivity.	
	(b)	Capability to manually terminate a remote session.	
		The session is to be terminated by operation of the user.	
(2)	Con	npensating countermeasure	
	(a)	Protect against the same threats as the original requirement	
	(b)	Provide an equal level of protection as the original requirement	
	(c)	Not be a security control that is required by other requirements	
	(d)	Not introduce higher security risk	

Surveys

■ Test procedure of security capabilities

37. Remote session termination	
-1. If this requirement applies, either of the following (1) or (2) is to be performed.	
(1) The demonstration test for the capability to terminate a remote session	
Either of the following functions is to be implemented.	
(a) Capability to terminate a remote session automatically	
The following items are to be complied with.	
i) The inactivity time until the end of the session is to be configurable.	

ii) The session is to be terminated after a configurable period of inactivity.
(b) Capability to manually terminate a remote session.
The session is to be terminated by operation of the user.
(2) Confirmation of compensating countermeasure
Confirm that the information is as described in Description of security capabilities.



38. Cryptographic integrity protection

Reg. Table X4.1 Item 38, Part X of the Rules

Ref. IEC62443-3-3 / SR 3.1, RE 1

The CBS shall employ cryptographic mechanisms to recognize changes to information during communication with or via untrusted networks.

Explanation

Summary

Item 38, Table X4.1, Part X states that it is necessary to <u>recognize changes to information during communication by cryptographic technology</u>. "cryptographic technology" refers to technology used to ensure that information has not been altered, tampered with or corrupted between source and destination.

Purpose

The purpose is to <u>recognise changes to information during communication</u>. Failure to detect unauthorised changes to information could result in incorrect information being communicated to the system, which could affect system operation.

Countermeasures

The countermeasure described here is the cryptographic mechanisms to recognise changes to information during communication. For example, it is applicable to Digital signatures ¹. Cryptography is explained in detail in "22. Use of cryptography".



Use of cryptography

P. 109

Compensating countermeasures

Compensating countermeasures should be adopted in cases where the aforementioned capabilities or countermeasures have not been implemented.

Scope

This requirement does not apply to the following cases:

- No network communication with untrusted networks

Additional security capabilities are not applied, this requirement is out of scope.

¹ **Digital signature:** Technology to prove that the sender of a message is the author of that message and to ensure that the message has not been tampered with after transmission

Document reviews

Description of security capabilities

38. Cryptographic integrity protection	
-1.	If this requirement applies, any of the following mechanisms or countermeasures (1) or (2)
	is to be implemented:
(1)	The cryptographic mechanisms to recognise changes to information during
communication	
(2)	Compensating countermeasure
	(a) Protect against the same threats as the original requirement
	(b) Provide an equal level of protection as the original requirement
	(c) Not be a security control that is required by other requirements
	(d) Not introduce higher security risk

Surveys

■ Test procedure of security capabilities

This requirement will be verified through the document reviews. Therefore, the surveys are not required.



39. Input validation

Reg. Table X4.1 Item 39, Part X of the Rules

Ref. IEC62443-3-3 / SR 3.5

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.

Explanation

Summary

Item 39, Table X4.1, Part X states that it is necessary to <u>validate any input data via untrusted</u> networks.

Purpose

On untrusted networks, attackers are more likely to enter unauthorised data. Security should be improved by validating input data and preventing unauthorized data from being received.

Countermeasures

The countermeasure described here is the capability to validate the syntax, length and content of any input data.

Countermeasure	Description
Syntax validation	Checks whether the input data conforms to the specified format and
	rules. For example, checks whether the data type, format, character
	encoding, and encoding of numbers and dates are correct.
Length validation	Checks whether the input data is within the specified length or range. For
	example, checks whether the number of characters, number of digits, and
	maximum and minimum values are appropriate.
Content validation	Checks whether the input data meets the specified conditions or criteria.
	For example, checks whether the input data contains missing, prohibited, or
	inconsistent values.

"Validation" refers to a series of processes, including the processing of validation results. In other words, it is necessary to clarify how to respond to invalid data, such as refusing to accept the data if it is determined to be invalid.

Compensating countermeasures

Compensating countermeasures should be adopted in cases where the aforementioned capabilities or countermeasures have not been implemented.

Scope

This requirement does not apply to the following cases:

- No network communication with untrusted networks

Additional security capabilities are not applied, this requirement is out of scope.

Document reviews

Description of security capabilities

39.	39. Input validation	
-1.	If th	is requirement applies, either of the following (1) or (2) is to be implemented.
(1)	The	capability to validate the syntax, length and content of any input data
	(a)	Verify the following input data elements
		i) Syntax
		ii) Length
		iii) Content
	(b)	If the data is determined to be invalid, take appropriate action. (e.g., refuse to accept
		the input data.)
(2)	Compensating countermeasure	
	(a)	Protect against the same threats as the original requirement
	(b)	Provide an equal level of protection as the original requirement
	(c)	Not be a security control that is required by other requirements
	(d)	Not introduce higher security risk

Surveys

■ Test procedure of security capabilities

39.	39. Input validation	
-1.	-1. If this requirement applies, either of the following (1) or (2) is to be performed.	
(1)	Demonstration test for the capability to validate the syntax, length and content of any	
	input data	
	If the data is determined to be invalid, take appropriate action. (e.g., refuse to accept the	
	input data.)	
(2)	Confirmation of compensating countermeasure	
	Confirm that the information is as described in Description of security capabilities.	



40. Session integrity

Reg. Table X4.1 Item 40, Part X of the Rules

Ref. IEC62443-3-3 / SR 3.8

The CBS shall protect the integrity of sessions¹. Invalid session IDs shall be rejected.

Explanation

Summary

Item 40, Table X4.1, Part X states that it is necessary to protect the integrity of sessions and reject invalid session IDs. To protect the integrity of sessions means that the session is associated with authorised users and maintains this association, using the session ID. The session ID refers to the identifier (ID) that identifies the session.

Purpose

The purpose is to <u>prevent unauthorised use of the session ID</u>. If the integrity of the session ID is not protected, the session ID can be abused by a session hijacking² or a session fixation³.

Countermeasures

The countermeasure described here is two capabilities as follows.

- The capability to protect the integrity of sessions
- The capability to reject invalid session IDs

Compensating countermeasures

Compensating countermeasures should be adopted in cases where the aforementioned capabilities or countermeasures have not been implemented.

Scope

This requirement does not apply to the following cases:

- No network communication with untrusted networks

Additional security capabilities are not applied, this requirement is out of scope.

- If the session is not used

If the session is not used, e.g., no browser functionality, this requirement does not apply.

¹ **Session** A sequence of operations from the time a session user logs into the system to the time he logs out. **Session ID** is a unique identifier (ID) that identifies the session used by the user.

² Session hijacking An attack technique that illegally hijacks an existing session

³ **Session fixation** An attack technique in which the attacker forces the victim to use a pre-determined session ID and impersonates the victim.

Document reviews

Description of security capabilities

40. Session integrity
-1. If this requirement applies, either of the following (1) or (2) is to be implemented.
(1) The capability to protect the integrity of sessions and reject invalid session IDs
The following items are to be satisfied.
(a) Protecting the integrity of sessions and reject invalid session IDs
(b) Rejecting invalid session IDs
(2) Compensating countermeasure
(a) Protect against the same threats as the original requirement
(b) Provide an equal level of protection as the original requirement
(c) Not be a security control that is required by other requirements
(d) Not introduce higher security risk

Surveys

■ Test procedure of security capabilities

rest procedure or security capabilities		
	40.	Session integrity
	-1.	If this requirement applies, either of the following (1) or (2) is to be performed.
	(1)	Demonstration test for the capability to protect the integrity of sessions and reject invalid
		session IDs
		The following items are to be satisfied.
		(a) Protecting the integrity of sessions and reject invalid session IDs
		(b) Rejecting invalid session IDs
	(2)	Confirmation of compensating countermeasure
		Confirm that the information is as described in Description of security capabilities.
ľ	Note:	There are other required capabilities with respect to sessions. Please refer to the
f	ollow	ving pages
] s	Session lock P. 84
Ц	I	nvalidation of session IDs after session termination P.154



41. Invalidation of session IDs after session

termination

Reg. Table X4.1 Item 41, Part X of the Rules

Ref. IEC62443-3-3 / SR 3.8, RE 1

The system shall invalidate session IDs¹ upon user logout or other session termination (including browser sessions).

Explanation

Summary

Item 41, Table X4.1, Part X states that it is necessary to invalidate session IDs upon user logout or other session termination (including browser sessions).

Purpose

The purpose is to prevent the risk of session abuse by quickly disabling the session ID. If the session ID remains valid after the session is terminated, the session ID can be abused by a session hijacking² or a session fixation³.

Countermeasures

The countermeasure described here is the capability to invalidate session IDs upon user logout or other session termination (including browser sessions).

Compensating countermeasures

Compensating countermeasures should be adopted in cases where the aforementioned capabilities or countermeasures have not been implemented.

Scope

This requirement does not apply to the following cases:

- No network communication with untrusted networks

Additional security capabilities are not applied, this requirement is out of scope.

- If the session is not used

If the session is not used, e.g., no browser functionality, this requirement does not apply.

¹ **Session** A sequence of operations from the time a session user logs into the system to the time he logs out. **Session ID** is a unique identifier (ID) that identifies the session used by the user.

² Session hijacking An attack technique that illegally hijacks an existing session

³ **Session fixation** An attack technique in which the attacker forces the victim to use a pre-determined session ID and impersonates the victim.

Document reviews

Description of security capabilities

	41.	Invalidation of session IDs after session termination
	-1.	If this requirement applies, either of the following (1) or (2) is to be implemented.
	(1)	The capability to invalidate session IDs upon user logout or other session termination
		(including browser sessions)
	(2)	Compensating countermeasure
		(a) Protect against the same threats as the original requirement
		(b) Provide an equal level of protection as the original requirement
		(c) Not be a security control that is required by other requirements
		(d) Not introduce higher security risk
S	Surv	eys
	Tes	t procedure of security capabilities
		Invalidation of session IDs after session termination
	41.	Invalidation of session IDs after session termination
	41. -1.	Invalidation of session IDs after session termination If this requirement applies, either of the following (1) or (2) is to be performed.
	41. -1.	Invalidation of session IDs after session termination If this requirement applies, either of the following (1) or (2) is to be performed. Demonstration test for the capability to invalidate session IDs upon user logout or other
	41. -1. (1)	Invalidation of session IDs after session termination If this requirement applies, either of the following (1) or (2) is to be performed. Demonstration test for the capability to invalidate session IDs upon user logout or other session termination (including browser sessions)
	41. -1. (1)	Invalidation of session IDs after session termination If this requirement applies, either of the following (1) or (2) is to be performed. Demonstration test for the capability to invalidate session IDs upon user logout or other session termination (including browser sessions) Confirmation of compensating countermeasure
	411. (1) (2) Note:	Invalidation of session IDs after session termination If this requirement applies, either of the following (1) or (2) is to be performed. Demonstration test for the capability to invalidate session IDs upon user logout or other session termination (including browser sessions) Confirmation of compensating countermeasure
	41. (1) (2) Note:	Invalidation of session IDs after session termination If this requirement applies, either of the following (1) or (2) is to be performed. Demonstration test for the capability to invalidate session IDs upon user logout or other session termination (including browser sessions) Confirmation of compensating countermeasure Confirm that the information is as described in Description of security capabilities. There are other required capabilities with respect to sessions. Please refer to the

Chapter 6 Explanation of Secure Development Lifecycle requirements

This chapter provides details on the secure development lifecycle required by Part X (UR E27). In this context, "secure product development lifecycle" means the lifecycle for the development and maintenance of secure products. This includes, for example, the delivery of security updates after delivery and security defence-in-depth strategies. This lifecycle incorporates some of the requirements of the standard IEC 62443-4-1 into Chapter 4, Part X (UR E27).

Overview of Secure Development Lifecycle requirements

■ What are Secure Development Lifecycle requirements?

Chapter 4, Part X (UR E27) includes seven secure product development lifecycle requirements that reference IEC 62443-4-1. These requirements are as follows.

Secure Development Lifecycle Requirements

1. Controls for private keys	P. 159
2. Security update documentation	P. 161
3. Dependent component and Operation system security update documentation	P. 163
4. Security update delivery	P. 165
5. Product defence in depth	P. 167
6. Defence in depth measures expected in the environment	P. 169
7. Security hardening guidelines	P. 171

■ Requires processes or controls according to the secure product

development lifecycle

Manufacturers are required to implement <u>processes or controls according to the secure product</u> <u>development lifecycle</u> to ensure that their products remain secure at each stage, including the design,

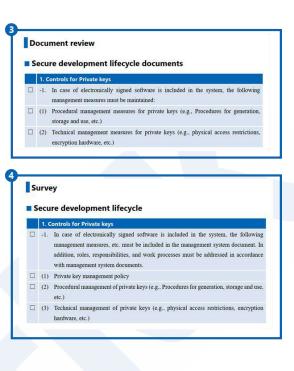
manufacturing and maintenance stages.

These processes and management means are procedures or instructions that manufacturers are to follow to maintain secure products. They can, for example, be the processes for creating procedures to provide security updates or the processes for creating security defences and are addressed as part of management systems defined by manufacturers. Therefore, they are to be documented in management system documents, such as quality control manuals or associated procedures.

Detail of Secure Development Lifecycle requirements

How to read the following pages





1 Requirements

The names and details for the secure product development lifecycle requirements. Chapter 4, Part X (UR E27) provides two rules for each requirement.

2 Explanation

The explanation of the secure product development lifecycle requirements.

B Documentation review

A document review checklist for the secure product development lifecycle requirements

- Secure Development Lifecycle Document: Documentation required by 4.4.1(6), Part X.

4 Survey

A survey checklist for the secure product development lifecycle requirements.

- Secure Development Lifecycle: Surveys required by 2.2.3-4, Part X

1. Controls for private keys

Reg. 4.5.2, Part X of the Rules

Ref. IEC62443-4-1 / SM-8

The manufacturer shall have procedural and technical controls in place to protect private keys used for code signing, if applicable, from unauthorized access or modification.

Reg. 2.2.3-4 (1), Part X of the Rules

This requirement applies if the system includes software that is digitally signed for the purpose of enabling the user to verify its authenticity.

The supplier shall present management system documentation substantiating that policies, procedures and technical controls are in place to protect generation, storage and use of private keys used for code signing from unauthorized access.

The policies and procedures shall address roles, responsibilities and work processes. The technical controls shall include e.g. physical access restrictions and cryptographic hardware (e.g. Hardware security module¹) for storage of the private key.

Explanation

This section describes the management of private keys used for code signing.

Code signing is a technique for the electronic signing² of software by developers to ensure that it has not been tampered with and that its software was made by the specified developer. The private keys used to sign codes are an important part of proving software developer identity.

The controls described here is to <u>have procedural and technical controls in place to protect private</u> keys used for code signing from unauthorised access or tampering.

The following are some examples of procedural controls.

- Defining roles and responsibilities for the handling of private keys.
- Generating private keys in secure environments with limited access.
- Storing private keys with encryption, password protection and other measures.
- Work processes, such as approval and recording, are established for the use of private keys.

The following are some examples of technical control.

 Private keys are stored in external storage media such as USB memory sticks or SD cards and said media are then further stored in lockable places such as safes or lockers as a physical access control.

¹ Hardware Security Module (HSM): Dedicated hardware devices that securely generate and store private keys. HSM securely stores confidential information and protects it from unauthorized access and tampering.

² Electronically signing: Mechanisms that use electronic means to certify that the senders and contents of documents or messages are correct. Electronic signatures include public key cryptography, digital certificates, and other technologies.

- Private keys are stored in single-purpose devices such as hardware security modules as a cryptographic hardware control.

In addition, the controls described above, including the private key management policy, are to be established by manufacturers. Furthermore, surveys of management system documentation and records are required to verify the establishment of such controls, and the management policy should include relevant roles and responsibilities.

Document reviews

Secure development lifecycle documents

1. C	1. Controls for private keys	
-1.	-1. If the system includes software that is digitally signed, either of the following controls are	
	to be maintained.	
(1)	Procedural controls for private keys (e.g., procedures for generation, storage and use)	
(2)	Technical controls for private keys (e.g., physical access restrictions and encryption	
	hardware)	

Surveys

Secure development lifecycle

1. Controls for private keys If the system includes software that is digitally signed, the following controls are to be included in the management system documentation. In addition, roles, responsibilities and work processes are to be addressed in accordance with the management system documentation. (1) Private key control policy (2) Procedural controls for private keys (e.g., procedures for generation, storage and use) (3) Technical controls for private keys (e.g., physical access restrictions and encryption hardware)

2. Security update documentation

Reg. 4.5.3, Part X of the Rules

Ref. IEC62443-4-1 / SUM-2

A process shall be employed to ensure that documentation about product security updates is made available to users (which could be through establishing a cyber security point of contact or periodic publication which can be accessed by the user) that includes but is not limited to:

- (1) The product version number(s) to which the security patch¹ applies;
- (2) Instructions on how to apply approved patches manually and via an automated process;
- (3) Description of any impacts that applying the patch to the product can have, including reboot;
- (4) Instructions on how to verify that an approved patch has been applied; and
- (5) Risks of not applying the patch and mediations that can be used for patches that are not approved or deployed by the asset owner.

Reg. 2.2.3-4 (2), Part X of the Rules

The supplier² shall present management system documentation substantiating that a process is established in the organization to ensure security updates are informed to the users. The information to the users shall include the items listed in section 5.2.

Explanation

This section describes the security update documentation.

The response is to <u>adopt a process for system owners to obtain the security update documentation</u>. The security update documentation is to include the following:

- The product version number(s) to which the security patch applies

Security patches are additional programs that are distributed to solve problems contained in the current software. The security update documentation is to make clear which version of the software the security patch is intended for.

- 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 applied
- Risks of not applying the patch and mediations that can be used for patches that are not approved or deployed by the asset owner

"Mediation" refers to the risk mitigation measures that can be substituted for unapproved patches. Such measures are necessary to clarify and make decisions based on the risks of non-patching and mediation.

¹ (Security) Patch: Software designed to update installed software or data to address security vulnerabilities and bugs, or to improve operating systems or applications.

² Supplier: The manufacturers or providers of systems. Suppliers are responsible for providing systems to system integrators or system owners.

Processes are to <u>be established by organisations to inform system owners of security updates</u>. Furthermore, surveys of management system documentation and records are required to verify the establishment of such processes.

Document reviews

■ Secure development lifecycle documents

2. Security update documentation	
-1.	Verify that a process has been adopted to ensure that security update documentation,
	including the following items, is available to users.
(1)	The product version number(s) to which the security patch applies
(2)	Instructions on how to apply approved patches manually and via an automated process
(3)	Description of any impacts that applying the patch to the product can have, including
	reboot
(4)	Instructions on how to verify that an approved patch has been applied
(5)	Risks of not applying the patch and mediations that can be used for patches that are not
	approved or deployed by the asset owner

Surveys

■ Secure development lifecycle

2. 5	Security update documentation
-1.	The management system documentation includes a process for informing system owners
	of security updates.
	The information to be provided to the system owner shall include the following items:
(1)	The product version number(s) to which the security patch applies
(2)	Instructions on how to apply approved patches manually and via an automated process
(3)	Description of any impacts that applying the patch to the product can have, including
	reboot
(4)	Instructions on how to verify that an approved patch has been applied
(5)	Risks of not applying the patch and mediations that can be used for patches that are not
	approved or deployed by the asset owner

3. Dependent component and Operation system security update documentation

Reg. 4.5.4, Part X of the Rules

Ref. IEC62443-4-1 / SUM-3

A process shall be employed to ensure that documentation about dependent component or operating system security updates is available to users that includes but is not limited to:

(1) Stating whether the product is compatible with the dependent component or operating system security update;

Reg. 2.2.3-4 (3), Part X of the Rules

The supplier shall present management system documentation, as required by section 5.3, substantiating that a process is established in the organization to ensure users are informed whether the system is compatible with updated versions of acquired software in the system (new versions/patches of operating system or firmware). The information shall address how to manage risks related to not applying the updated acquired software.

Explanation

This section describes the documentation for security updates for dependent components or operating systems.

Dependent components are products that are included in systems to ensure proper operation. Since such components are often manufactured by someone other than suppliers, security updates are delivered by someone other than system suppliers. Moreover security updates for base operating systems are delivered by the vendors that provide the platforms; for example, Microsoft provides updates for its Windows operating system.

The controls described here is to <u>adopt processes for system owners to obtain documentation on security updates for dependent components or operating systems</u>. Documentation of security updates is to include statements about whether the dependent components or operating systems support security updates.

In addition, processes are to be established by organisations to inform system owners whether the system supports updated versions of acquired software. If systems do not support acquired software, information such as the risks of not applying updates and measures to reduce such risks shall be included. Furthermore, surveys of management system documentation and records are required to verify the establishment of such processes.

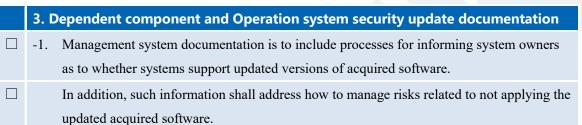
Document reviews

■ Secure development lifecycle documents

3. Dependent component and Operation system security update documentation -1. System owners have adopted processes to obtain security update documents for dependent components or operating systems that include the following. Stating whether the product is compatible with the dependent component or operating system security update

Surveys

■ Secure development lifecycle



4. Security update delivery

Reg. 4.5.5, Part X of the Rules

Ref. IEC62443-4-1 / SUM-4

A process shall be employed to ensure that security updates for all supported products and product versions are made available to product users in a manner that facilitates verification that the security patch¹ is authentic.

IACS supplement: The manufacturer shall have QA process² to test the updates before releasing.

Reg. 2.2.3-4 (4), Part X of the Rules

The supplier shall present management system documentation, as required by section 5.4, substantiating that a process is established in the organization ensuring that system security updates are made available to users, and describing how the user may verify the authenticity of the updated software.

Explanation

This section describes security update delivery.

The control here is to require <u>system owners to adopt processes for obtaining security updates in</u> <u>ways that ensure security patches are authentic.</u> Testing before releasing security updates are to be specified in the QA process.

Processes are also to be <u>established by organisations to ensure that security updates are made</u> <u>available to system owners</u>. The security patches provided here are to be verified as authentic, as described above. Furthermore, onsite surveys of management system documentation and records are required to verify the establishment of such processes.

Document reviews

Secure development lifecycle documents

4. Security Update Delivery

- -1. Processes to acquire security updates for system owners shall be adopted in ways that ensure that security patches are authentic.
- -2. QA process shall be adopted for the test of updates before the release of a security update.

¹ (Security) Patch Software designed to update installed software or data to address security vulnerabilities and bugs or to improve an operating system or application

² QA process Quality Assurance process. A sequence of activities to ensure that a product or service meets specific requirements, standards, or metrics.

Surveys

■ Secure development lifecycle

4. Security Update Delivery -1. Management system documentation is to include processes for ensuring that security updates are provided to system owners. In addition, such information is to include ways for verifying the authenticity of the updated software.

5. Product defence in depth

Reg. 4.5.6, Part X of the Rules

Ref. IEC62443-4-1 / SG-1

A process shall exist to create product documentation that describes the security defence in depth strategy for the product to support installation, operation and maintenance that includes:

- (1) Security capabilities implemented by the product and their role in the defence in depth strategy;
- (2) Threats addressed by the defence in depth strategy; and
- (3) Product user mitigation strategies for known security risks associated with the product, including risks associated with legacy code¹.

Reg. 2.2.3-4 (5), Part X of the Rules

The supplier shall present management system documentation, as required by section 5.5, substantiating that a process is established in the organization to document a strategy for defence-in-depth measures to mitigate security threats to software in the CBS during installation, maintenance and operation.

Examples of threats could be installation of unauthorised software, weaknesses in the patching process, tampering with software in the operational phase of the ship.

Explanation

This section describes the product defence-in-depth.

"Defence-in-depth" is a strategy that reduces security risks by combining multiple security measures, rather than relying on a single security measure.

The response here is to <u>adopt a process that describes a defence-in-depth strategy for security.</u>

Product documentation is to include the following:

- Security capabilities implemented by the product and their role in the defence in depth strategy

Identify the specific security capabilities the product provides and describe how each works in the defence-in-depth strategy.

- Threats addressed by the defence in depth strategy

Identify specific threats addressed by the defence-in-depth strategy and describe how each affects the security layer of the product. An example of a threat is as stated in the requirements.

- Product user mitigation strategies for known security risks associated with the product, including risks associated with legacy code

Describes measures to mitigate or eliminate known security risks. Especially, older source code,

¹ **Legacy code**: Programs created by using outdated technologies or techniques. This could include security risks such as not being able to comply with the latest security standards or not being able to apply the latest security patches.

called legacy code, may contain security risks such as not complying with new security standards or being unable to apply security patches.

<u>The processes described above are to be established by organizations</u>. Furthermore, surveys of management system documentation and records are required to verify the establishment of such processes.

Document reviews

Secure development lifecycle documents

5. P	5. Product defence in depth	
-1.	Processes have been adopted for developing security defence-in-depth strategies,	
	including the following product documentation.	
(1)	Security capabilities implemented by the product and their role in the defence in depth	
	strategy	
(2)	Threats addressed by the defence in depth strategy	
(3)	Product user mitigation strategies for known security risks associated with the product,	
	including risks associated with legacy code	

Surveys

Secure development lifecycle

5. Product defence in depth

-1. Management system documentation is to include processes for creating security defence-in-depth strategies.

6. Defence in depth measures expected in the

environment

Reg. 4.5.7, Part X of the Rules

Ref. IEC62443-4-1 / SG-2

A process shall be employed to create product user documentation that describes the security defence in depth measures expected to be provided by the external environment in which the product is to be used.

Reg. 2.2.3-4 (6), Part X of the Rules

The supplier shall present management system documentation, as required by section 5.6, substantiating that a process is established in the organization to document defence-in-depth measures expected to be provided by the external environment, such as physical arrangement, policies and procedures.

Explanation

This section describes the defence-in-depth measures expected to be provided for external environments. The following are some examples of such measures.

Defence-in-depth	Examples
measures	
Physical	Locked doors, security boxes, etc.
arrangement	
Policy	Use encryption, how data is stored and destroyed, etc.
Procedure	Backup critical data, steps to recover from data loss, etc.

The controls described here are to <u>adopt processes</u> that <u>describe the security defence-in-depth</u> <u>measures expected to be provided by the external environments in which products are used</u>. This is important for building defence-in-depth in combination with external security measures and product security measures.

<u>In addition, the processes described above are to be established by organizations</u>. Furthermore, surveys of management system documentation and records are required to verify the establishment of such processes.

Document reviews

Secure development lifecycle documents



-1. Processes have been adopted to develop documentation for product users that describes the security defence-in-depth measures expected to be provided by the external environments in which the products are used.

Surveys

■ Secure development lifecycle

6. Defence in depth measures expected in the environment

-1. Management system documentation is to include processes for creating product user documentation that describes the security defence-in-depth measures expected to be provided by the external environments in which the products are used.

7. Security hardening guidelines

Reg. 4.5.8, Part X of the Rules

Ref. IEC62443-4-1 / SG-3

A process shall be employed to create product user documentation that includes guidelines for hardening¹ the product when installing and maintaining the product. The guidelines shall include, but are not limited to, instructions, rationale and recommendations for the following:

- (1) Integration of the product, including third-party components, with its product security context
- (2) Integration of the product's application programming interfaces ²/protocols ³ with user applications⁴;
- (3) Applying and maintaining the product's defence in depth strategy⁵
- (4) Configuration and use of security options/capabilities in support of local security policies, and for each security option/capability:
 - (a) its contribution to the product's defence in depth strategy
 - (b) descriptions of configurable and default values that include how each affects security along with any potential impact each has on work practices; and
 - (c) setting/changing/deleting its value;
- (5) Instructions and recommendations for the use of all security-related tools and utilities that support administration, monitoring, incident handling and evaluation of the security of the product;
- (6) Instructions and recommendations for periodic security maintenance activities;
- (7) Instructions for reporting security incidents for the product to the supplier;
- (8) Description of the security best practices⁶ for maintenance and administration of the product.

Reg. 2.2.3-4 (7), Part X of the Rules

The supplier shall present management system documentation, as required by section 5.7, substantiating that a process is established in the organization to ensure that hardening guidelines are produced for the system.

The guidelines shall specify how to reduce vulnerabilities in the system by removal/prohibiting /disabling of unnecessary software, accounts, services, etc.

Explanation

¹ Hardening: The process of minimizing a system's susceptibility to attacks by decreasing the system's attack surface area.

² Application Programming Interface (API): Reducing a system's vulnerability by minimizing its attack surface. A set of protocols and rules that enable information exchange among software and applications.

³ **Protocol** A combination of standardized rules and signals employed by computers on a network to facilitate communication - examples of these being HTTP, FTP, and SMTP.

⁴ User application: A program installed on a computer that is created for the user's business or purpose.

⁵ **Defence in depth strategy**: A strategy to mitigate security risks by combining multiple security measures rather than relying on a single security measure. Such strategies are defined in Part X as an "information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization".

⁶ **Best practice**: Guidelines for the secure design, development, testing, and maintenance of products as determined by suppliers are to be generally recommended security and industry practices.

This section describes security hardening guidelines for product hardening. "Hardening" is the act of reducing system vulnerability by reducing the system's exposure to attacks; for example, systems are less vulnerable to attacks by removing unnecessary software, accounts and services.

The controls described here require the <u>adoption of processes that includes product hardening</u> guidelines to be applied during product installation and maintenance. These guidelines are to include the following.

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

A "security context" refers to the security environments in which systems or applications are implemented, including whether products require physical security or external firewall protection. By designing environments to include external security features, a defence-in-depth strategy can be developed that is appropriate for a particular environment. The goal here is for products to fit into security contexts and for security contexts to provide adequate protection for products. The processes required here include, for example, limiting system access through physical security and limiting communication through external firewalls. When third-party components are included in systems, such components are to conform to the security contexts of products and are to not reduce the overall security level of products.

- Integration of the product's application programming interfaces /protocols with user applications

Since product API and protocols share product functions and data with user applications, insufficient authentication and encryption can result in access keys being stolen or communications being intercepted by third-party when such API and protocols are not fully integrated with user applications. Therefore, products using API and protocols are to be provided with instructions, rationales and recommendations for securely integrating user applications with API.

- Applying and maintaining the product's defence in depth strategy

Defence-in-depth is to be maintained to respond to new threats and vulnerabilities by reviewing and updating it as appropriate. Therefore, relevant documentation is to includes information on safe operation and maintenance instructions and is to also explain the owner responsibilities regarding defence-in-depth operation and maintenance.

- Configuration and use of security options/capabilities in support of local security policies, and for each security option/capability

"Local security policies" are security requirements and standards in the local environments in which products operate. Such policies should be adapted to local environments and provided with security options and features for support. Descriptions of security configuration options should include the following.

- Contribution to the product defence-in-depth strategy

Security options and feature should be identified according to which layer and which role they play in product defence-in-depth strategies.

- Describe configurable values and their default values
 Consideration should be given to the balance between security and availability when selecting this option and the effects and reasons for default values should be explained.
- Setting, changing, and deleting values
 Appropriate permissions and procedures much be observed when setting, changing or deleting values. Note that security configuration settings are to be implemented in systems as security functions in accordance with the system requirement "29 Network and Security Configuration Settings". See "29 Network and Security Configuration Settings" for more details.

Network and security configuration settings

P. 125

 Instructions and recommendations for the use of all security-related tools and utilities that support administration, monitoring, incident handling, and evaluation of the security of the product

A "security-related tool or utility" is any software or device used to enhance product security or to solve problems. Encryption tools, log analysis tools, backup tools and antivirus software are examples of tools and utilities that are necessary to effectively manage, monitor, respond and evaluate incidents related to product security. Relevant documentation should, therefore, include descriptions on how to use such tools and utilities when they are provided.

- Instructions and recommendations for periodic security maintenance activities

A "routine security maintenance activity" is a task performed to maintain product security such as applying patches and updates; checking and deleting logs and backup files; and updating passwords and certificates. Regular security maintenance activities are necessary to address new threats and vulnerabilities to products and to improve product security. Relevant documentation should, therefore, include descriptions and recommendations for periodic security maintenance activity methods.

- Instructions for reporting security incidents for the product to the supplier

Since security incidents related to products can affect product availability, reporting such incidents to suppliers allows the causes and scopes of incidents to be investigated and appropriate countermeasures and remediation measures to be implemented. Relevant documentation, therefore, should include procedures for reporting security incidents to suppliers.

- Description of the security best practices for maintenance and administration of the product.

"Security best practices for product administration and maintenance" are recommended procedures and policies to help ensure the safe operation and maintenance of products, for example, updates and patching. The purposes of such practices are to maintain product security status and protect it against

vulnerabilities and attacks. Relevant documentation should, therefore, include descriptions of the best practices for secure product management.

In addition, the processes described above are to be established by organisations. Furthermore, surveys of management system documentation and records in presence of Society surveyors are required to verify the establishment of such processes.

Document reviews

■ Secure development lifecycle documents

7. S	ecurity hardening guidelines
-1.	Processes have been adopted that include product hardening guidelines during product
	installation.
	And maintenance and includes instructions, rationales and recommendations for the
	following.
(1)	Integration of the product, including third-party components, with its product security
	context
(2)	Integration of the product's application programming interfaces/protocols with user
	applications
(3)	Applying and maintaining the product's defence in depth strategy
(4)	Configuration and use of security options/capabilities in support of local security policies,
	and for each security option/capability
	(a) its contribution to the product's defence in depth strategy
	(b) descriptions of configurable and default values that include how each affects security
	along with any potential impact each has on work practices
	(c) setting/changing/deleting its value
(5)	Instructions and recommendations for the use of all security-related tools and utilities that
	support administration, monitoring, incident handling, and evaluation of the security of the
	product
(6)	Instructions and recommendations for periodic security maintenance activities
(7)	Instructions for reporting security incidents for the product to the supplier
(8)	Description of the security best practices for maintenance and administration of the
	product.

Surveys

■ Secure development lifecycle

7. Security hardening guidelines

-1. Management system documentation is to include processes for developing products that include product hardening guidelines for installation and maintenance.

Reference

- (1) IACS Unified Requirements, E26 (April 2022) Cyber resilience of ships
- (2) IACS Unified Requirements, E27 (Rev.1) (September 2023) Cyber resilience of on-board systems and equipment
- (3) IEC TS 62443-1-1: 2009 Terminology, concepts and models
- (4) IEC 62443-3-3: 2013 System security requirements and security levels
- (5) IEC 62443-4-1: 2018 Secure product development lifecycle requirements

Appendix 1 Checklist of Document reviews

Ma	anufa	acturer :
Ту	ре	:
Se	rial N	
)οςι	ume	entation
1. C	BS a	sset inventory
-1.	The	following items are to be included.
(1)	List	of hardware components
	(a)	Name
	(b)	Brand/manufacturer
	(c)	Model/type
	(d)	Short description of functionality/purpose
	(e)	Physical interfaces (e.g., network, serial)
	(f)	Name/type of system software (e.g., operating system, firmware)
	(g)	Version and patch level of system software
(2)	Sup	ported communication protocols
	(a)	List of software components
	(b)	The hardware component where it is installed
	(c)	Brand/manufacturer
	(d)	Model/type
	(e)	Short description of functionality/purpose
2. T	opol	ogy diagrams
-1.	The	following items are to be included.
(1)	Phy	sical topology diagram
	(a)	All endpoints and network equipment, including identification of redundant units
	(b)	Communication cables, including communication with I/O units (Networks, serial links, etc.)
	(c)	Communication cables to other networks or systems
(2)	Log	ical topology diagram
	(a)	Communication endpoints (Workstations, controllers, servers, etc.)

(b) Network devices (Switches, routers, firewalls, etc.)		
	(c) Physical computer and virtual computers	
	(d) Physical communication path and virtual communication paths	
	(e) Communication protocols	
3. D	Description of Security capabilities	
-1.	The following items are to be included.	
(1)	Security capabilities and compensating countermeasures	
	(a) See "Chapter 5 Explanation of System requirements" for more information.	
(2)	Network interface	
	(a) Networks within the scope of Part X, Chapter 4 (UR E27)	
	(b) Untrusted Networks	
	For the components responsible for protecting security zone boundaries, the detail	
	whether they are delivered as a part of system should be described.	
(3)	Any supporting documents necessary to verify compliance with the requirements	
4. T	est procedure of security capabilities	
-1.	The following items are to be included.	
(1)	Demonstration tests of security capabilities and confirmation of compensating	
	countermeasures	
	See "Chapter 5 Explanation of System requirements" for more information.	
	(a) Necessary test setup	
	(b) Test equipment	
	(c) Initial condition(s)	
	(d) Test methodology, detailed test steps	
	(e) Expected results and acceptance criteria	
	(f) Entry column to update test results and record findings during the testing	
	ecurity configuration guidelines	
-1.	The following items are to be included.	
(1)	Description of the recommended configuration settings for security capabilities	
(2)	Specified default values	
C 6		
	ecure development lifecycle documents	
-1.	The following items are to be included.	
(1)	Records how the security aspects have been addressed	
	Recorded Documents should be prepared at the following stages:	

Ш	(a) Requirement analysis phase
	(b) Design phase
	(c) Implementation phase
	(d) Verification phase
	(e) Release phase
	(f) Maintenance phase
	(g) End of life phase
	(2) Processes and Controls for Secure development lifecycle
	See "Chapter 6 Explanation of Secure development lifecycle requirements" for more
	information.
	(3) Software updates and patching
	7. Plans for maintenance and verification of the CBS
	-1. The following items are to be included.
	(1) Description of recommended settings for security capabilities
	(2) Instructions for how the user can verify correct operation of the system's security functions
	The capabilities implemented by the system requirements "19 Security functionality
	verification" should be included.
	8. Information supporting the owner's incident response and recovery plan
	8. Information supporting the owner's incident response and recovery plan-1. The following procedures or instructions are included.
	-1. The following procedures or instructions are included.
	-1. The following procedures or instructions are included.(1) Local independent control
	-1. The following procedures or instructions are included.(1) Local independent control(2) Network isolation
	 -1. The following procedures or instructions are included. (1) Local independent control (2) Network isolation (3) Forensics by use of audit records
	 -1. The following procedures or instructions are included. (1) Local independent control (2) Network isolation (3) Forensics by use of audit records (4) Deterministic output
	 -1. The following procedures or instructions are included. (1) Local independent control (2) Network isolation (3) Forensics by use of audit records (4) Deterministic output (5) Backup
	 -1. The following procedures or instructions are included. (1) Local independent control (2) Network isolation (3) Forensics by use of audit records (4) Deterministic output (5) Backup (6) Restore
	 -1. The following procedures or instructions are included. (1) Local independent control (2) Network isolation (3) Forensics by use of audit records (4) Deterministic output (5) Backup (6) Restore
	 -1. The following procedures or instructions are included. (1) Local independent control (2) Network isolation (3) Forensics by use of audit records (4) Deterministic output (5) Backup (6) Restore (7) Controlled shutdown, reset, roll-back and restart
	-1. The following procedures or instructions are included. (1) Local independent control (2) Network isolation (3) Forensics by use of audit records (4) Deterministic output (5) Backup (6) Restore (7) Controlled shutdown, reset, roll-back and restart
	-1. The following procedures or instructions are included. (1) Local independent control (2) Network isolation (3) Forensics by use of audit records (4) Deterministic output (5) Backup (6) Restore (7) Controlled shutdown, reset, roll-back and restart 9. Management of change plan -1. Cybersecurity change management procedures are included. This does not apply if the
	 -1. The following procedures or instructions are included. (1) Local independent control (2) Network isolation (3) Forensics by use of audit records (4) Deterministic output (5) Backup (6) Restore (7) Controlled shutdown, reset, roll-back and restart 9. Management of change plan -1. Cybersecurity change management procedures are included. This does not apply if the change management procedures required by Part X, Chapter 3 (UR E22) have been submitted.
	 -1. The following procedures or instructions are included. (1) Local independent control (2) Network isolation (3) Forensics by use of audit records (4) Deterministic output (5) Backup (6) Restore (7) Controlled shutdown, reset, roll-back and restart 9. Management of change plan -1. Cybersecurity change management procedures are included. This does not apply if the change management procedures required by Part X, Chapter 3 (UR E22) have been
	 -1. The following procedures or instructions are included. (1) Local independent control (2) Network isolation (3) Forensics by use of audit records (4) Deterministic output (5) Backup (6) Restore (7) Controlled shutdown, reset, roll-back and restart 9. Management of change plan -1. Cybersecurity change management procedures are included. This does not apply if the change management procedures required by Part X, Chapter 3 (UR E22) have been submitted.
	 -1. The following procedures or instructions are included. (1) Local independent control (2) Network isolation (3) Forensics by use of audit records (4) Deterministic output (5) Backup (6) Restore (7) Controlled shutdown, reset, roll-back and restart 9. Management of change plan -1. Cybersecurity change management procedures are included. This does not apply if the change management procedures required by Part X, Chapter 3 (UR E22) have been submitted. 10. Test reports

(3) Correct configuration of security capabilities
(4) Secure development lifecycle
(5) Hardening at installation
-2. A signature from the supplier is to be included.

System requirements

■ Description of security capabilities

1. H	luma	n user identification and authentication
-1.	If th	is requirement applies, either of the following (1) or (2) is to be implemented.
(1)	Capa	ability to identify and authenticate users(person)
	(a)	identifying by an identifier.
	(b)	authenticating by an identifier and an authenticator.
(2)	Con	pensating countermeasure
	(a)	Protect against the same threats as the original requirement
	(b)	Provide an equal level of protection as the original requirement
	(c)	Not be a security control that is required by other requirements
	(d)	Not introduce higher security risk
2. A	lccou	int management
-1.	If th	is requirement applies, either of the following (1) or (2) is to be implemented.
(1)	The	capability to support the management of all accounts by authorized users
	(a)	The following capabilities should be implemented.
		i) Adding, modifying and removing account
		ii) Activating and disabling account (In case compensating countermeasures are
		taken, the reasons shall be provided)
	(b)	Only authorized users can manage account.
(2)	Con	pensating countermeasure
	(a)	Protect against the same threats as the original requirement
	(b)	Provide an equal level of protection as the original requirement
	(c)	Not be a security control that is required by other requirements
	(d)	Not introduce higher security risk
3. le	denti	fier management
-1.	If th	is requirement applies, either of the following (1) or (2) is to be implemented.
(1)	The	capability to support the management of identifiers by user, group and role

Add, modifying and remove identifiers			
(2)	(2) Compensating countermeasure		
	a) Protect against the same threats as the original requirement		
	b) Provide an equal level of protection as the original requirement		
(c) Not be a security control that is required by other requirements			
	d) Not introduce higher security risk		
4. A	thenticator management		
-1.	f this requirement applies, either of the following (1) or (2) is to be implemented.		
(1)	The capability to manage authenticators		
	The following capabilities should be implemented.		
	a) Initialize authenticator content (e.g., initializing a password)		
	b) Change all default authenticators upon control system installation (e.g., changing from the initial password)		
	c) Change/refresh all authenticators (e.g., changing of the password)		
	d) Protect all authenticators from unauthorized disclosure and modification when stored	d	
	and transmitted. (e.g., password encryption)		
(2)	Compensating countermeasure		
	a) Protect against the same threats as the original requirement		
	b) Provide an equal level of protection as the original requirement		
	c) Not be a security control that is required by other requirements		
	d) Not introduce higher security risk		
5. V	reless access management		
-1.	f this requirement applies, either of the following (1) or (2) is to be implemented.		
(1)	The capability to identify and authenticate all users (humans, software processes or		
	levices) engaged in wireless communication		
	a) Human user identification and authentication		
	i) identifying by an identifier.		
	ii) authenticating by an identifier and an authenticator.		
	b) Software process identification and authentication		
	i) identifying by an identifier.		
	ii) authenticating by an identifier and an authenticator.		
	c) Device identification and authentication		
	i) identifying by an identifier. ii) authorizating by an identifier and an authorizator.		
(2)	ii) authenticating by an identifier and an authenticator.		
(2)	Compensating countermeasure		

	(a)	Protect against the same threats as the original requirement	
	(b)	Provide an equal level of protection as the original requirement	
	(c)	Not be a security control that is required by other requirements	
	(d)	Not introduce higher security risk	
6. S	tren	gth of password-based authentication	
-1.	If th	is requirement applies, either of the following (1) or (2) is to be implemented.	
(1)	The	capability to enforce configurable password strength	
	(a)	Minimum length	
		The decision was made based on the guidelines set forth in the countermeasures.	
	(b)	Variety of character types	
		The decision was made based on the guidelines set forth in the countermeasures.	
(2)	Con	npensating countermeasure	
	(a)	Protect against the same threats as the original requirement	
	(b)	Provide an equal level of protection as the original requirement	
	(c)	Not be a security control that is required by other requirements	
	(d)	Not introduce higher security risk	
7. <i>A</i>	Authe	enticator feedback	
7. <i>A</i> -1.		is requirement applies, either of the following (1) or (2) is to be implemented.	
	If th		
-1.	If th	is requirement applies, either of the following (1) or (2) is to be implemented.	
-1.	If the	is requirement applies, either of the following (1) or (2) is to be implemented. capability to obscure feedback during the authentication process	
-1. (1)	If the	is requirement applies, either of the following (1) or (2) is to be implemented. capability to obscure feedback during the authentication process password being entered is hidden.	
-1. (1)	If the The Con	is requirement applies, either of the following (1) or (2) is to be implemented. capability to obscure feedback during the authentication process password being entered is hidden. appensating countermeasure	
-1. (1)	If the The Con (a)	is requirement applies, either of the following (1) or (2) is to be implemented. capability to obscure feedback during the authentication process password being entered is hidden. pensating countermeasure Protect against the same threats as the original requirement	
-1. (1)	If the The Con (a) (b)	is requirement applies, either of the following (1) or (2) is to be implemented. capability to obscure feedback during the authentication process password being entered is hidden. mpensating countermeasure Protect against the same threats as the original requirement Provide an equal level of protection as the original requirement	
-1. (1)	If the The Con (a) (b) (c)	is requirement applies, either of the following (1) or (2) is to be implemented. capability to obscure feedback during the authentication process password being entered is hidden. pensating countermeasure Protect against the same threats as the original requirement Provide an equal level of protection as the original requirement Not be a security control that is required by other requirements	
-1. (1)	If the The Com (a) (b) (c) (d)	is requirement applies, either of the following (1) or (2) is to be implemented. capability to obscure feedback during the authentication process password being entered is hidden. pensating countermeasure Protect against the same threats as the original requirement Provide an equal level of protection as the original requirement Not be a security control that is required by other requirements	
-1. (1)	If the The Con (a) (b) (c) (d)	is requirement applies, either of the following (1) or (2) is to be implemented. capability to obscure feedback during the authentication process password being entered is hidden. mpensating countermeasure Protect against the same threats as the original requirement Provide an equal level of protection as the original requirement Not be a security control that is required by other requirements Not introduce higher security risk	
-1. (1) (2)	If the The Con (a) (b) (c) (d)	is requirement applies, either of the following (1) or (2) is to be implemented. capability to obscure feedback during the authentication process password being entered is hidden. Inpensating countermeasure Protect against the same threats as the original requirement Provide an equal level of protection as the original requirement Not be a security control that is required by other requirements Not introduce higher security risk Prization enforcement	
-1. (1) (2) 8. A -1.	If the The Con (a) (b) (c) (d) Authorite and	is requirement applies, either of the following (1) or (2) is to be implemented. capability to obscure feedback during the authentication process password being entered is hidden. mensating countermeasure Protect against the same threats as the original requirement Provide an equal level of protection as the original requirement Not be a security control that is required by other requirements Not introduce higher security risk prization enforcement is requirement applies, either of the following (1) or (2) is to be implemented. capability to support the assignment of privileges according to the separation of duties the principle of least privilege	
-1. (1) (2) 8. A -1.	If the The Con (a) (b) (c) (d) Authorite and	is requirement applies, either of the following (1) or (2) is to be implemented. capability to obscure feedback during the authentication process password being entered is hidden. pensating countermeasure Protect against the same threats as the original requirement Provide an equal level of protection as the original requirement Not be a security control that is required by other requirements Not introduce higher security risk prization enforcement is requirement applies, either of the following (1) or (2) is to be implemented. capability to support the assignment of privileges according to the separation of duties the principle of least privilege following elements are to be controlled by access control lists or other means.	
-1. (1) (2) 8. A -1.	If the The Con (a) (b) (c) (d) Author The and The (a)	is requirement applies, either of the following (1) or (2) is to be implemented. capability to obscure feedback during the authentication process password being entered is hidden. pensating countermeasure Protect against the same threats as the original requirement Provide an equal level of protection as the original requirement Not be a security control that is required by other requirements Not introduce higher security risk prization enforcement is requirement applies, either of the following (1) or (2) is to be implemented. capability to support the assignment of privileges according to the separation of duties the principle of least privilege following elements are to be controlled by access control lists or other means. Subject (e.g., all users, including groups)	
-1. (1) (2) 8. A -1.	If the The Con (a) (b) (c) (d) Authorite and The	is requirement applies, either of the following (1) or (2) is to be implemented. capability to obscure feedback during the authentication process password being entered is hidden. pensating countermeasure Protect against the same threats as the original requirement Provide an equal level of protection as the original requirement Not be a security control that is required by other requirements Not introduce higher security risk prization enforcement is requirement applies, either of the following (1) or (2) is to be implemented. capability to support the assignment of privileges according to the separation of duties the principle of least privilege following elements are to be controlled by access control lists or other means.	
-1. (1) (2) 8. A -1.	If the The Con (a) (b) (c) (d) Author The and The (a) (b) (c)	is requirement applies, either of the following (1) or (2) is to be implemented. capability to obscure feedback during the authentication process password being entered is hidden. pensating countermeasure Protect against the same threats as the original requirement Provide an equal level of protection as the original requirement Not be a security control that is required by other requirements Not introduce higher security risk prization enforcement is requirement applies, either of the following (1) or (2) is to be implemented. capability to support the assignment of privileges according to the separation of duties the principle of least privilege following elements are to be controlled by access control lists or other means. Subject (e.g., all users, including groups)	

Ш		(a)	Protect against the same threats as the original requirement
		(b)	Provide an equal level of protection as the original requirement
		(c)	Not be a security control that is required by other requirements
		(d)	Not introduce higher security risk
	9. V	Virel	ess use control
	-1.	If th	nis requirement applies, either of the following (1) or (2) is to be implemented.
	(1)	The	capability to authorize, monitor and enforce usage restrictions for wireless
		con	nectivity to the system
		(a)	The following functions are implemented in accordance with generally accepted
			industry security practices
			i) Authorization
			ii) Monitoring
			iii) Usage restrictions
	(2)	Con	npensating countermeasure
		(a)	Protect against the same threats as the original requirement
		(b)	Provide an equal level of protection as the original requirement
		(c)	Not be a security control that is required by other requirements
		(d)	Not introduce higher security risk
		(d)	Not introduce higher security risk
	10.		Not introduce higher security risk control for portable and mobile devices
	10. -1.	Use	
		Use If th	control for portable and mobile devices
	-1.	Use If the	control for portable and mobile devices as requirement applies, either of the following (1) or (2) is to be implemented.
	-1.	Use If the	control for portable and mobile devices as requirement applies, either of the following (1) or (2) is to be implemented. The abilities for restricting the use of portable and mobile devices and restricting data
	-1.	Use If th Cap tran	control for portable and mobile devices as requirement applies, either of the following (1) or (2) is to be implemented. Abbilities for restricting the use of portable and mobile devices and restricting data smission
	-1.	Use If th Cap tran	control for portable and mobile devices his requirement applies, either of the following (1) or (2) is to be implemented. habilities for restricting the use of portable and mobile devices and restricting data smission Restrictions on the use of portable and handheld devices
	-1.	Use If th Cap tran (a)	control for portable and mobile devices his requirement applies, either of the following (1) or (2) is to be implemented. habilities for restricting the use of portable and mobile devices and restricting data smission Restrictions on the use of portable and handheld devices Only authorized devices are permitted to be used
	-1.	Use If th Cap tran (a) (b)	control for portable and mobile devices his requirement applies, either of the following (1) or (2) is to be implemented. habilities for restricting the use of portable and mobile devices and restricting data smission Restrictions on the use of portable and handheld devices Only authorized devices are permitted to be used Restrictions on data transfer for portable and mobile devices
	-1. (1)	Use If th Cap tran (a) (b)	control for portable and mobile devices his requirement applies, either of the following (1) or (2) is to be implemented. habilities for restricting the use of portable and mobile devices and restricting data smission Restrictions on the use of portable and handheld devices Only authorized devices are permitted to be used Restrictions on data transfer for portable and mobile devices The transfer of device codes and data are to be restricted
	-1. (1)	Use If th Cap tran (a) (b)	control for portable and mobile devices his requirement applies, either of the following (1) or (2) is to be implemented. habilities for restricting the use of portable and mobile devices and restricting data smission Restrictions on the use of portable and handheld devices Only authorized devices are permitted to be used Restrictions on data transfer for portable and mobile devices The transfer of device codes and data are to be restricted Impensating countermeasure
	-1. (1)	Use If th Cap tran (a) (b) Con (a)	control for portable and mobile devices as requirement applies, either of the following (1) or (2) is to be implemented. abilities for restricting the use of portable and mobile devices and restricting data smission Restrictions on the use of portable and handheld devices Only authorized devices are permitted to be used Restrictions on data transfer for portable and mobile devices The transfer of device codes and data are to be restricted Impensating countermeasure Protect against the same threats as the original requirement
	-1. (1)	Use If the Cape tran (a) (b) Con (a) (b)	control for portable and mobile devices as requirement applies, either of the following (1) or (2) is to be implemented. abilities for restricting the use of portable and mobile devices and restricting data smission Restrictions on the use of portable and handheld devices Only authorized devices are permitted to be used Restrictions on data transfer for portable and mobile devices The transfer of device codes and data are to be restricted Impensating countermeasure Protect against the same threats as the original requirement Provide an equal level of protection as the original requirement
	-1. (1)	Use If the Cape tran (a) (b) Con (a) (b) (c)	control for portable and mobile devices his requirement applies, either of the following (1) or (2) is to be implemented. Habilities for restricting the use of portable and mobile devices and restricting data smission Restrictions on the use of portable and handheld devices Only authorized devices are permitted to be used Restrictions on data transfer for portable and mobile devices The transfer of device codes and data are to be restricted Impensating countermeasure Protect against the same threats as the original requirement Provide an equal level of protection as the original requirement Not be a security control that is required by other requirements
	-1. (1)	Use If th Cap tran (a) (b) Con (a) (b) (c) (d)	control for portable and mobile devices his requirement applies, either of the following (1) or (2) is to be implemented. Habilities for restricting the use of portable and mobile devices and restricting data smission Restrictions on the use of portable and handheld devices Only authorized devices are permitted to be used Restrictions on data transfer for portable and mobile devices The transfer of device codes and data are to be restricted Impensating countermeasure Protect against the same threats as the original requirement Provide an equal level of protection as the original requirement Not be a security control that is required by other requirements
	-1. (1)	Use If th Cap tran (a) (b) Con (a) (b) (c) (d)	control for portable and mobile devices as requirement applies, either of the following (1) or (2) is to be implemented. abilities for restricting the use of portable and mobile devices and restricting data smission Restrictions on the use of portable and handheld devices Only authorized devices are permitted to be used Restrictions on data transfer for portable and mobile devices The transfer of device codes and data are to be restricted Impensating countermeasure Protect against the same threats as the original requirement Provide an equal level of protection as the original requirement Not be a security control that is required by other requirements Not introduce higher security risk

	(a) Capability to control the use of mobile codes (e.g., remove browsers, prohibit mobile code behaviour in policy settings).	ile		
(2)	(2) Compensating countermeasure			
	(a) Protect against the same threats as the original requirement			
	(b) Provide an equal level of protection as the original requirement			
	(c) Not be a security control that is required by other requirements			
	(d) Not introduce higher security risk			
12.	ession lock			
-1.	If this requirement applies, either of the following (1) or (2) is to be implemented.			
(1)	Session lock functionality, either automatic or manual			
	(a) For automatic session locks, the following is to be checked:			
	i) The session locks after a period of inactivity			
	ii) The inactivity period is configurable.			
	(b) For manual session locks, the following is to be checked:			
	i) Session lock is manually enabled.			
(2)	Compensating countermeasure			
	(a) Protect against the same threats as the original requirement			
	(b) Provide an equal level of protection as the original requirement			
	(c) Not be a security control that is required by other requirements			
	(d) Not introduce higher security risk			
13.	uditable events			
-1.	If this requirement applies, either of the following (1) or (2) is to be implemented.			
(1)	The function to generate audit records of important events			
	(a) The audit records of the following events are necessary			
	i) Access control			
	ii) Operating system events			
	iii) Backup and restore events			
	iv) Configuration changes			
	v) Loss of communication			
(2)	Compensating countermeasure			
	(a) Protect against the same threats as the original requirement			
	(b) Provide an equal level of protection as the original requirement			
	(c) Not be a security control that is required by other requirements			
	(d) Not introduce higher security risk			

14. Audit storage capacity		
-1.	If this requirement applies, either of the following (1) or (2) is to be implemented.	
(1)	The capabilities allocating sufficient audit record storage capacity according to commonly	
	recognized recommendations for log management	
	(a) Based on commonly recognized recommendations for log management (e.g. NIST	
	SP800-92)。	
	(b) Ensuring the capacity to supplement audit records over the required period.	
(2)	Compensating countermeasure	
	(a) Protect against the same threats as the original requirement	
	(b) Provide an equal level of protection as the original requirement	
	(c) Not be a security control that is required by other requirements	
	(d) Not introduce higher security risk	
15.	Response to audit processing failures	
-1.	If this requirement applies, either of the following (1) or (2) is to be implemented.	
(1)	Capabilities to prevent the loss of essential services and functions when the audit process	
	fails	
	(a) Prevent the loss of essential services and functions in the event of a failure of the	
	audit process. (e.g., Separating audit functions from essential functions)	
(2)	Compensating countermeasure	
	(a) Protect against the same threats as the original requirement	
	(b) Provide an equal level of protection as the original requirement	
	(c) Not be a security control that is required by other requirements	
	(d) Not introduce higher security risk	
16.	Timestamps	
-1.	If this requirement applies, either of the following (1) or (2) is to be implemented.	
(1)	The capability to include the date and time in the audit record	
	(a) To include the timestamp in the audit record (e.g., Real-time clock IC, System clock)	
(2)	Compensating countermeasure	
	(a) Protect against the same threats as the original requirement	
	(b) Provide an equal level of protection as the original requirement	
	(c) Not be a security control that is required by other requirements	
	(d) Not introduce higher security risk	
17.	Communication integrity	
-1.	If this requirement applies, either of the following (1) or (2) is to be implemented.	
(1)	The capability to protect the integrity of transmitted information	

Ш) The following functions are to be provi	ded
			een the received and transmitted data, a
		function to request the sender to re	
		ii) A function to issue an alarm when transmitted data continue to be det	discrepancies between the received and ected.
) Where wireless communications are use	ed, the information transmitted is to be
		encrypted.	
	(2)	ompensating countermeasure	
) Protect against the same threats as the c	riginal requirement
) Provide an equal level of protection as	he original requirement
) Not be a security control that is required	d by other requirements
) Not introduce higher security risk	
	18.	alicious code protection	
	-1.	this requirement applies, either of the follo	wing (1) or (2) is to be implemented.
	(1)	ne capability to implement suitable protecti	on measures to prevent, detect and mitigate
	` '	e effects due to malware	1 /
) The following capabilities are to be imp	elemented:
		i) Capability to prevent the effects of	f malware (e.g., Application whitelist
		restrictions, removable media exec	cution restrictions, Sandbox capabilities)
		ii) Capability to detect the effects of a (IDS), anti-malware scan)	malware (e.g., intrusion detection system
		iii) Capability to mitigate the effects of infected terminals)	f malware (e.g., delete files, quarantine
	(2)	ompensating countermeasure	
) Protect against the same threats as the o	riginal requirement
) Provide an equal level of protection as	he original requirement
) Not be a security control that is required	d by other requirements
) Not introduce higher security risk	
	19.	curity functionality verification	
	-1.	this requirement applies, either of the follow	wing (1) or (2) is to be implemented.
	(1)	ne capability to support verification of the i	ntended operation of security functions and
		port when anomalies occur during mainten	ance
) Capability to support verification of the	intended operation of security functions
		Verify the intended operation of security	y functions
) Capability to report when anomalies oc	cur during maintenance
		Report when anomalies occur during m	aintenance (e.g. if antivirus software is

		installed, a message is output when virus or malware identification codes or patterns		
	(0)	fail to update, etc.)		
	(2)			
		(a) Protect against the same threats as the original requirement		
		(b) Provide an equal level of protection as the original requirement		
		(c) Not be a security control that is required by other requirements		
		(d) Not introduce higher security risk		
	20.	Deterministic output		
	-1.	If this requirement applies, either of the following (1) or (2) is to be implemented.		
	(1)	The capability to set outputs to a predetermined state		
		The output can be changed to at least one of the following states		
		(a) Unpowered state		
		(b) Last-known value, or Fixed value		
		Compensating countermeasure		
	21.	Information confidentiality		
	-1.	If this requirement applies, either of the following (1) or (2) is to be implemented.		
	(1)	Confidentiality protection capabilities of information for which explicit authorization is		
	required with respect to reading, whether in storage or in transmission			
		(a) The following capabilities are to be confirmed.		
		i) Capabilities to protect the confidentiality of information in storage.		
		ii) Capabilities to protect the confidentiality of information during transmission.		
		(b) When wireless communication is used, encryption mechanisms are to be employed.		
	(2)	Compensating countermeasure		
		(a) Protect against the same threats as the original requirement		
		(b) Provide an equal level of protection as the original requirement		
		(c) Not be a security control that is required by other requirements		
		(d) Not introduce higher security risk		
		(a) and a substituting control		
	22.	Use of cryptography		
	-1.	If this requirement applies, any of the following mechanisms or countermeasures (1) or (2)		
		is to be implemented:		
	(1)	Encryption algorithm, key length, and mechanism according to generally accepted		
_	(-)	security industry practices and recommendations		
		Generally accepted security industry practices and recommendations are employed for the		
		following items		
		(a) Cryptographic algorithm		

	(b)	Key size		
	(c)) Key mechanism		
(2)	Con	ompensating countermeasure		
	(a)	a) Protect against the same threats as the original requirement		
	(b)	Provide an equal level of protection as the original requirement		
	(c)	Not be a security control that is required by other requirements		
	(d)	Not introduce higher security risk		
23.	Audi	it log accessibility		
-1.	If th	is requirement applies, either of the following (1) or (2) is to be implemented.		
(1)	The	function of read-only access to the audit log by authorized human users and/or tools.		
	(a)	The function of access to the audit log by authorized human users and/or tools.		
	(b)	The access to the audit log is read-only.		
(2)	Con	npensating countermeasure		
	(a)	Protect against the same threats as the original requirement		
	(b)	Provide an equal level of protection as the original requirement		
	(c)	Not be a security control that is required by other requirements		
	(d)	Not introduce higher security risk		
24.	Deni	ial of service protection		
24. -1.		ial of service protection is requirement applies, either of the following (1) or (2) is to be implemented.		
	If th			
-1.	If th Min	is requirement applies, either of the following (1) or (2) is to be implemented.		
-1.	If th Min Mai	is requirement applies, either of the following (1) or (2) is to be implemented. imum capability to maintain essential functions during DoS events		
-1.	If th Min Main proc	is requirement applies, either of the following (1) or (2) is to be implemented. imum capability to maintain essential functions during DoS events ntenance of essential functions during DoS events (e.g., deprioritising communication		
-1. (1)	If th Min Main proc	is requirement applies, either of the following (1) or (2) is to be implemented. imum capability to maintain essential functions during DoS events intenance of essential functions during DoS events (e.g., deprioritising communication esses)		
-1. (1)	If the Min Main processor Com	is requirement applies, either of the following (1) or (2) is to be implemented. imum capability to maintain essential functions during DoS events intenance of essential functions during DoS events (e.g., deprioritising communication esses) impensating countermeasures		
-1. (1)	If the Min Main process Communication (a)	is requirement applies, either of the following (1) or (2) is to be implemented. imum capability to maintain essential functions during DoS events intenance of essential functions during DoS events (e.g., deprioritising communication esses) impensating countermeasures Protect against the same threats as the original requirement		
-1. (1)	If the Min Main process Command (a)	is requirement applies, either of the following (1) or (2) is to be implemented. imum capability to maintain essential functions during DoS events intenance of essential functions during DoS events (e.g., deprioritising communication esses) impensating countermeasures Protect against the same threats as the original requirement Provide an equal level of protection as the original requirement		
-1. (1)	If the Min Main process Community (a) (b) (c)	is requirement applies, either of the following (1) or (2) is to be implemented. imum capability to maintain essential functions during DoS events intenance of essential functions during DoS events (e.g., deprioritising communication esses) inpensating countermeasures Protect against the same threats as the original requirement Provide an equal level of protection as the original requirement Not be a security control that is required by other requirements		
-1. (1)	If the Min Main process Community (a) (b) (c) (d)	is requirement applies, either of the following (1) or (2) is to be implemented. imum capability to maintain essential functions during DoS events intenance of essential functions during DoS events (e.g., deprioritising communication esses) inpensating countermeasures Protect against the same threats as the original requirement Provide an equal level of protection as the original requirement Not be a security control that is required by other requirements		
-1. (1)	If th Min Main process (a) (b) (c) (d)	is requirement applies, either of the following (1) or (2) is to be implemented. imum capability to maintain essential functions during DoS events intenance of essential functions during DoS events (e.g., deprioritising communication esses) inpensating countermeasures Protect against the same threats as the original requirement Provide an equal level of protection as the original requirement Not be a security control that is required by other requirements Not introduce higher security risk		
-1. (1) (2)	If th Min Main proce Com (a) (b) (c) (d) Reso If th	is requirement applies, either of the following (1) or (2) is to be implemented. imum capability to maintain essential functions during DoS events Intenance of essential functions during DoS events (e.g., deprioritising communication essess) Impensating countermeasures Protect against the same threats as the original requirement Provide an equal level of protection as the original requirement Not be a security control that is required by other requirements Not introduce higher security risk		
-1. (1) (2) 25. -1.	If th Min Main proce Com (a) (b) (c) (d) Reso If th Capa	is requirement applies, either of the following (1) or (2) is to be implemented. imum capability to maintain essential functions during DoS events Intenance of essential functions during DoS events (e.g., deprioritising communication desses) Impensating countermeasures Protect against the same threats as the original requirement Provide an equal level of protection as the original requirement Not be a security control that is required by other requirements Not introduce higher security risk Internal control of the following (1) or (2) is to be implemented.		
-1. (1) (2) 25. -1.	If the Min Main process (a) (b) (c) (d) Resources of the Caparage of the Capar	is requirement applies, either of the following (1) or (2) is to be implemented. imum capability to maintain essential functions during DoS events intenance of essential functions during DoS events (e.g., deprioritising communication resses) repensating countermeasures Protect against the same threats as the original requirement Provide an equal level of protection as the original requirement Not be a security control that is required by other requirements Not introduce higher security risk requirement applies, either of the following (1) or (2) is to be implemented. ability to restrict the use of resources by security functions to avoid exhausting		
-1. (1) (2) 25. -1. (1)	If the Min Main process (a) (b) (c) (d) Resources of the Caparage of the Capar	is requirement applies, either of the following (1) or (2) is to be implemented. imum capability to maintain essential functions during DoS events Intenance of essential functions during DoS events (e.g., deprioritising communication resses) Impensating countermeasures Protect against the same threats as the original requirement Provide an equal level of protection as the original requirement Not be a security control that is required by other requirements Not introduce higher security risk Purce management is requirement applies, either of the following (1) or (2) is to be implemented. ability to restrict the use of resources by security functions to avoid exhausting threes.		

		(c)	Not be a security control that is required by other requirements		
		(d)	Not introduce higher security risk		
	26.	Syst	em backup		
	-1.	-1. If this requirement applies, either of the following (1) or (2) is to be implemented.			
	(1)	Cap	pability to back up critical files to be recovered		
		(a)	Backup of data needed to recover the system		
		(b)	Does not affect normal operation		
	(2)	Cor	mpensating countermeasure		
		(a)	Protect against the same threats as the original requirement		
		(b)	Provide an equal level of protection as the original requirement		
		(c)	Not be a security control that is required by other requirements		
		(d)	Not introduce higher security risk		
	27.	Syst	em recovery and reconstitution		
	-1.	If th	nis requirement applies, either of the following (1) or (2) is to be implemented.		
	(3)	Cap	pability to be recovery and reconstitution to a known secure state after a disruption or		
		failure			
		Capability to achieve the following events: It is not necessary to achieve all events by this			
		capability.			
		(a)	System parameters are set to default or secure value		
		(b)	Security-critical patches are reinstalled		
		(c)	Security-related configuration are rechecked and re-established		
		(d)	System documentation and operating procedures are available		
		(e)	Application and system software is reinstalled with secure setting		
		(f)	Reconstitution from the backup data		
Ш	(2)	Con	mpensating countermeasure		
		(a)	Protect against the same threats as the original requirement		
		(b)	Provide an equal level of protection as the original requirement		
		(b) (c)	Provide an equal level of protection as the original requirement Not be a security control that is required by other requirements		
		(b)	Provide an equal level of protection as the original requirement		
		(b) (c) (d)	Provide an equal level of protection as the original requirement Not be a security control that is required by other requirements Not introduce higher security risk		
		(b) (c) (d)	Provide an equal level of protection as the original requirement Not be a security control that is required by other requirements Not introduce higher security risk ernative power source		
	-1.	(b) (c) (d) Alte	Provide an equal level of protection as the original requirement Not be a security control that is required by other requirements Not introduce higher security risk Provide an equal level of protection as the original requirement Not be a security control that is required by other requirements Not introduce higher security risk Provide an equal level of protection as the original requirement Not be a security control that is required by other requirements Not introduce higher security risk Provide an equal level of protection as the original requirement Not be a security control that is required by other requirements Not introduce higher security risk Provide an equal level of protection as the original requirement.		
		(b) (c) (d) Alter If the	Provide an equal level of protection as the original requirement Not be a security control that is required by other requirements Not introduce higher security risk Provide an equal level of protection as the original requirement Not be a security control that is required by other requirements Not introduce higher security risk Provide an equal level of protection as the original requirement Not be a security control that is requirements Not introduce higher security risk Provide an equal level of protection as the original requirement Not be a security control that is required by other requirements Not introduce higher security risk Provide an equal level of protection as the original requirement Not be a security control that is required by other requirements Not introduce higher security risk Provide an equal level of protection as the original requirement Not be a security control that is required by other requirements Not introduce higher security risk Provide an equal level of protection as the original requirement and t		
	-1.	(b) (c) (d) Alte If the Cap secu	Provide an equal level of protection as the original requirement Not be a security control that is required by other requirements Not introduce higher security risk Provide an equal level of protection as the original requirement Not be a security control that is required by other requirements Not introduce higher security risk Provide an equal level of protection as the original requirement Not be a security control that is required by other requirements Not introduce higher security risk Provide an equal level of protection as the original requirement Not be a security control that is required by other requirements Not introduce higher security risk Provide an equal level of protection as the original requirement.		

Ш		(a) Existing security state			
		(b) Documented degraded mode			
	(2)	Compensating countermeasure			
		(a) Protect against the same threats as the original requirement			
		(b) Provide an equal level of protection as the original requirement			
		(c) Not be a security control that is required by other requirements			
		(d) Not introduce higher security risk			
	29.	Network and security configuration settings			
	-1.	If this requirement applies, either of the following	(1) or (2) is to be implemented.		
	(1)	Capability set according to the network and securit	y configuration recommended in the		
		guidelines provided by the supplier			
		The following items can be established:			
		(a) Network configuration			
		(b) Security configuration			
	(2)	Compensating countermeasure			
		(a) Protect against the same threats as the origina	l requirement		
		(b) Provide an equal level of protection as the ori	ginal requirement		
		(c) Not be a security control that is required by or	ther requirements		
		(d) Not introduce higher security risk			
	30.	Least Functionality			
	-1.	If this requirement applies, either of the following	(1) or (2) is to be implemented.		
	(1)	Least Functionality			
		To minimise the "Installation, availability, and access rights" of the following items to the			
		minimum levels necessary.			
		(a) Operating systems software components, produced to the components of the compone	eesses and services.		
		(b) Network services, ports, protocols, route and	host accesses, and all software.		
	(2)	Compensating countermeasure			
		(a) Protect against the same threats as the origina	l requirement		
		(b) Provide an equal level of protection as the ori	ginal requirement		
		(c) Not be a security control that is required by or	her requirements		
		(d) Not introduce higher security risk			
	31.	Multifactor authentication for human users			
		. Multifactor authentication for human users			
	-1.	If this requirement applies, either of the following	(1) or (2) is to be implemented.		

	(a)	Being authenticated by two or more different authentication factors			
	(b)	Being able to log in when a valid authenticator is used			
(2)	Cor	mpensating countermeasure			
	(a)	Protect against the same threats as the original requirement			
	(b)	Provide an equal level of protection as the original requirement			
	(c)	Not be a security control that is required by other requirements			
	(d)	Not introduce higher security risk			
32.	Soft	ware process and device identification and authentication			
-1.	If th	nis requirement applies, either of the following (1) or (2) is to be implemented.			
(1)	The	capability to identify and authenticate software processes and devices			
	(a)	Software process identification and authentication			
		i) identifying by an identifier.			
		ii) authenticating by an identifier and an authenticator.			
	(b)	Device identification and authentication			
		i) identifying by an identifier.			
		ii) authenticating by an identifier and an authenticator.			
(2)	Cor	mpensating countermeasure			
	(a)	Protect against the same threats as the original requirement			
	(b)	Provide an equal level of protection as the original requirement			
	(c)	Not be a security control that is required by other requirements			
	(d)	Not introduce higher security risk			
33.	Uns	uccessful login attempts			
-1.		nis requirement applies, any of the following capability or countermeasures (1) or (2) is			
		e implemented:			
(1)	-	pability to limit consecutive invalid login attempts			
		following items are met:			
	(a)	Access is denied when the number of consecutive invalid login attempts exceeds the			
	<i>a</i> >	configured number of attempts.			
	(b)	Denied access lasts either for a specified period of time or until unlocked by an administrator.			
(2)	Cor	npensating countermeasure			
(2)	(a)	Protect against the same threats as the original requirement			
	(a) (b)	Provide an equal level of protection as the original requirement			
	(c)	Not be a security control that is required by other requirements			
	(d)	Not introduce higher security risk			

34.	System use notification		
-1. If this requirement applies, either of the following (1) or (2) is to be implemented.			
(1)	(1) The capability to display and configurate a system use notification message		
The following capabilities should be implemented.			
	(a) The capability to display a system use notification message		
	Displaying a system use notification message before authenticating.		
	(b) The capability to configurate a system use notification message		
	Can be configurable by authorized personnel.		
(2)	Compensating countermeasure		
	(a) Protect against the same threats as the original requirement		
	(b) Provide an equal level of protection as the original requirement		
	(c) Not be a security control that is required by other requirements		
	(d) Not introduce higher security risk		
35.	Access via Untrusted Networks		
-1.	If this requirement applies, either of the following (1) or (2) is to be implemented.		
(1)	The capability to monitor and control access via untrusted networks		
(2)	Compensating countermeasure		
	(a) Protect against the same threats as the original requirement		
	(b) Provide an equal level of protection as the original requirement		
	(c) Not be a security control that is required by other requirements		
	(d) Not introduce higher security risk		
36.	Explicit access request approval		
-1.	If this requirement applies, either of the following (1) or (2) is to be implemented.		
(1)	The capability to deny access from or via untrusted networks unless explicitly approved		
	by authorized personnel on board		
	(a) The capability to assign access approval permissions to human users		
	(b) The capability to deny unapproved access		
(2)	Compensating countermeasure		
	(a) Protect against the same threats as the original requirement		
	(b) Provide an equal level of protection as the original requirement		
	(c) Not be a security control that is required by other requirements		
	(d) Not introduce higher security risk		
37.	Remote session termination		
-1.	If this requirement applies, either of the following (1) or (2) is to be implemented.		

Ш	(1)	Capability to terminate a remote session			
		Either of the following functions is to be implemented.			
		(a) Capability to terminate a remote session automatically			
		The following items are to be complied with.			
		i) The inactivity time until the end of the session is to be configurable.			
		ii) The session is to be terminated after a configurable period of inactivity.			
		(b) Capability to manually terminate a remote session.			
		The session is to be terminated by operation of the user.			
	(2)	Compensating countermeasure			
		(a) Protect against the same threats as the original requirement			
		(b) Provide an equal level of protection as the original requirement			
		(c) Not be a security control that is required by other requirements			
		(d) Not introduce higher security risk			
	38.	Cryptographic integrity protection			
	-1.	If this requirement applies, any of the following mechanisms or countermeasures (1) or (2)			
		is to be implemented:			
	(1)	The cryptographic mechanisms to recognise changes to information during			
		communication			
	(2)	Compensating countermeasure			
		(a) Protect against the same threats as the original requirement			
		(b) Provide an equal level of protection as the original requirement			
		(c) Not be a security control that is required by other requirements			
		(d) Not introduce higher security risk			
	39.	nput validation			
	-1.	If this requirement applies, either of the following (1) or (2) is to be implemented.			
	(1)	The capability to validate the syntax, length and content of any input data			
		(a) Verify the following input data elements			
		i) Syntax			
		ii) Length			
		iii) Content			
		(b) If the data is determined to be invalid, take appropriate action. (e.g., refuse to accept the input data.)			
	(2)	Compensating countermeasure			
		(a) Protect against the same threats as the original requirement			
П		(b) Provide an equal level of protection as the original requirement			
	(2)	Compensating countermeasure (a) Protect against the same threats as the original requirement			

		(c) Not be a security control that is required by other requirements		
		(d) Not introduce higher security risk		
	40.	Session integrity		
	-1.	If this requirement applies, either of the following (1) or (2) is to be implemented.		
	(1)	The capability to protect the integrity of sessions and reject invalid session IDs		
		The following items are to be satisfied.		
		(a) Protecting the integrity of sessions and reject invalid session IDs		
		(b) Rejecting invalid session IDs		
	(2)	Compensating countermeasure		
		(a) Protect against the same threats as the original requirement		
		(b) Provide an equal level of protection as the original requirement		
		(c) Not be a security control that is required by other requirements		
		(d) Not introduce higher security risk		
	41.	Invalidation of session IDs after session termination		
	-1.	If this requirement applies, either of the following (1) or (2) is to be implemented.		
	(1)	The capability to invalidate session IDs upon user logout or other session termination		
		(including browser sessions)		
	(2)	Compensating countermeasure		
		(a) Protect against the same threats as the original requirement		
		(b) Provide an equal level of protection as the original requirement		
		(c) Not be a security control that is required by other requirements		
		(d) Not introduce higher security risk		
S	ecu	re development lifecycle requirements		
		and the state of t		
	Sec	ure development lifecycle documents		
	1 C	ontrols for private keys		
	-1.	If the system includes software that is digitally signed, either of the following controls are		
	1.	to be maintained.		
	(1)	Procedural controls for private keys (e.g., procedures for generation, storage and use)		
	(2)	Technical controls for private keys (e.g., physical access restrictions and encryption		
		hardware)		

2. Security update documentation

-1.	Verify that a process has been adopted to ensure that security update documentation, including the following items, is available to users.			
(1)	The product version number(s) to which the security patch applies			
(2)	Instructions on how to apply approved patches manually and via an automated process			
(3)	Description of any impacts that applying the patch to the product can have, including reboot			
(4)	Instructions on how to verify that an approved patch has been applied			
(5)	Risks of not applying the patch and mediations that can be used for patches that are not			
(3)	approved or deployed by the asset owner			
	with the property of the most			
3. [Dependent component and Operation system security update documentation			
-1.	System owners have adopted processes to obtain security update documents for dependent			
1.	components or operating systems that include the following.			
	Stating whether the product is compatible with the dependent component or operating			
	system security update			
4. 5	ecurity Update Delivery			
-1.	Processes to acquire security updates for system owners shall be adopted in ways that			
	ensure that security patches are authentic.			
2	· ·			
-2.	QA process shall be adopted for the test of updates before the release of a security update.			
-2.	QA process shall be adopted for the test of updates before the release of a security update.			
	Product defence in depth Processes have been adopted for developing security defence-in-depth strategies,			
5. F	Product defence in depth			
5. F	Product defence in depth Processes have been adopted for developing security defence-in-depth strategies,			
5. F	Product defence in depth Processes have been adopted for developing security defence-in-depth strategies, including the following product documentation.			
5. F	Product defence in depth Processes have been adopted for developing security defence-in-depth strategies, including the following product documentation. Security capabilities implemented by the product and their role in the defence in depth			
5. F -1.	Product defence in depth Processes have been adopted for developing security defence-in-depth strategies, including the following product documentation. Security capabilities implemented by the product and their role in the defence in depth strategy			
5. P -1. (1)	Product defence in depth Processes have been adopted for developing security defence-in-depth strategies, including the following product documentation. Security capabilities implemented by the product and their role in the defence in depth strategy Threats addressed by the defence in depth strategy			
5. P -1. (1)	Product defence in depth Processes have been adopted for developing security defence-in-depth strategies, including the following product documentation. Security capabilities implemented by the product and their role in the defence in depth strategy Threats addressed by the defence in depth strategy Product user mitigation strategies for known security risks associated with the product,			
5. P -1. (1) (2) (3)	Product defence in depth Processes have been adopted for developing security defence-in-depth strategies, including the following product documentation. Security capabilities implemented by the product and their role in the defence in depth strategy Threats addressed by the defence in depth strategy Product user mitigation strategies for known security risks associated with the product,			
5. P -1. (1) (2) (3)	Processes have been adopted for developing security defence-in-depth strategies, including the following product documentation. Security capabilities implemented by the product and their role in the defence in depth strategy Threats addressed by the defence in depth strategy Product user mitigation strategies for known security risks associated with the product, including risks associated with legacy code			
5. P -1. (1) (2) (3)	Processes have been adopted for developing security defence-in-depth strategies, including the following product documentation. Security capabilities implemented by the product and their role in the defence in depth strategy Threats addressed by the defence in depth strategy Product user mitigation strategies for known security risks associated with the product, including risks associated with legacy code			
5. P -1. (1) (2) (3)	Processes have been adopted for developing security defence-in-depth strategies, including the following product documentation. Security capabilities implemented by the product and their role in the defence in depth strategy Threats addressed by the defence in depth strategy Product user mitigation strategies for known security risks associated with the product, including risks associated with legacy code Defence in depth measures expected in the environment Processes have been adopted to develop documentation for product users that describes			
5. P -1. (1) (2) (3)	Processes have been adopted for developing security defence-in-depth strategies, including the following product documentation. Security capabilities implemented by the product and their role in the defence in depth strategy Threats addressed by the defence in depth strategy Product user mitigation strategies for known security risks associated with the product, including risks associated with legacy code Defence in depth measures expected in the environment Processes have been adopted to develop documentation for product users that describes the security defence-in-depth measures expected to be provided by the external			
5. P -1. (1) (2) (3)	Processes have been adopted for developing security defence-in-depth strategies, including the following product documentation. Security capabilities implemented by the product and their role in the defence in depth strategy Threats addressed by the defence in depth strategy Product user mitigation strategies for known security risks associated with the product, including risks associated with legacy code Defence in depth measures expected in the environment Processes have been adopted to develop documentation for product users that describes the security defence-in-depth measures expected to be provided by the external			
5. P -1. (1) (2) (3)	Processes have been adopted for developing security defence-in-depth strategies, including the following product documentation. Security capabilities implemented by the product and their role in the defence in depth strategy Threats addressed by the defence in depth strategy Product user mitigation strategies for known security risks associated with the product, including risks associated with legacy code Defence in depth measures expected in the environment Processes have been adopted to develop documentation for product users that describes the security defence-in-depth measures expected to be provided by the external environments in which the products are used.			

	And maintenance and includes instructions, rationales and recommendations for the
	following.
(1)	Integration of the product, including third-party components, with its product security
	context
(2)	Integration of the product's application programming interfaces/protocols with user
	applications
(3)	Applying and maintaining the product's defence in depth strategy
(4)	Configuration and use of security options/capabilities in support of local security policies,
	and for each security option/capability
	(a) its contribution to the product's defence in depth strategy
	(b) descriptions of configurable and default values that include how each affects security
	along with any potential impact each has on work practices
	(c) setting/changing/deleting its value
(5)	Instructions and recommendations for the use of all security-related tools and utilities that
	support administration, monitoring, incident handling, and evaluation of the security of the
	product
(6)	Instructions and recommendations for periodic security maintenance activities
(7)	Instructions for reporting security incidents for the product to the supplier
(8)	Description of the security best practices for maintenance and administration of the
	product.

Appendix 2 Checklist of Surveys

	Ma	anufacturer	:
	Ту	pe	:
	Se	rial No.	:
S	urv	•	
		ieneral surve	
	-1.		g documents should be prepared in advance.
	(1)	CBS Asset In	•
	(2)	Topology Dia	
	-2.		g inspections should be performed:
	(1)	Document Ve	
			indicating completion of the design
			indicating completion of manufacturing
			indicating completion of internal testing
	(2)	•	
		•	configuration
		Compar	ison with computer system asset inventory and topology diagram
			ty capabilities
	-1.	The following	g document should be prepared in advance.
		Test procedur	re of security capabilities
	-2.	The following	g survey should be carried out:
		Adopted to sy	ystem requirements.
		See "Chapter	5 Explanation of System requirements" for more information.
	3. C	orrect confi	guration of security capabilities
	-1.		g document should be prepared in advance:
		•	figuration Guidelines
	-2.		g survey should be carried out:
		•	ne requirements of network and security configuration settings.
		See "Networl	x and security configuration settings" in the "Chapter 5 Explanation of

4. S	ecure development lifecycle
-1.	The following document should be prepared in advance.
	Secure product development lifecycle documents
-2.	The following survey should be carried out:
	Adopted Secure development lifecycle requirements.
	See "Chapter 6 Secure development lifecycle requirements" for more information.
	em requirements t procedure of security capabilities
1. F	luman user identification and authentication
-1.	If this requirement applies, either of the following (1) or (2) is to be performed.
(1)	Demonstration test for the capability of Human user identification and authentication
	(c) Can log in with a valid identifier and authenticator
	(d) Cannot log in with an invalid identifier and authenticator
(2)	Confirmation of compensating countermeasure
	Confirm that the information is as described in Description of security capabilities.
2. <i>A</i>	Account management
-1.	If this requirement applies, either of the following (1) or (2) is to be performed.
(1)	Demonstration test for the capability to support the management of all accounts by
	authorized users
	(a) The following capabilities should be implemented:
	i) Adding, modifying and removing account
	ii) Activating and disabling account
	(b) Account management permissions should be as follows:
	i) Only authorized users can manage account.
	ii) Unauthorized users cannot manage account.
(2)	Confirmation of compensating countermeasure
	Confirm that the information is as described in Description of security capabilities.
3. le	dentifier management
-1.	If this requirement applies, either of the following (1) or (2) is to be performed.
(1)	Demonstration test for the capability to support the management of identifiers by user,

System requirements" for more information.

	group and role
	Add, modifying and remove identifiers
(2)	Confirmation of compensating countermeasure
	Confirm that the information is as described in Description of security capabilities.
4. <i>A</i>	Authenticator management
-1.	If this requirement applies, either of the following (1) or (2) is to be performed.
(1)	Demonstration test for the capability to manage authenticators
	The following capabilities should be implemented.
	(a) Initialize authenticator content (e.g., initializing a password)
	(b) Change all default authenticators upon control system installation (e.g., changing
	from the initial password)
	(c) Change/refresh all authenticators (e.g., changing of the password)
	(d) Protect all authenticators from unauthorized disclosure and modification when stored
	and transmitted. (e.g., password encryption)
(2)	Confirmation of compensating countermeasure
	Confirm that the information is as described in Description of security capabilities.
5. V	Vireless access management
-1.	If this requirement applies, either of the following (1) or (2) is to be performed.
(1)	Demonstration test for the capability to identify and authenticate all users (humans,
(1)	Demonstration test for the capability to identify and authenticate all users (humans, software processes or devices) engaged in wireless communication
(1)	
(1)	software processes or devices) engaged in wireless communication
(1)	software processes or devices) engaged in wireless communication (a) Human user identification and authentication
(1)	software processes or devices) engaged in wireless communication (a) Human user identification and authentication i) Can log in with a valid identifier and authenticator
(1)	software processes or devices) engaged in wireless communication (a) Human user identification and authentication i) Can log in with a valid identifier and authenticator ii) Cannot log in with an invalid identifier and authenticator
(1)	software processes or devices) engaged in wireless communication (a) Human user identification and authentication i) Can log in with a valid identifier and authenticator ii) Cannot log in with an invalid identifier and authenticator (b) Software process identification and authentication
(1)	software processes or devices) engaged in wireless communication (a) Human user identification and authentication i) Can log in with a valid identifier and authenticator ii) Cannot log in with an invalid identifier and authenticator (b) Software process identification and authentication i) Can log in with a valid identifier and authenticator
(1)	software processes or devices) engaged in wireless communication (a) Human user identification and authentication i) Can log in with a valid identifier and authenticator ii) Cannot log in with an invalid identifier and authenticator (b) Software process identification and authentication i) Can log in with a valid identifier and authenticator ii) Cannot log in with an invalid identifier and authenticator
(1)	software processes or devices) engaged in wireless communication (a) Human user identification and authentication i) Can log in with a valid identifier and authenticator ii) Cannot log in with an invalid identifier and authenticator (b) Software process identification and authentication i) Can log in with a valid identifier and authenticator ii) Cannot log in with an invalid identifier and authenticator (c) Device identification and authentication
(2)	software processes or devices) engaged in wireless communication (a) Human user identification and authentication i) Can log in with a valid identifier and authenticator ii) Cannot log in with an invalid identifier and authenticator (b) Software process identification and authentication i) Can log in with a valid identifier and authenticator ii) Cannot log in with an invalid identifier and authenticator (c) Device identification and authentication i) Can log in with a valid identifier and authenticator
	software processes or devices) engaged in wireless communication (a) Human user identification and authentication i) Can log in with a valid identifier and authenticator ii) Cannot log in with an invalid identifier and authenticator (b) Software process identification and authentication i) Can log in with a valid identifier and authenticator ii) Cannot log in with an invalid identifier and authenticator (c) Device identification and authentication i) Can log in with a valid identifier and authenticator ii) Cannot log in with an invalid identifier and authenticator
(2)	software processes or devices) engaged in wireless communication (a) Human user identification and authentication i) Can log in with a valid identifier and authenticator ii) Cannot log in with an invalid identifier and authenticator (b) Software process identification and authentication i) Can log in with a valid identifier and authenticator ii) Cannot log in with an invalid identifier and authenticator (c) Device identification and authentication i) Can log in with a valid identifier and authenticator ii) Cannot log in with a valid identifier and authenticator Confirmation of compensating countermeasure Confirm that the information is as described in Description of security capabilities.
(2)	software processes or devices) engaged in wireless communication (a) Human user identification and authentication i) Can log in with a valid identifier and authenticator ii) Cannot log in with an invalid identifier and authenticator (b) Software process identification and authentication i) Can log in with a valid identifier and authenticator ii) Cannot log in with an invalid identifier and authenticator (c) Device identification and authentication i) Can log in with a valid identifier and authenticator ii) Cannot log in with an invalid identifier and authenticator Confirmation of compensating countermeasure Confirm that the information is as described in Description of security capabilities.
(2)	software processes or devices) engaged in wireless communication (a) Human user identification and authentication i) Can log in with a valid identifier and authenticator ii) Cannot log in with an invalid identifier and authenticator (b) Software process identification and authentication i) Can log in with a valid identifier and authenticator ii) Cannot log in with an invalid identifier and authenticator (c) Device identification and authentication i) Can log in with a valid identifier and authenticator ii) Cannot log in with a valid identifier and authenticator Confirmation of compensating countermeasure Confirm that the information is as described in Description of security capabilities.
(2)	software processes or devices) engaged in wireless communication (a) Human user identification and authentication i) Can log in with a valid identifier and authenticator ii) Cannot log in with an invalid identifier and authenticator (b) Software process identification and authentication i) Can log in with a valid identifier and authenticator ii) Cannot log in with an invalid identifier and authenticator (c) Device identification and authentication i) Can log in with a valid identifier and authenticator ii) Cannot log in with an invalid identifier and authenticator Confirmation of compensating countermeasure Confirm that the information is as described in Description of security capabilities.

			Adopted to the following items:
			i) A password can be set that is not less than the determined minimum length:
			ii) A password cannot be set that is less than the determined minimum length:
			(b) Variety of character types
			A password can be set for the determined character types.
		(2)	Confirmation of compensating countermeasure
			Confirm that the information is as described in Description of security capabilities.
		7. A	uthenticator feedback
		-1.	If this requirement applies, either of the following (1) or (2) is to be performed.
		(1)	Demonstration test for the capability to obscure feedback during the authentication
			process
			The password being entered is hidden.
		(2)	Confirmation of compensating countermeasure
			Confirm that the information is as described in Description of security capabilities.
1			
		8. A	uthorization enforcement
		-1.	If this requirement applies, either of the following (1) or (2) is to be performed.
		(1)	The Demonstration test for the capability to support the assignment of privileges
			according to the separation of duties and the principle of least privilege
			The following elements are to be managed in accordance with the principles of
			segregation of duties and least privilege by means of access control lists, etc.
			(a) Subject (e.g., all users, including groups)
			(b) Object (e.g., files, databases, network resources)
			(c) Permissions (e.g., read, write, execute)
		(2)	Confirmation of compensating countermeasure
			Confirm that the information is as described in Description of security capabilities.
ı			
ļ		9. V	Vireless use control
		-1.	If this requirement applies, either of the following (1) or (2) is to be performed.
	Ш	(1)	Demonstration test for the capabilities to authorize, monitor, and usage restrict of wireless
			connections to the system
			The following items are to be satisfied.
			(a) The SSID and encryption key setting status can be checked on the configuration
			screen, etc. (b) SSID and aparantian key settings for testing are available.
			(b) SSID and encryption key settings for testing are available. (c) The list of connected devices is available on the connected Windows PC's screen, etc.
			(c) The list of connected devices is available on the connected Windows PC's screen, etc.And the MAC addresses are available.
			ATIU UIC IVIAC AUUICSSES AIC AVAITABLE.

	(d) If there is a usage restriction function (e.g., MAC address), only authorized devices can be connected.
(2)	Confirmation of compensating countermeasure
	Confirm that the information is as described in Description of security capabilities.
10.	Use control for portable and mobile devices
-1.	If this requirement applies, either of the following (1) or (2) is to be performed.
(1)	Demonstration test for the capabilities of use limitation and data transfer limitation for
	portable and handheld devices
	(a) Restriction of use of portable and mobile devices.
	The following shall be complied with
	i) Authorized devices can be used.
	ii) Unauthorized devices cannot be used.
	(b) Unauthorized devices cannot be used.
	The transfer of device codes and data are to be restricted
(2)	Confirmation of compensating countermeasure
	Confirm that the information is as described in Description of security capabilities.
11.	Mobile code
11. -1.	If this requirement applies, either of the following (1) or (2) is to be implemented.
	If this requirement applies, either of the following (1) or (2) is to be implemented. The Demonstration test for the capability to control the use of mobile codes
-1.	If this requirement applies, either of the following (1) or (2) is to be implemented. The Demonstration test for the capability to control the use of mobile codes (a) Control the use of mobile codes (e.g., remove browsers, prohibit mobile code
-1. (1)	If this requirement applies, either of the following (1) or (2) is to be implemented. The Demonstration test for the capability to control the use of mobile codes (a) Control the use of mobile codes (e.g., remove browsers, prohibit mobile code behaviour in policy settings).
-1.	If this requirement applies, either of the following (1) or (2) is to be implemented. The Demonstration test for the capability to control the use of mobile codes (a) Control the use of mobile codes (e.g., remove browsers, prohibit mobile code behaviour in policy settings). Confirmation of compensating countermeasure
-1. (1)	If this requirement applies, either of the following (1) or (2) is to be implemented. The Demonstration test for the capability to control the use of mobile codes (a) Control the use of mobile codes (e.g., remove browsers, prohibit mobile code behaviour in policy settings).
-1. (1)	If this requirement applies, either of the following (1) or (2) is to be implemented. The Demonstration test for the capability to control the use of mobile codes (a) Control the use of mobile codes (e.g., remove browsers, prohibit mobile code behaviour in policy settings). Confirmation of compensating countermeasure Confirm that the information is as described in Description of security capabilities.
-1. (1) (2)	If this requirement applies, either of the following (1) or (2) is to be implemented. The Demonstration test for the capability to control the use of mobile codes (a) Control the use of mobile codes (e.g., remove browsers, prohibit mobile code behaviour in policy settings). Confirmation of compensating countermeasure Confirm that the information is as described in Description of security capabilities.
-1. (1) (2) 12. -1.	If this requirement applies, either of the following (1) or (2) is to be implemented. The Demonstration test for the capability to control the use of mobile codes (a) Control the use of mobile codes (e.g., remove browsers, prohibit mobile code behaviour in policy settings). Confirmation of compensating countermeasure Confirm that the information is as described in Description of security capabilities. Session lock If this requirement applies, either of the following (1) or (2) is to be performed.
-1. (1) (2)	If this requirement applies, either of the following (1) or (2) is to be implemented. The Demonstration test for the capability to control the use of mobile codes (a) Control the use of mobile codes (e.g., remove browsers, prohibit mobile code behaviour in policy settings). Confirmation of compensating countermeasure Confirm that the information is as described in Description of security capabilities. Session lock If this requirement applies, either of the following (1) or (2) is to be performed. For automatic session locks, the following is to be checked:
-1. (1) (2) 12. -1.	If this requirement applies, either of the following (1) or (2) is to be implemented. The Demonstration test for the capability to control the use of mobile codes (a) Control the use of mobile codes (e.g., remove browsers, prohibit mobile code behaviour in policy settings). Confirmation of compensating countermeasure Confirm that the information is as described in Description of security capabilities. Session lock If this requirement applies, either of the following (1) or (2) is to be performed. For automatic session locks, the following is to be checked: (a) The session locks after a period of inactivity
-1. (1) (2) 12. -1.	If this requirement applies, either of the following (1) or (2) is to be implemented. The Demonstration test for the capability to control the use of mobile codes (a) Control the use of mobile codes (e.g., remove browsers, prohibit mobile code behaviour in policy settings). Confirmation of compensating countermeasure Confirm that the information is as described in Description of security capabilities. Session lock If this requirement applies, either of the following (1) or (2) is to be performed. For automatic session locks, the following is to be checked: (a) The session locks after a period of inactivity i) The inactivity period is configurable.
-1. (1) (2) 12. -1.	If this requirement applies, either of the following (1) or (2) is to be implemented. The Demonstration test for the capability to control the use of mobile codes (a) Control the use of mobile codes (e.g., remove browsers, prohibit mobile code behaviour in policy settings). Confirmation of compensating countermeasure Confirm that the information is as described in Description of security capabilities. Session lock If this requirement applies, either of the following (1) or (2) is to be performed. For automatic session locks, the following is to be checked: (a) The session locks after a period of inactivity i) The inactivity period is configurable. ii) For manual session locks, the following is to be checked:
-1. (1) (2) 12. -1.	If this requirement applies, either of the following (1) or (2) is to be implemented. The Demonstration test for the capability to control the use of mobile codes (a) Control the use of mobile codes (e.g., remove browsers, prohibit mobile code behaviour in policy settings). Confirmation of compensating countermeasure Confirm that the information is as described in Description of security capabilities. Session lock If this requirement applies, either of the following (1) or (2) is to be performed. For automatic session locks, the following is to be checked: (a) The session locks after a period of inactivity i) The inactivity period is configurable. ii) For manual session locks, the following is to be checked: (b) Session lock is manually enabled.
-1. (1) (2) 12. -1. (1)	If this requirement applies, either of the following (1) or (2) is to be implemented. The Demonstration test for the capability to control the use of mobile codes (a) Control the use of mobile codes (e.g., remove browsers, prohibit mobile code behaviour in policy settings). Confirmation of compensating countermeasure Confirm that the information is as described in Description of security capabilities. Session lock If this requirement applies, either of the following (1) or (2) is to be performed. For automatic session locks, the following is to be checked: (a) The session locks after a period of inactivity i) The inactivity period is configurable. ii) For manual session locks, the following is to be checked: (b) Session lock is manually enabled. i) For automatic session locks, the following is to be checked:
-1. (1) (2) 12. -1.	If this requirement applies, either of the following (1) or (2) is to be implemented. The Demonstration test for the capability to control the use of mobile codes (a) Control the use of mobile codes (e.g., remove browsers, prohibit mobile code behaviour in policy settings). Confirmation of compensating countermeasure Confirm that the information is as described in Description of security capabilities. Session lock If this requirement applies, either of the following (1) or (2) is to be performed. For automatic session locks, the following is to be checked: (a) The session locks after a period of inactivity i) The inactivity period is configurable. ii) For manual session locks, the following is to be checked: (b) Session lock is manually enabled.

13. Auditable events

Ш	-1.	If this requirement applies, either of the following (1) or (2) is to be performed.
	(1)	The tests of the function to generate audit records of important events
		(a) It is to be confirmed the audit records of the following events can be generated.
		i) Access control
		ii) Operating system events
		iii) Backup and restore events
		iv) Configuration changes
		v) Loss of communication
	(2)	Confirmation of compensating countermeasure
		Confirm that the information is as described in Description of security capabilities.
	14.	Audit storage capacity
	-1.	If this requirement applies, either of the following (1) or (2) is to be performed.
	(1)	The Demonstration test for the capability allocating sufficient audit record storage
		capacity according to commonly recognized recommendations for log management
		(a) Based on commonly recognized recommendations for log management (e.g. NIST SP800-92).
		(b) Ensuring the capacity to supplement audit records over the required period.
	(2)	Confirmation of compensating countermeasure
		Confirm that the information is as described in Description of security capabilities.
	15.	Response to audit processing failures
	-1.	If this requirement applies, either of the following (1) or (2) is to be performed.
	(1)	Demonstration test for Capabilities to prevent the loss of essential services and functions
		when the audit process fails
		(a) Prevent the loss of essential services and functions in the event of a failure of the
		audit process. (e.g., Separating audit functions from essential functions)
	(2)	Confirmation of compensating countermeasure
		Confirm that the information is as described in Description of security capabilities.
	16.	Timestamps
	-1.	If this requirement applies, either of the following (1) or (2) is to be performed.
	(1)	Demonstration test for the capability to include the date and time in the audit record
		(a) To include the timestamp in the audit record (e.g., Real-time clock IC, System clock)
	(2)	Confirmation of compensating countermeasure
		Confirm that the information is as described in Description of security capabilities.

17. Communication integrity

-l.	If this requirement applies, either of the following (1) or (2) is to be performed.
(1)	Demonstration test for capability to protect the integrity of transmitted information
	(a) The following functions are to be provided
	i) When there is a discrepancy between the received and transmitted data, a function to request the sender to retransmit the data.
	ii) A function to issue an alarm when discrepancies between the received and transmitted data continue to be detected.
	(b) Where wireless communications are used, the information transmitted is to be encrypted.
(2)	Confirmation of compensating countermeasure
	Confirm that the information is as described in Description of security capabilities.
18.	Malicious code protection
-1.	If this requirement applies, either of the following (1) or (2) is to be performed.
(1)	Demonstration test for the capability to implement suitable protection measures to
	prevent, detect and mitigate the effects due to malware;
	(a) The following capabilities are implemented:
	i) Capability to prevent the effects of malware (e.g., Application whitelist restrictions, removable media execution restrictions, Sandbox capabilities)
	ii) Capability to detect the effects of malware (e.g., intrusion detection system (IDS), anti-malware scan)
	iii) Capability to mitigate the effects of malware (e.g., delete files, quarantine infected terminals)
(2)	Confirmation of compensating countermeasure
	Confirm that the information is as described in Description of security capabilities.
19.	Security functionality verification
-1.	If this requirement applies, either of the following (1) or (2) is to be performed.
(1)	The demonstration test for the capability to support verification of the intended operation
	of security functions and report when anomalies occur during maintenance
	(a) Capability to support verification of the intended operation of security functions
	i) Verify the intended operation of security functions
	(b) Capability to report when anomalies occur during maintenance
	i) Report when anomalies occur during maintenance (e.g., if antivirus software is
	installed, a message is output when virus or malware identification codes or
(2)	patterns fail to update.)
(2)	Confirmation of compensating countermeasure Confirm that the information is as described in Description of security capabilities.
	Commit that the information is as described in Description of security capabilities.

20.	Deterministic output
-1.	If this requirement applies, either of the following (1) or (2) is to be performed.
(1)	The Demonstration test for the capability to set outputs to a predetermined state
	The output can be changed to at least one of the following states
	(a) Unpowered state
	(b) Last-known value, or Fixed value
(2)	Confirmation of compensating countermeasure
	Confirm that the information is as described in Description of security capabilities.
21.	Information confidentiality
	The surveys are not required.
22.	Use of cryptography
	The surveys are not required.
23.	Audit log accessibility
-1.	If this requirement applies, either of the following (1) or (2) is to be performed.
(1)	Capability to set output to a predefined state
	(a) Conform to the following items.
	i) Access to the audit log by authorized human users and/or tools is available.
	ii) Access to the audit log by unauthorized human users and/or tools is not
	available.
	(b) The access to the audit log is read-only.
(2)	Confirmation of compensating countermeasure
	Confirm that the information is as described in Description of security capabilities.
24.	Denial of service protection
-1.	If this requirement applies, either of the following (1) or (2) is to be performed.
(1)	Demonstration test for Minimum capability to maintain essential functions during DoS
	events
	Maintenance of essential functions during DoS event (e.g., confirming the results of DoS
	event simulation tests)
(2)	Confirmation of compensating countermeasure
	Confirm that the information is as described in Description of security capabilities.
	<u>-</u>
	Resource management
-1.	If this requirement applies, either of the following (1) or (2) is to be performed.

(1)	Demonstration test for the capability to restrict the use of resources by security functions so that resources are not exhausted
(2)	Confirmation of compensating countermeasure
` '	Confirm that the information is as described in the security capability descriptions.
26.	System Backup
-1.	If this requirement applies, either of the following (1) or (2) is to be performed.
(1)	Demonstrated capability to back up critical files to be recovered
	Backup of data needed to recover the system
(2)	Confirmation of compensating countermeasure
	Confirm that the information is as described in the security capability descriptions.
27.	System recovery and reconstitution
-1.	If this requirement applies, either of the following (1) or (2) is to be performed.
(3)	Demonstrated ability to conduct back up critical files to be recovered.
	The system can be recovered and reconstituted to a known secure state in accordance with
	the methods specified in "Information supporting the owner's incident response and
	recovery plan".
(4)	Confirmation of compensating countermeasure
	Confirm that the information is as described in the security capability descriptions.
	Confirm that the information is as described in the security capability descriptions.
28.	Confirm that the information is as described in the security capability descriptions. Alternative power source
28. -1.	
	Alternative power source If this requirement applies, either of the following (1) or (2) is to be performed. Demonstration test for the capability to switch to and from alternative power sources
-1.	Alternative power source If this requirement applies, either of the following (1) or (2) is to be performed. Demonstration test for the capability to switch to and from alternative power sources without affecting existing security conditions or documented degraded modes
-1.	Alternative power source If this requirement applies, either of the following (1) or (2) is to be performed. Demonstration test for the capability to switch to and from alternative power sources without affecting existing security conditions or documented degraded modes Switching to and from an alternative power source without affecting the following
-1.	Alternative power source If this requirement applies, either of the following (1) or (2) is to be performed. Demonstration test for the capability to switch to and from alternative power sources without affecting existing security conditions or documented degraded modes Switching to and from an alternative power source without affecting the following conditions:
-1.	Alternative power source If this requirement applies, either of the following (1) or (2) is to be performed. Demonstration test for the capability to switch to and from alternative power sources without affecting existing security conditions or documented degraded modes Switching to and from an alternative power source without affecting the following conditions: (a) Existing security state
-1.	Alternative power source If this requirement applies, either of the following (1) or (2) is to be performed. Demonstration test for the capability to switch to and from alternative power sources without affecting existing security conditions or documented degraded modes Switching to and from an alternative power source without affecting the following conditions: (a) Existing security state (b) Documented degraded mode
-1.	Alternative power source If this requirement applies, either of the following (1) or (2) is to be performed. Demonstration test for the capability to switch to and from alternative power sources without affecting existing security conditions or documented degraded modes Switching to and from an alternative power source without affecting the following conditions: (a) Existing security state (b) Documented degraded mode Confirmation of compensating countermeasure
-1. (1)	Alternative power source If this requirement applies, either of the following (1) or (2) is to be performed. Demonstration test for the capability to switch to and from alternative power sources without affecting existing security conditions or documented degraded modes Switching to and from an alternative power source without affecting the following conditions: (a) Existing security state (b) Documented degraded mode
-1. (1)	Alternative power source If this requirement applies, either of the following (1) or (2) is to be performed. Demonstration test for the capability to switch to and from alternative power sources without affecting existing security conditions or documented degraded modes Switching to and from an alternative power source without affecting the following conditions: (a) Existing security state (b) Documented degraded mode Confirmation of compensating countermeasure Confirm that the information is as described in the security capability descriptions.
-1. (1) (3)	Alternative power source If this requirement applies, either of the following (1) or (2) is to be performed. Demonstration test for the capability to switch to and from alternative power sources without affecting existing security conditions or documented degraded modes Switching to and from an alternative power source without affecting the following conditions: (a) Existing security state (b) Documented degraded mode Confirmation of compensating countermeasure Confirm that the information is as described in the security capability descriptions.
-1. (1)	Alternative power source If this requirement applies, either of the following (1) or (2) is to be performed. Demonstration test for the capability to switch to and from alternative power sources without affecting existing security conditions or documented degraded modes Switching to and from an alternative power source without affecting the following conditions: (a) Existing security state (b) Documented degraded mode Confirmation of compensating countermeasure Confirm that the information is as described in the security capability descriptions. Network and security configuration settings If this requirement applies, either of the following (1) or (2) is to be performed.
-1. (1) (3)	Alternative power source If this requirement applies, either of the following (1) or (2) is to be performed. Demonstration test for the capability to switch to and from alternative power sources without affecting existing security conditions or documented degraded modes Switching to and from an alternative power source without affecting the following conditions: (a) Existing security state (b) Documented degraded mode Confirmation of compensating countermeasure Confirm that the information is as described in the security capability descriptions. Network and security configuration settings If this requirement applies, either of the following (1) or (2) is to be performed. Demonstration test for the capability set according to the network and security
-1. (1) (3) 29.	Alternative power source If this requirement applies, either of the following (1) or (2) is to be performed. Demonstration test for the capability to switch to and from alternative power sources without affecting existing security conditions or documented degraded modes Switching to and from an alternative power source without affecting the following conditions: (a) Existing security state (b) Documented degraded mode Confirmation of compensating countermeasure Confirm that the information is as described in the security capability descriptions. Network and security configuration settings If this requirement applies, either of the following (1) or (2) is to be performed. Demonstration test for the capability set according to the network and security configuration recommended in the guidelines provided by the supplier
-1. (1) (3) 29.	Alternative power source If this requirement applies, either of the following (1) or (2) is to be performed. Demonstration test for the capability to switch to and from alternative power sources without affecting existing security conditions or documented degraded modes Switching to and from an alternative power source without affecting the following conditions: (a) Existing security state (b) Documented degraded mode Confirmation of compensating countermeasure Confirm that the information is as described in the security capability descriptions. Network and security configuration settings If this requirement applies, either of the following (1) or (2) is to be performed. Demonstration test for the capability set according to the network and security

	(b) Security configuration
(3)	Confirmation of compensating countermeasure
	Confirm that the information is as described in the security capability descriptions.
30.	Least Functionality
-1.	If this requirement applies, either of the following (1) or (2) is to be performed.
(1)	Demonstration test for Least Functionality
	Unnecessary features and services, if implemented, have been disabled.
(2)	Confirmation of compensating countermeasure
	Confirm that the information is as described in the security capability descriptions.
31.	Multifactor authentication for human users
-1.	If this requirement applies, either of the following (1) or (2) is to be performed.
(1)	Demonstration test for the capability of multi-factor authentication when authenticating
	human users
	(a) Can log in with a valid identifier and authenticator
	(b) Cannot log in with an invalid authenticator
(2)	Confirmation of compensating countermeasure
	Confirm that the information is as described in Description of security capabilities.
32.	Software process and device identification and authentication
32. -1.	Software process and device identification and authentication If this requirement applies, either of the following (1) or (2) is to be performed.
-1.	If this requirement applies, either of the following (1) or (2) is to be performed.
-1.	If this requirement applies, either of the following (1) or (2) is to be performed. Demonstration test for the capability to identify and authenticate software processes and
-1.	If this requirement applies, either of the following (1) or (2) is to be performed. Demonstration test for the capability to identify and authenticate software processes and devices
-1.	If this requirement applies, either of the following (1) or (2) is to be performed. Demonstration test for the capability to identify and authenticate software processes and devices (a) Software process identification and authentication
-1.	If this requirement applies, either of the following (1) or (2) is to be performed. Demonstration test for the capability to identify and authenticate software processes and devices (a) Software process identification and authentication i) Can log in with a valid identifier and authenticator
-1.	If this requirement applies, either of the following (1) or (2) is to be performed. Demonstration test for the capability to identify and authenticate software processes and devices (a) Software process identification and authentication i) Can log in with a valid identifier and authenticator ii) Cannot log in with an invalid identifier and authenticator
-1.	If this requirement applies, either of the following (1) or (2) is to be performed. Demonstration test for the capability to identify and authenticate software processes and devices (a) Software process identification and authentication i) Can log in with a valid identifier and authenticator ii) Cannot log in with an invalid identifier and authenticator (b) Device identification and authentication
-1.	If this requirement applies, either of the following (1) or (2) is to be performed. Demonstration test for the capability to identify and authenticate software processes and devices (a) Software process identification and authentication i) Can log in with a valid identifier and authenticator ii) Cannot log in with an invalid identifier and authenticator (b) Device identification and authentication i) Can log in with a valid identifier and authenticator
-1. (1)	If this requirement applies, either of the following (1) or (2) is to be performed. Demonstration test for the capability to identify and authenticate software processes and devices (a) Software process identification and authentication i) Can log in with a valid identifier and authenticator ii) Cannot log in with an invalid identifier and authenticator (b) Device identification and authentication i) Can log in with a valid identifier and authenticator ii) Cannot log in with an invalid identifier and authenticator
-1. (1)	If this requirement applies, either of the following (1) or (2) is to be performed. Demonstration test for the capability to identify and authenticate software processes and devices (a) Software process identification and authentication i) Can log in with a valid identifier and authenticator ii) Cannot log in with an invalid identifier and authenticator (b) Device identification and authentication i) Can log in with a valid identifier and authenticator ii) Cannot log in with an invalid identifier and authenticator Confirmation of compensating countermeasure Confirm that the information is as described in Description of security capabilities.
-1. (1)	If this requirement applies, either of the following (1) or (2) is to be performed. Demonstration test for the capability to identify and authenticate software processes and devices (a) Software process identification and authentication i) Can log in with a valid identifier and authenticator ii) Cannot log in with an invalid identifier and authenticator (b) Device identification and authentication i) Can log in with a valid identifier and authenticator ii) Cannot log in with an invalid identifier and authenticator Confirmation of compensating countermeasure
-1. (1)	If this requirement applies, either of the following (1) or (2) is to be performed. Demonstration test for the capability to identify and authenticate software processes and devices (a) Software process identification and authentication i) Can log in with a valid identifier and authenticator ii) Cannot log in with an invalid identifier and authenticator (b) Device identification and authentication i) Can log in with a valid identifier and authenticator ii) Cannot log in with an invalid identifier and authenticator Confirmation of compensating countermeasure Confirm that the information is as described in Description of security capabilities.
-1. (1)	If this requirement applies, either of the following (1) or (2) is to be performed. Demonstration test for the capability to identify and authenticate software processes and devices (a) Software process identification and authentication i) Can log in with a valid identifier and authenticator ii) Cannot log in with an invalid identifier and authenticator (b) Device identification and authentication i) Can log in with a valid identifier and authenticator ii) Cannot log in with an invalid identifier and authenticator Confirmation of compensating countermeasure Confirm that the information is as described in Description of security capabilities. Unsuccessful login attempts If this requirement applies, either of the following (1) or (2) is to be performed. Demonstration test for the ability to identify and authenticate software processes and
-1. (1) (2) 33.	If this requirement applies, either of the following (1) or (2) is to be performed. Demonstration test for the capability to identify and authenticate software processes and devices (a) Software process identification and authentication i) Can log in with a valid identifier and authenticator ii) Cannot log in with an invalid identifier and authenticator (b) Device identification and authentication i) Can log in with a valid identifier and authenticator ii) Cannot log in with an invalid identifier and authenticator Confirmation of compensating countermeasure Confirm that the information is as described in Description of security capabilities. Unsuccessful login attempts If this requirement applies, either of the following (1) or (2) is to be performed.

	_	(a) Deny access if the number of consecutive invalid login attempts exceeds the configured number of attempts
		(b) Denied access is to be last for a specified period of time or until unlocked by an administrator
	(2)	Confirmation of compensating countermeasure
		Confirm that the information is as described in the security capability descriptions.
	34.	System use notification
	-1.	If this requirement applies, either of the following (1) or (2) is to be performed.
	(1)	Demonstration test for the capability to display and configurate a system use notification message
Г	7	The following capabilities should be implemented.
]	(a) The capability to display a system use notification message
]	Displaying a system use notification message before authenticating.
]	(b) The capability to configurate a system use notification message
]	The following items are to be satisfied.
		i) Can be configurable by authorized personnel.
		ii) Cannot be configurable by unauthorized personnel.
	(2)	Confirmation of compensating countermeasure
		Confirm that the information is as described in Description of security capabilities.
	35.	Access via Untrusted Networks
	35. -1.	Access via Untrusted Networks If this requirement applies, either of the following (1) or (2) is to be performed.
	-1.	If this requirement applies, either of the following (1) or (2) is to be performed.
	-1. (1)	If this requirement applies, either of the following (1) or (2) is to be performed. Demonstration test for the capability to monitor and control access via untrusted networks
	-1. (1)	If this requirement applies, either of the following (1) or (2) is to be performed. Demonstration test for the capability to monitor and control access via untrusted networks Confirmation of compensating countermeasure
	-1. (1)	If this requirement applies, either of the following (1) or (2) is to be performed. Demonstration test for the capability to monitor and control access via untrusted networks Confirmation of compensating countermeasure Confirm that the information is as described in Description of security capabilities.
	-1. (1) (2)	If this requirement applies, either of the following (1) or (2) is to be performed. Demonstration test for the capability to monitor and control access via untrusted networks Confirmation of compensating countermeasure Confirm that the information is as described in Description of security capabilities.
	-1. (1) (2) 36.	If this requirement applies, either of the following (1) or (2) is to be performed. Demonstration test for the capability to monitor and control access via untrusted networks Confirmation of compensating countermeasure Confirm that the information is as described in Description of security capabilities. Explicit access request approval If this requirement applies, either of the following (1) or (2) is to be performed. Demonstration test for the capability to deny access from or via untrusted networks unless
	36.	If this requirement applies, either of the following (1) or (2) is to be performed. Demonstration test for the capability to monitor and control access via untrusted networks Confirmation of compensating countermeasure Confirm that the information is as described in Description of security capabilities. Explicit access request approval If this requirement applies, either of the following (1) or (2) is to be performed. Demonstration test for the capability to deny access from or via untrusted networks unless explicitly approved by authorized personnel on board
	36.	If this requirement applies, either of the following (1) or (2) is to be performed. Demonstration test for the capability to monitor and control access via untrusted networks Confirmation of compensating countermeasure Confirm that the information is as described in Description of security capabilities. Explicit access request approval If this requirement applies, either of the following (1) or (2) is to be performed. Demonstration test for the capability to deny access from or via untrusted networks unless explicitly approved by authorized personnel on board (a) The capability to assign access approval permissions to human users
	36. (1) (1) (2)	If this requirement applies, either of the following (1) or (2) is to be performed. Demonstration test for the capability to monitor and control access via untrusted networks Confirmation of compensating countermeasure Confirm that the information is as described in Description of security capabilities. Explicit access request approval If this requirement applies, either of the following (1) or (2) is to be performed. Demonstration test for the capability to deny access from or via untrusted networks unless explicitly approved by authorized personnel on board (a) The capability to assign access approval permissions to human users (b) The capability to deny unapproved access
	36.	If this requirement applies, either of the following (1) or (2) is to be performed. Demonstration test for the capability to monitor and control access via untrusted networks Confirmation of compensating countermeasure Confirm that the information is as described in Description of security capabilities. Explicit access request approval If this requirement applies, either of the following (1) or (2) is to be performed. Demonstration test for the capability to deny access from or via untrusted networks unless explicitly approved by authorized personnel on board (a) The capability to assign access approval permissions to human users (b) The capability to deny unapproved access Confirmation of compensating countermeasure
	36. (1) (1) (2)	If this requirement applies, either of the following (1) or (2) is to be performed. Demonstration test for the capability to monitor and control access via untrusted networks Confirmation of compensating countermeasure Confirm that the information is as described in Description of security capabilities. Explicit access request approval If this requirement applies, either of the following (1) or (2) is to be performed. Demonstration test for the capability to deny access from or via untrusted networks unless explicitly approved by authorized personnel on board (a) The capability to assign access approval permissions to human users (b) The capability to deny unapproved access
	361. (1) (1) (2) (2) (2)	If this requirement applies, either of the following (1) or (2) is to be performed. Demonstration test for the capability to monitor and control access via untrusted networks Confirmation of compensating countermeasure Confirm that the information is as described in Description of security capabilities. Explicit access request approval If this requirement applies, either of the following (1) or (2) is to be performed. Demonstration test for the capability to deny access from or via untrusted networks unless explicitly approved by authorized personnel on board (a) The capability to assign access approval permissions to human users (b) The capability to deny unapproved access Confirmation of compensating countermeasure Confirm that the information is as described in Description of security capabilities.
	361. (1) (1) (2) (2) (2)	If this requirement applies, either of the following (1) or (2) is to be performed. Demonstration test for the capability to monitor and control access via untrusted networks Confirmation of compensating countermeasure Confirm that the information is as described in Description of security capabilities. Explicit access request approval If this requirement applies, either of the following (1) or (2) is to be performed. Demonstration test for the capability to deny access from or via untrusted networks unless explicitly approved by authorized personnel on board (a) The capability to assign access approval permissions to human users (b) The capability to deny unapproved access Confirmation of compensating countermeasure

(1)	Demonstration test for the capability to terminate a remote session
	Either of the following functions is to be implemented.
	(a) Capability to terminate a remote session automatically
	The following items are to be complied with.
	i) The inactivity time until the end of the session is to be configurable.
	ii) The session is to be terminated after a configurable period of inactivity.
	(b) Capability to manually terminate a remote session.
	The session is to be terminated by operation of the user.
(2)	Confirmation of compensating countermeasure
	Confirm that the information is as described in Description of security capabilities.
38.	Cryptographic integrity protection
	The surveys are not required.
39.	Input validation
-1.	If this requirement applies, either of the following (1) or (2) is to be performed.
(1)	Demonstration test for the capability to validate the syntax, length and content of any
	input data
	If the data is determined to be invalid, take appropriate action. (e.g., refuse to accept the
	input data.)
(2)	Confirmation of compensating countermeasure
	Confirm that the information is as described in Description of security capabilities.
	Session integrity 16 diameter 15 and 16 diameter 17 and 16 diameter 17 and 16 diameter 18
	If this requirement applies, either of the following (1) or (2) is to be performed.
(1)	Demonstration test for the capability to protect the integrity of sessions and reject invalid session IDs
	The following items are to be satisfied.
	(a) Protecting the integrity of sessions and reject invalid session IDs(b) Rejecting invalid session IDs
(2)	Confirmation of compensating countermeasure
(2)	Confirm that the information is as described in Description of security capabilities.
	Commin that the information is as described in Bescription of security capacitaties.
41	Invalidation of session IDs after session termination
	If this requirement applies, either of the following (1) or (2) is to be performed.
-1.	If this requirement applies, chile of the following tirror (2) is to be benormed.
-1. (1)	
-1. (1)	Demonstration test for the capability to invalidate session IDs upon user logout or other session termination (including browser sessions)
	(2) 38. (1) (2) 40. (1) (2)

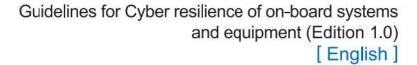
(3) Confirm that the information is as described in Description of security capabilities.

Secure development lifecycle requirements

■ Secure development lifecycle

1. C	ontrols for private keys
-1.	If the system includes software that is digitally signed, the following controls are to be
	included in the management system documentation. In addition, roles, responsibilities and
	work processes are to be addressed in accordance with the management system
	documentation.
(1)	Private key control policy
(2)	Procedural controls for private keys (e.g., procedures for generation, storage and use)
(3)	Technical controls for private keys (e.g., physical access restrictions and encryption
	hardware)
2. S	ecurity update documentation
-1.	The management system documentation includes a process for informing system owners
	of security updates.
	The information to be provided to the system owner shall include the following items:
(1)	The product version number(s) to which the security patch applies
(2)	Instructions on how to apply approved patches manually and via an automated process
(3)	Description of any impacts that applying the patch to the product can have, including
	reboot
(4)	Instructions on how to verify that an approved patch has been applied
(5)	Risks of not applying the patch and mediations that can be used for patches that are not
	approved or deployed by the asset owner
3. E	Dependent component and Operation system security update documentation
-1.	Management system documentation is to include processes for informing system owners
	as to whether systems support updated versions of acquired software.
	In addition, such information shall address how to manage risks related to not applying the
	updated acquired software.
4. S	ecurity Update Delivery
-1.	Management system documentation is to include processes for ensuring that security
	undates are provided to system awners

	In addition, such information is to include ways for verifying the authenticity of the
	updated software.
5. P	Product defence in depth
-1.	Management system documentation is to include processes for creating security
	defence-in-depth strategies.
6. E	Defence in depth measures expected in the environment
-1.	Management system documentation is to include processes for creating product user
	documentation that describes the security defence-in-depth measures expected to be
	provided by the external environments in which the products are used.
7. S	ecurity hardening guidelines
-1.	Management system documentation is to include processes for developing products that
	include product hardening guidelines for installation and maintenance.





NIPPON KAIJI KYOKAI

Innovation Development Division Maritime Education and **Training Certification Department**

4-7 Kioi-cho, Chiyoda-ku, Tokyo 102-8567, JAPAN Tel: +81-3-5226-2177 E-mail: met@classnk.or.jp

Plan Approval and Technical Solution Division **Machinery Department**

3-3 Kioi-cho, Chiyoda-ku, Tokyo 102-0094, JAPAN Tel: +81-3-5226-2022 E-mail: mcd@classnk.or.jp

www.classnk.com