2023

Guidance for Conformity Certification of Maritime Equipment Cyber Security

GC-31-E

KR

APPLICATION OF “GUIDANCE FOR CONFORMITY CERTIFICATION OF MARITIME EQUIPMENT CYBER SECURITY”

1. Unless expressly specified otherwise, the requirements in the Guidance apply to computer-based systems when the application for Certification of cyber security onboard ships is dated on or after 1 July 2023.
2. The amendments to the Guidance for 2021 edition and their effective date are as follows;

Effective Date : 1 July 2023

CHAPTER 1 GENERAL

Section 1 General

- 101. 1, 2, 3, and 4 have been amended.
- 102. has been amended.
- 105. has been newly added.

Section 2 Procedures for Certification

- newly added.

CHAPTER 2 COMMON REQUIREMENTS FOR EQUIPMENT CYBER SECURITY

- Completely amended.

CHAPTER 3 ADDITIONAL REQUIREMENTS FOR EQUIPMENT CYBER SECURITY

- Completely amended.

ANNEX 1 MAPPING THE REQUIREMENTS TO SECURITY LEVEL

- Completely amended..

CONTENTS

CHAPTER 1 GENERAL

Section 1 General

101. Application

1. This Guidance is to apply to all computer-based systems or their components mounted on ships and offshore facilities. *(2023)*
2. This Guidance defines the security level of computer-based systems and its requirement according to the level, and the application scope is determined by request of the ship owner. *(2023)*
3. Conformity certification in accordance with this Guidance is voluntary unless otherwise stated in the Rules for the Classification of Steel Ships(hereafter referred to as "the **Rules for Steel Ships**") and **Guidance for Approval of Manufacturing Process and Type Approval, Etc.** *(2023)*
4. This Guidance do not address the environmental performance of the hardware and software functions of computer-based systems. *(2023)*
5. Items not included in this Guidance may comply with ISO, IEC or equivalent recognized standards by the appropriate consideration of the Society.
6. Where the specific requirements in international regulation such as IMO are or as Information technology & operating technology develops, when it deems necessary, additional requirements to this Guidance may be required.

102. Definitions *(2023)*

The definitions of terms are to follow the **Rules for Steel ships**, unless otherwise specified in this Guidance.

1. **Authentication** refers to the verification of the claimed identity of an entity.
2. **Authenticator** refers to means used to confirm the identity of an entity.
3. **Authenticity** refers to the quality of records that can be deduced from internal and external evidence, including physical characteristics, structure, content and context of records, in which some records are intact and undamaged.
4. **Authorization** refers to privileges or permissions granted to system objects to access system resources.
5. **Availability** refers to property of ensuring timely and reliable access to and use of system information and functionality.
6. **Component** refers to entity belonging to a system that exhibits the characteristics of one or more of a host device, network device, software application, or embedded device.
7. **Confidentiality** refers to assurance that information is not disclosed to unauthorized individuals, processes, or device .
8. **Computer Based System(CBS)** refers to a programmable electronic device, or interoperable set of programmable electronic devices, organized to achieve one or more specified purposes such as collection, processing, maintenance, use, sharing, dissemination, or disposition of information. CBS on-board include IT and OT systems. A CBS may be a combination of subsystems connected via network. On-board CBS may be connected directly or via public means of communications (e.g. Internet) to ashore CBSs, other vessels' CBS and/or other facilities.
9. **Conduit** refers to a logical grouping of communication channels connecting two or more zones that share common security requirements.
10. **Device** refers to an individual physical asset that provides a set of functions.
11. **Embedded device** refers to a special purpose device designed to directly monitor or control a system is called a special purpose device.
12. **Event** refers to occurrence of or change to a particular set of circumstances.

13. **Firewall** refers to a logical or physical barrier that monitors and controls incoming and outgoing network traffic controlled via predefined rules.

14. **Firmware** refers to Software embedded in electronic devices that provide control, monitoring and data manipulation of engineered products and systems. These are normally self-contained and not accessible to user manipulation.

15. **Host** refers to general purpose device running an operating system capable of hosting one or more software applications, data stores or functions from one or more suppliers

16. **Identifier** refers to A pattern of symbols unique within a secure domain that represents or identifies the name of an entity claiming or requesting identity.

17. **Integrity** refers to property of protecting the accuracy and completeness of assets.

18. **Interface** refers to a logical entry point that provides access to a module for logical information flow.

19. **Least Privilege** refers to basic principle that holds that users (humans, software processes or devices) should be assigned the fewest privileges consistent with their assigned duties and functions.

20. **Malicious Code** refers to software used or created to disrupt computer operation.

21. **Mobile Code** refers to program transferred between assets that can be executed without explicit installation by the recipient.

22. **Network device** refers to device that facilitates data flow between devices, or restricts the flow of data, but does not directly interact with a control process.

23. **Non-repudiation** refers to ability to prove the occurrence of a claimed event or action and its originating entities.

24. **Patches** refers to software designed to update installed software or supporting data to address security vulnerabilities and other bugs or to improve operating systems or applications.

25. **Protocol** refers to a common set of rules and signals used by computers on a network to communicate.

26. **Recovery** refers to Maintain a resilience plan and develop and implement appropriate activities to restore functions or services that have been compromised by cyber security events. The recovery function supports timely return to normal operation to reduce the impact of cyber security events.

27. **Remote Access** refers to access to a component by any user (human, software process or device) communicating from outside the perimeter of the zone being addressed.

28. **Removable External Data Storage(REDS)** source refers to user removable non-network data source, including, but not limited to compact discs, memory sticks and Bluetooth devices.

29. **Secret** refers to A protected information state from being known by a system object except for the purpose of knowing the information.

30. **Security Level** refers to level corresponding to the required set of countermeasures and inherent security properties of devices and systems for a zone or conduit based on assessment of risk for the zone or conduit.

31. **Session** refers to semi-permanent, stateful and interactive information interchange between two or more communicating components.

32. **Switch** refers to a network infrastructure device that is used to interconnect nodes within a network.

33. **Untrusted** refers to not meeting predefined requirements to ensure that an operation, data transaction source, network or software process can be relied upon to behave as expected.

34. **User** refers to individuals, organizational objects, or automated processes that access the system, whether authorized or not.

35. **Update** refer to A gradual change to hardware or software to address a security vulnerability, bug, reliability, or operational problem.

36. **Upgrade** refer to A gradual hardware or software change to add new functionality.

37. Zone refer to A set of entities representing the division of a system based on functional, logical, and physical (including location) relationships.

103. Equivalence

The equivalence of alternative and novel features which deviate from or are not directly applicable to the Guidance is to be in accordance with **Pt 1**, **Ch 1**, **104**. of **Rules for the Classification of Steel Ships**. *(2020)*

104. Exclusion from the Guidance

The Society cannot assume responsibility for other technical characteristics for cyber-physical systems not covered by this Guidance. However, the Society may advise on such matters upon inquiry.

105. References *(2023)*

For the purpose of application of the requirements of this Guidance, the following identified standards can be used and other industry standars my be considered:

(1) IEC 62443-3-3, Industrial communication networks - Network and system security. Part 3-3: System security requirements and security levels

(2) IEC 62443-4-2, Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components.

Section 2 Procedures for Certification *(2023)*

201. Certification application

1. The applicant is, in principle, to be the manufacturer of the computer-based systems and/or that component. However, the applicant, where deemed appropriate by the Society, need not always be the manufacturer of the computer-based systems and/or that component.

2. The manufacturer wishing to obtain a conformity certification is to submit a copy of the application of conformity certification of the Society, together with three copies of the required data for approval and two copies of the required data for reference, to the Society. However, the required data previously submitted to the Society, according to the Technical Rules, may be exempted from submission.

3. The Society may require the submission of the data specified in **4.** where deemed necessary by the Society.

4. Document for approval

(1) Specification of cyber security functions

(A) Description of how the system meets the applicable requirements

(B) Description of items whose cyber security requirements are not related to components of the system.(If applicable)

(C) Intercomponent authentication mechanism data.(If applicable)

(2) Network topology diagram

(A) Source and Destination IP addresses.(If applicable)

(B) Physical connection method.(e.g. Ethernet, RS-232, RS-422, etc.)

(3) System drawings

(A) Physical interface of each component.(network port, serial port)

(B) Each component's wireless interface.(e.g. WIFI, cellular, Bluetooth, mobile hotspot, etc.) (if applicable)

(4) List of assets

(A) Name of component

(B) Brand/Manufacturer (Supplier)

(C) Model or reference number (some units may contain multiple reference numbers)

(D) Operating system current version and embedded firmware (software version) and implementation date

(5) Cyber security conformity test procedures

(A) Necessary test setup

(B) Initial condition

(C) Test methodology

(D) Test equipment

(E) Acceptance criteria

(6) Report of vulnerability scanning

5. Document for reference

(1) Manual for user and/or operator

202. Document review

The Society examines the conformity test program, drawings and data and where deemed appropriate, those are to be approved and returned to the manufacturers.

203. Cyber security conformity test

1. After completion of the document reviews specified in **202.**, the cyber security conformity tests are to be carried out for the test products in the presence of the Surveyor in accordance with the approved conformity test program and test method as deemed appropriate by the Society.

2. Products which have been failed to pass the cyber security conformity tests specified in **1.** should not be retested without revision of drawings and/or specifications. If, following analysis of the experimental data from tests, it is found that the failure of conformity tests have been caused by the poor test conditions, etc., retest without revision may be permitted subject to the Society's approval.

3. In principle, the conformity tests are to be carried out at the manufacturing sites. However, the test may be done outside of manufacturing sites subject to the Society's approval.

4. The conformity tests may be partly or wholly omitted, subject to the approval by the Society, in cases where the manufacturer has been approved by other Classification Society or an inspection organization recognized by the Society.

5. After completion of the conformity tests, the manufacturer is to submit three copies of the test records to the Society.

204. Plant audit

This is to comply with the requirements in **Ch 3 105. of Guidance for Approval of Manufacturing Process and Type Approval, Etc.** Where type approval of equipment is carried out simultaneously or already done, plant audit may be omitted.

205. Notification and announcement of approval

This is to comply with the requirements in **Ch 3 106. of Guidance for Approval of Manufacturing Process and Type Approval, Etc.**

206. Changes in the approved contents

This is to comply with the requirements in **Ch 3 107. of Guidance for Approval of Manufacturing Process and Type Approval, Etc.**

207. Validity and renewal of approval certificate

1. The approval certificate will be valid within three years from the date of issue. In case where the approval certificate is renewed in accordance with the requirements specified in the preceding **206.**, the expiration date will not be changed.

2. This is to comply with the requirements in **Ch 3 108. of Guidance for Approval of Manufacturing Process and Type Approval, Etc.** However, the renewed approval certificate will be valid within three years from the expiry date of old approval certificate.

208. Confirmation test and/or occasional plant audit

This is to comply with the requirements in **Ch 3 109. of Guidance for Approval of Manufacturing Process and Type Approval, Etc.**

209. Suspension or withdrawal of approval

This is to comply with the requirements in **Ch 3 110. of Guidance for Approval of Manufacturing Process and Type Approval, Etc.** ⚓

CHAPTER 2 COMMON REQUIREMENTS FOR EQUIPMENT CYBER SECURITY *(2023)*

Section 1 General

101. General

1. The common requirements for equipment cyber security are defined as shown in **Table 1** based on the foundational requirements of IEC 62443-4-2.

Table 1 Common Requirement for Equipment cyber security

Common Requirement	Definition
Identification and authentication control	Identify and authenticate all users (humans, software processes and devices), and allow them access to the system or assets.
Use control	Enforce the assigned privileges of an authenticated user (human, software process or device) to perform the requested action on the application or device and monitor the use of these privileges.
System integrity	Ensure the integrity of the application or device to prevent unauthorized manipulation.
Data confidentiality	Ensure the confidentiality of information on communication channels and in data repositories to prevent unauthorized disclosure.
Restricted data flow	Segment the control system via zones and conduits to limit the unnecessary flow of data.
Timely response to events	Respond to security violations by notifying the proper authority, reporting needed evidence of the violation and taking timely corrective action when incidents are discovered.
Resource availability	Ensure the availability of the application or device against the degradation or denial of essential services.

2. The security level (SL) is defined as shown in **Table 2**, and Unless expressly specified otherwise, in order for a component to comply with high security level requirements, it should comply with all of the lower security level requirements.

Table 2 Definition of Security Level (SL)

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

Section 2 Identification and authentication

201. Human user identification and authentication *(2021)*

1. Components should provide the capability to identify and authenticate all human users according to ISA 62443-3-3 SR 1.1 on all interfaces capable of human user access. However, User identification and authentication should not hamper fast, local emergency actions.

2. Components should provide the capability to uniquely identify and authenticate all human users.

3. Components should provide the capability to employ multifactor authentication for all human user access to the component.

4. Requirements for SLs

(1) SL 1 : **201. 1**
(2) SL 2 : **201. 2**
(3) SL 3 : **201. 3**
(4) SL 4 : **201. 3**

202. Software process and device identification and authentication

1. Components should provide the capability to identify itself and authenticate to any other component (software application, embedded devices, host devices and network devices), according to ISA 62443-3-3 SR 1.2. *(2021)*

2. Components should provide the capability to uniquely identify and authenticate itself to any other component.

3. Requirements for SLs

(1) SL 1 : Not applicable
(2) SL 2 : **202. 1**
(3) SL 3 : **202. 2**
(4) SL 4 : **202. 2**

203. Account management

1. Components should provide the capability to support the management of all accounts directly or integrated into a system that manages accounts according to ISA 62443-3-3 SR 1.3. *(2021)*

2. Requirements for SLs

(1) SL 1 : **203. 1**
(2) SL 2 : **203. 1**
(3) SL 3 : **203. 1**
(4) SL 4 : **203. 1**

204. Identifier management

1. Components should provide the capability to integrate into a system that supports the management of identifiers and/or provide the capability to support the management of identifiers directly according to ISA 62443-3-3 SR 1.4. *(2021)*

2. Requirements for SLs

(1) SL 1 : **204. 1**
(2) SL 2 : **204. 1**
(3) SL 3 : **204. 1**
(4) SL 4 : **204. 1**

205. Authenticator management

1. Components should provide the capability to:

(1) support the use of initial authenticator content;
(2) support the recognition of changes to default authenticators made at installation time;

(3) function properly with periodic authenticator change/refresh operation; and
(4) protect authenticators from unauthorized disclosure and modification when stored, used and transmitted.

2. The authenticators on which the component rely should be protected via hardware mechanisms like OTP memory.

3. Requirements for SLs

(1) SL 1 : **205. 1**
(2) SL 2 : **205. 1**
(3) SL 3 : **205. 2**
(4) SL 4 : **205. 2**

206. Strength of password-based authentication

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

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

3. Components should provide, or integrate into a system that provides, the capability to protect against any given human user account from reusing a password for a configurable number of generations. In addition, the component should provide the capability to enforce password minimum and maximum lifetime restrictions for human users. These capabilities should conform to commonly accepted security industry practices.

4. Components should provide the capability to prompt the user to change their password upon a configurable time prior to expiration.

5. Requirements for SLs

(1) SL 1 : **206. 2**
(2) SL 2 : **206. 2**
(3) SL 3 : **206. 3**
(4) SL 4 : **206. 4**

207. Public key infrastructure certificates

1. When public key infrastructure (PKI) is utilized, the component should provide or integrate into a system that provides the capability to interact and operate in accordance with ISA 62443-3-3 SR 1.8. *(2021)*

2. Requirements for SLs

(1) SL 1 : Not applicable
(2) SL 2 : **207. 1**
(3) SL 3 : **207. 1**
(4) SL 4 : **207. 1**

208. Strength of public key-based authentication

1. For components that utilize public-key-based authentication, those components should provide directly or integrate into a system that provides the capability within the same environment to:

(1) validate certificates by checking the validity of the signature of a given certificate;
(2) validate the certificate chain or, in the case of self-signed certificates, by deploying leaf certificates to all hosts that communicate with the subject to which the certificate is issued;
(3) validate certificates by checking a given certificate's revocation status;
(4) establish user (human, software process or device) control of the corresponding private key;
(5) map the authenticated identity to a user (human, software process or device); and
(6) ensure that the algorithms and keys used for the public key authentication comply with **503.**

2. Components should provide the capability to protect critical, long-lived private keys via hardware mechanisms.

3. Requirements for SLs

(1) SL 1 : Not applicable
(2) SL 2 : **208. 1**
(3) SL 3 : **208. 2**
(4) SL 4 : **208. 2**

209. Authenticator feedback

1. When a component provides an authentication capability the component should provide the capability to obscure feedback of authenticator information during the authentication process.

2. Requirements for SLs

(1) SL 1 : **209. 1**
(2) SL 2 : **209. 1**
(3) SL 3 : **209. 1**
(4) SL 4 : **209. 1**

210. Unsuccessful login attempts

1. When a component provides an authentication capability the component should provide the capability to enforce a limit of a configurable number of consecutive invalid access attempts by any user (human, software process or device) during a configurable time period and deny access for a specified period of time or until unlocked by an administrator when this limit has been reached.

2. Requirements for SLs

(1) SL 1 : **210. 1**
(2) SL 2 : **210. 1**
(3) SL 3 : **210. 1**
(4) SL 4 : **210. 1**

211. System use notification

1. When a component provides local human user access/HMI, it should provide the capability to display a system use notification message before authenticating. The system use notification message should be configurable by authorized personnel.

2. Requirements for SLs

(1) SL 1 : **211. 1**
(2) SL 2 : **211. 1**
(3) SL 3 : **211. 1**
(4) SL 4 : **211. 1**

212. Strength of symmetric key-based authentication

1. For components that utilize symmetric keys, the component should provide the capability to:

(1) establish the mutual trust using the symmetric key
(2) store securely the shared secret (the authentication is valid as long as the shared secret remains secret)
(3) restrict access to the shared secret
(4) ensure that the algorithms and keys used for the symmetric key authentication comply with **503.**

2. Components should provide the capability to protect critical, long lived symmetric keys via hardware mechanisms.

3. Requirements for SLs

(1) SL 1 : Not applicable
(2) SL 2 : **212. 1**
(3) SL 3 : **212. 2**
(4) SL 4 : **212. 2**

Section 3 Use Control

301. Authorization enforcement

1. Components should provide an authorization enforcement mechanism for all identified and authenticated users based on their assigned responsibilities.

2. Components should provide an authorization enforcement mechanism for all users based on their assigned responsibilities and least privilege.

3. Components should, directly or through a compensating security mechanism, provide for an authorized role to define and modify the mapping of permissions to roles for all human users.

4. Components should support a supervisor manual override for a configurable time or sequence of events.

5. Components should support dual approval when action can result in serious impact on the industrial process. However, dual approval mechanisms should not be employed when an immediate response is necessary to safeguard health, safety and environment consequences, for example, emergency shutdown of an industrial process

6. **Requirements for SLs**

(1) SL 1 : **301. 1**
(2) SL 2 : **301. 3**
(3) SL 3 : **301. 4**
(4) SL 4 : **301. 5**

302. Wireless use

1. If a component supports usage through wireless interfaces it should provide the capability to integrate into the system that supports usage authorization, monitoring and restrictions according to commonly accepted industry practices.

2. **Requirements for SLs**

(1) SL 1 : **302. 1**
(2) SL 2 : **302. 1**
(3) SL 3 : **302. 1**
(4) SL 4 : **302. 1**

303. Session lock

1. If a component provides a human user interface, whether accessed locally or via a network, the component should provide the capability

(1) to protect against further access by initiating a session lock after a configurable time period of inactivity or by manual initiation by the user (human, software process or device); and
(2) for the session lock to remain in effect until the human user who owns the session, or another authorized human user, re-establishes access using appropriate identification and authentication procedures.

2. **Requirements for SLs**

(1) SL 1 : **303. 1**
(2) SL 2 : **303. 1**
(3) SL 3 : **303. 1**
(4) SL 4 : **303. 1**

304. Remote session termination

1. If a component supports remote sessions, the component should provide the capability to terminate a remote session either automatically after a configurable time period of inactivity, manually by a local authority, or manually by the user (human, software process or device) who initiated the session.

2. **Requirements for SLs**

(1) SL 1 : Not applicable
(2) SL 2 : **304. 1**
(3) SL 3 : **304. 1**
(4) SL 4 : **304. 1**

305. Concurrent session control

1. Components should provide the capability to limit the number of concurrent sessions per interface for any given user (human, software process or device).

2. Requirements for SLs

(1) SL 1 : Not applicable
(2) SL 2 : Not applicable
(3) SL 3 : **305. 1**
(4) SL 4 : **305. 1**

306. Auditable events

1. Components should provide the capability to generate audit records relevant to security for the following categories:

(1) access control
(2) request errors
(3) system events
(4) backup and restore event
(5) configuration changes
(6) audit log events

2. Individual audit records should include:

(1) timestamp
(2) source (originating device, software process or human user account)
(3) category
(4) type
(5) event ID
(6) event result

3. Requirements for SLs

(1) SL 1 : **306. 2**
(2) SL 2 : **306. 2**
(3) SL 3 : **306. 2**
(4) SL 4 : **306. 2**

307. Audit storage capacity

1. Components should provide the capability to allocate audit record storage capacity according to commonly recognized recommendations for log management and provide mechanisms to protect against a failure of the component when it reaches or exceeds the audit storage capacity.

2. Components should provide the capability to issue a warning when the allocated audit record storage reaches a configurable threshold.

3. Requirements for SLs

(1) SL 1 : **307. 1**
(2) SL 2 : **307. 1**
(3) SL 3 : **307. 2**
(4) SL 4 : **307. 2**

308. Response to audit processing failures

1. Components should provide the following capability to protect against the loss of essential services and functions in the event of an audit processing failure and to support appropriate actions in response to an audit processing failure according to commonly accepted industry practices and recommendations.

2. Requirements for SLs

(1) SL 1 : **308. 1**
(2) SL 2 : **308. 1**
(3) SL 3 : **308. 1**
(4) SL 4 : **308. 1**

309. Timestamps

1. Components should provide the capability to create timestamps (including date and time) for use in audit records.

2. Components should provide the capability to create timestamps that are synchronized with a system wide time source.

3. The time synchronization mechanism should provide the capability to detect unauthorized alteration and cause an audit event upon alteration.

4. Requirements for SLs

(1) SL 1 : **309. 1**
(2) SL 2 : **309. 2**
(3) SL 3 : **309. 2**
(4) SL 4 : **309. 3**

310. Non-repudiation

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

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

3. Requirements for SLs

(1) SL 1 : **310. 1**
(2) SL 2 : **310. 1**
(3) SL 3 : **310. 1**
(4) SL 4 : **310. 2**

311. Use control for portable and mobile devices

1. When components supports use of portable and mobile devices, the system should include the capability to;

(1) Limit the use of portable and mobile devices only to those permitted by design
(2) Restrict code and data transfer to/from portable and mobile devices
Note : Port limits / blockers (and silicone) could be accepted for a specific system

2. Requirements for SLs

(1) SL 1 : **311. 1**
(2) SL 2 : **311. 1**
(3) SL 3 : **311. 1**
(4) SL 4 : **311. 1**

Section 4 System Integrity

401. Communication integrity

1. Components should provide the capability to protect integrity of transmitted information.

2. Components should provide the capability to verify the authenticity of received information during communication.

3. Requirements for SLs

(1) SL 1 : **401. 1**
(2) SL 2 : **401. 2**
(3) SL 3 : **401. 2**
(4) SL 4 : **401. 2**

402. Security functionality verification

1. Components should provide the capability to support verification of the intended operation of security functions according to ISA 62443-3-3 SR 3.3. *(2021)*

2. Components should provide the capability to support verification of the intended operation of security functions during normal operations.

3. Requirements for SLs

(1) SL 1 : **402. 1**
(2) SL 2 : **402. 1**
(3) SL 3 : **402. 1**
(4) SL 4 : **402. 2**

403. Software and information integrity

1. Components should provide the capability to perform or support integrity checks on software, configuration and other information as well as the recording and reporting of the results of these checks or be integrated into a system that can perform or support integrity checks.

2. Components should provide the capability to perform or support authenticity checks on software, configuration and other information as well as the recording and reporting of the results of these checks or be integrated into a system that can perform or support authenticity checks.

3. If the component is performing the integrity check, it should be capable of automatically providing notification to a configurable entity upon discovery of an attempt to make an unauthorized change.

4. Requirements for SLs

(1) SL 1 : **403. 1**
(2) SL 2 : **403. 2**
(3) SL 3 : **403. 3**
(4) SL 4 : **403. 3**

404. Input validation

1. Components should validate the syntax, length and content of any input data that is used as an industrial process control input or input via external interfaces that directly impacts the action of the component.

2. Requirements for SLs

(1) SL 1 : **404. 1**
(2) SL 2 : **404. 1**
(3) SL 3 : **404. 1**
(4) SL 4 : **404. 1**

405. Deterministic output

1. Components that physically or logically connect to an automation process should provide the capability to set outputs to a predetermined state if normal operation as defined by the component supplier cannot be maintained.

2. Requirements for SLs

(1) SL 1 : **405. 1**
(2) SL 2 : **405. 1**
(3) SL 3 : **405. 1**
(4) SL 4 : **405. 1**

406. Error handling

1. Components should identify and handle error conditions in a manner that does not provide information that could be exploited by adversaries to attack the components.

2. Requirements for SLs

(1) SL 1 : Not applicable
(2) SL 2 : **406. 1**
(3) SL 3 : **406. 1**
(4) SL 4 : **406. 1**

407. Session integrity

1. Components should provide mechanisms to protect the integrity of communications sessions including:

(1) the capability to invalidate session identifiers upon user logout or other session termination (including browser sessions)
(2) the capability to generate a unique session identifier for each session and recognize only session identifiers that are system-generated
(3) the capability to generate unique session identifiers with commonly accepted sources of randomness

2. Requirements for SLs

(1) SL 1 : Not applicable
(2) SL 2 : **407. 1**
(3) SL 3 : **407. 1**
(4) SL 4 : **407. 1**

408. Protection of audit information

1. Components should protect audit information, audit logs, and audit tools (if present) from unauthorized access, modification and deletion.

2. Components should provide the capability to store audit records on hardware-enforced write-once media.

3. Requirements for SLs

(1) SL 1 : Not applicable
(2) SL 2 : **408. 1**
(3) SL 3 : **408. 1**
(4) SL 4 : **408. 2**

Section 5 Data Confidentiality

501. Communication integrity

1. Components should provide the capability to protect the confidentiality of information at rest for which explicit read authorization is supported and support the protection of the confidentiality of information in transit as defined in ISA 62443-3-3 SR 4.1. *(2021)*

2. Requirements for SLs

(1) SL 1 : **501. 1**
(2) SL 2 : **501. 1**
(3) SL 3 : **501. 1**
(4) SL 4 : **501. 1**

502. Information persistence

1. Components should provide the capability to erase all information, for which explicit read authorization is supported, from components to be released from active service and/or decommissioned.

2. Components should provide the capability to protect against unauthorized and unintended information transfer via volatile shared memory resources.

3. Components should provide the capability to verify that the erasure of information occurred.

4. Requirements for SLs

(1) SL 1 : Not applicable
(2) SL 2 : **502. 1**
(3) SL 3 : **502. 3**
(4) SL 4 : **502. 3**

503. Use of cryptography

1. If cryptography is required, the component should use cryptographic security mechanisms according to internationally recognized and proven security practices and recommendations.

2. Requirements for SLs

(1) SL 1 : **503. 1**
(2) SL 2 : **503. 1**
(3) SL 3 : **503. 1**
(4) SL 4 : **503. 1**

Section 6 Restricted Data Flow

601. Network segmentation

1. Components should support a segmented network to support zones and conduits, as needed, to support the broader network architecture based on logical segmentation and criticality.

2. Requirements for SLs

(1) SL 1 : **601. 1**
(2) SL 2 : **601. 1**
(3) SL 3 : **601. 1**
(4) SL 4 : **601. 1**

Section 7 Timely Response to Events

701. Audit log accessibility

1. Components should provide the capability for authorized humans and/or tools to access audit logs on a read-only basis.

2. Components should provide programmatic access to audit records by either using an application programming interface (API) or sending the audit records to a centralized system.

3. Requirements for SLs

(1) SL 1 : **701. 1**
(2) SL 2 : **701. 1**
(3) SL 3 : **701. 2**
(4) SL 4 : **701. 2**

702. Continuous monitoring

1. Components should provide the capability to be continuously monitored using commonly accepted security industry practices and recommendations to detect, characterize and report security breaches in a timely manner.

2. Requirements for SLs

(1) SL 1 : Not applicable
(2) SL 2 : **702. 1**
(3) SL 3 : **702. 1**
(4) SL 4 : **702. 1**

Section 8 Resource Availability

801. Denial of service(DoS) protection

1. Components should provide the capability to maintain essential functions when operating in a degraded mode as the result of a DoS event.

2. Components should provide the capability to mitigate the effects of information and/or message flooding types of DoS events.

3. Requirements for SLs

(1) SL 1 : **801. 1**
(2) SL 2 : **801. 2**
(3) SL 3 : **801. 2**
(4) SL 4 : **801. 2**

802. Resource management

1. Components should provide the capability to limit the use of resources by security functions to protect against resource exhaustion.

2. Requirements for SLs

(1) SL 1 : **802. 1**
(2) SL 2 : **802. 1**
(3) SL 3 : **802. 1**
(4) SL 4 : **802. 1**

803. System backup

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

2. Components should provide the capability to validate the integrity of backed up information prior to the initiation of a restore of that information.

3. Requirements for SLs

(1) SL 1 : **803. 1**
(2) SL 2 : **803. 2**
(3) SL 3 : **803. 2**
(4) SL 4 : **803. 2**

804. System recovery and reconstitution

1. Components should provide the capability to be recovered and reconstituted to a known secure state after a disruption or failure.

2. Requirements for SLs

(1) SL 1 : **804. 1**
(2) SL 2 : **804. 1**
(3) SL 3 : **804. 1**
(4) SL 4 : **804. 1**

805. Network and security configuration settings

1. Components should provide the capability to be configured according to recommended network and security configurations as described in guidelines provided by the system supplier. The component should provide an interface to the currently deployed network and security configuration settings.

2. Components should provide the capability to generate a report listing the currently deployed security settings in a machine-readable format.

3. Requirements for SLs

(1) SL 1 : **805. 1**
(2) SL 2 : **805. 1**
(3) SL 3 : **805. 2**
(4) SL 4 : **805. 2**

806. Least functionality

1. Components should provide the capability to specifically restrict the use of unnecessary functions, ports, protocols and/or services.

2. Requirements for SLs

(1) SL 1 : **806. 1**
(2) SL 2 : **806. 1**
(3) SL 3 : **806. 1**
(4) SL 4 : **806. 1**

807. System component inventory

1. Components should provide the capability to support a system component inventory according to ISA 62443-3-3 SR 7.8.

2. Requirements for SLs

(1) SL 1 : Not applicable
(2) SL 2 : **807. 1**
(3) SL 3 : **807. 1**
(4) SL 4 : **807. 1** ⚓

CHAPTER 3 ADDITIONAL REQUIREMENTS FOR EQUIPMENT CYBER SECURITY *(2023)*

Section 1 General

101. General

1. The additional requirements for equipment cyber security are defined as shown in **Table 3** based on the component requirements of IEC 62443-4-2.

Table 3 Definition of Additional requirement for equipment cyber security

Additional Requirement	Definition
Software Application	Software programs executing on the infrastructure that are used to interface with the process or the control system itself For example, configuration software and historian, etc.
Embedded Device	Special purpose device running embedded software designed to directly monitor, control or actuate an industrial process For example, PLC, IED(Intelligent Electronic Device), etc.
Host Device	General purpose device running a general purpose operating system capable of hosting one or more applications, data stores or functions For example, Operation workstation, Data historian, etc.
Network Device	Device that facilitates data flow between devices, or restricts the flow of data, but does not directly interact with a control process For example, Switch, Router, VPN terminator, etc.

Section 2 Additional Requirements for Software Application

201. Mobile code

1. In the event that a software application utilizes mobile code technologies, that application should provide the capability to enforce a security policy for the usage of mobile code technologies. The security policy should allow, at a minimum, the following actions for each mobile code technology used on the software application:

(1) Control execution of mobile code
(2) Control which users (human, software process, or device) are allowed to transfer mobile code to/from the application
(3) Control the execution of mobile code based on the results of an integrity check prior to the code being executed

2. The application should provide the capability to enforce a security policy that allows the device to control execution of mobile code based on the results of an authenticity check prior to the code being executed.

3. Requirements for SLs

(1) SL 1 : **201. 1**
(2) SL 2 : **201. 2**
(3) SL 3 : **201. 2**
(4) SL 4 : **201. 2**

202. Protection from malicious code

1. The application product supplier should qualify and document which protection from malicious code mechanisms are compatible with the application and note any special configuration requirements.

2. Requirements for SLs

(1) SL 1 : **202. 1**
(2) SL 2 : **202. 1**
(3) SL 3 : **202. 1**
(4) SL 4 : **202. 1**

Section 3 Additional Requirements for Embedded Device

301. Mobile code

1. In the event that an embedded device utilizes mobile code technologies, the embedded device should provide the capability to enforce a security policy for the usage of mobile code technologies. The security policy should allow, at a minimum, the following actions for each mobile code technology used on the embedded device:

(1) Control execution of mobile code
(2) Control which users (human, software process, or device) are allowed to transfer mobile code to the device
(3) Control the execution of mobile code based on the results of an integrity check prior to the code being executed

2. The embedded device should provide the capability to enforce a security policy that allows the device to control execution of mobile code based on the results of an authenticity check prior to the code being executed.

3. Requirements for SLs

(1) SL 1 : **1001. 1**
(2) SL 2 : **1001. 2**
(3) SL 3 : **1001. 2**
(4) SL 4 : **1001. 2**

302. Use of physical diagnostic and test interfaces

1. Embedded devices should protect against unauthorized use of the physical factory diagnostic and test interface(s).

2. Embedded devices should provide active monitoring of the device's diagnostic and test interface(s) and generate an audit log entry when attempts to access these interface(s) are detected.

3. Requirements for SLs

(1) SL 1 : Not applicable
(2) SL 2 : **1002. 1**
(3) SL 3 : **1002. 2**
(4) SL 4 : **1002. 2**

303. Protection from malicious code

1. The embedded device should provide the capability to protect from installation and execution of unauthorized software.

2. Requirements for SLs

(1) SL 1 : Not applicable
(2) SL 2 : **1003. 1**
(3) SL 3 : **1003. 1**
(4) SL 4 : **1003. 1**

304. Support for updates

1. The embedded device should support the ability to be updated and upgraded.

2. The embedded device should validate the authenticity and integrity of any software update or upgrade prior to installation.

3. Requirements for SLs

(1) SL 1 : **1004. 1**
(2) SL 2 : **1004. 2**
(3) SL 3 : **1004. 2**
(4) SL 4 : **1004. 2**

305. Physical tamper resistance and detection

1. The embedded device should provide tamper resistance and detection mechanisms to protect against unauthorized physical access into the device.

2. The embedded device should be capable of automatically providing notification to a configurable set of recipients upon discovery of an attempt to make an unauthorized physical access. All notifications of tampering should be logged as part of the overall audit logging function.

3. Requirements for SLs

(1) SL 1 : Not applicable
(2) SL 2 : **1005. 1**
(3) SL 3 : **1005. 2**
(4) SL 4 : **1005. 2**

306. Provisioning product supplier roots of trust

1. Embedded devices should provide the capability to provision and protect the confidentiality, integrity, and authenticity of product supplier keys and data to be used as one or more “roots of trust” at the time of manufacture of the device.

2. Requirements for SLs

(1) SL 1 : Not applicable
(2) SL 2 : **1006. 1**
(3) SL 3 : **1006. 1**
(4) SL 4 : **1006. 1**

307. Physical tamper resistance and detection

1. Embedded devices should provide the capability to provision and protect the confidentiality, integrity, and authenticity of asset owner keys and data to be used as “roots of trust”; and support the capability to provision without reliance on components that may be outside of the device’s security zone.

2. Requirements for SLs

(1) SL 1 : Not applicable
(2) SL 2 : **1007. 1**
(3) SL 3 : **1007. 1**
(4) SL 4 : **1007. 1**

308. Integrity of the boot process

1. Embedded devices should verify the integrity of the firmware, software, and configuration data needed for the component’s boot and runtime processes prior to use.

2. Embedded devices should use the component’s product supplier roots of trust to verify the authenticity of the firmware, software, and configuration data needed for the component’s boot process prior to it being used in the boot process.

3. Requirements for SLs

(1) SL 1 : **1008. 1**
(2) SL 2 : **1008. 2**
(3) SL 3 : **1008. 2**
(4) SL 4 : **1008. 2**

Section 4 Additional Requirements for Host Device *(2023)*

401. Mobile code

1. In the event that a host device utilizes mobile code technologies, that host device should provide the capability to enforce a security policy for the usage of mobile code technologies. The security policy should allow, at a minimum, the following actions for each mobile code technology used on the host device:

(1) Control execution of mobile code

(2) Control which users (human, software process, or device) are allowed to upload mobile code to the host device

(3) Control the code execution based upon integrity checks on the mobile code and prior to the code being executed.

2. The embedded device should provide the capability to enforce a security policy that allows the device to control execution of mobile code based on the results of an authenticity check prior to the code being executed.

3. Requirements for SLs

(1) SL 1 : **1101. 1**
(2) SL 2 : **1101. 2**
(3) SL 3 : **1101. 2**
(4) SL 4 : **1101. 2**

402. Use of physical diagnostic and test interfaces

1. Embedded devices should protect against unauthorized use of the physical factory diagnostic and test interface(s).

2. Embedded devices should provide active monitoring of the device’s diagnostic and test interface(s) and generate an audit log entry when attempts to access these interface(s) are detected.

3. Requirements for SLs

(1) SL 1 : Not applicable
(2) SL 2 : **1102. 1**
(3) SL 3 : **1102. 2**
(4) SL 4 : **1102. 2**

403. Protection from malicious code

1. To provide protection from malicious codes, there should be a mechanism for host device qualified by the product supplier. The product supplier should document special configuration requirements related to protection against malicious codes.

2. Host device should automatically report malware protection software and file version in use (as part of the full logging function)

3. Requirements for SLs

(1) SL 1 : **1103. 1**
(2) SL 2 : **1103. 2**
(3) SL 3 : **1103. 2**
(4) SL 4 : **1103. 2**

404. Support for updates

1. The embedded device should support the ability to be updated and upgraded.

2. The embedded device should validate the authenticity and integrity of any software update or upgrade prior to installation.

3. Requirements for SLs

(1) SL 1 : **1104. 1**

(2) SL 2 : **1104. 2**
(3) SL 3 : **1104. 2**
(4) SL 4 : **1104. 2**

405. Physical tamper resistance and detection

1. The embedded device should provide tamper resistance and detection mechanisms to protect against unauthorized physical access into the device.

2. The embedded device should be capable of automatically providing notification to a configurable set of recipients upon discovery of an attempt to make an unauthorized physical access. All notifications of tampering should be logged as part of the overall audit logging function.

3. Requirements for SLs

(1) SL 1 : Not applicable
(2) SL 2 : **1105. 1**
(3) SL 3 : **1105. 2**
(4) SL 4 : **1105. 2**

406. Provisioning product supplier roots of trust

1. Host devices should provide the capability to provision and protect the confidentiality, integrity, and authenticity of product supplier keys and data to be used as one or more “roots of trust” at the time of manufacture of the device.

2. Requirements for SLs

(1) SL 1 : Not applicable
(2) SL 2 : **1106. 1**
(3) SL 3 : **1106. 1**
(4) SL 4 : **1106. 1**

407. Provisioning asset owner roots of trust

1. Host devices should provide the capability to provision and protect the confidentiality, integrity, and authenticity of asset owner keys and data to be used as “roots of trust” and support the capability to provision without reliance on components that may be outside of the device’s security zone.

2. Requirements for SLs

(1) SL 1 : Not applicable
(2) SL 2 : **1107. 1**
(3) SL 3 : **1107. 1**
(4) SL 4 : **1107. 1**

408. Integrity of the boot process

1. Host devices should verify the integrity of the firmware, software, and configuration data needed for component’s boot process prior to it being used in the boot process.

2. Host devices should use the component’s product supplier roots of trust to verify the authenticity of the firmware, software, and configuration data needed for component’s boot process prior to it being used in the boot process.

3. Requirements for SLs

(1) SL 1 : **1108. 1**
(2) SL 2 : **1108. 2**
(3) SL 3 : **1108. 2**
(4) SL 4 : **1108. 2**

Section 5 Additional Requirements for Network Device *(2023)*

501. Wireless access management

1. A network device supporting wireless access management should provide the capability to identify and authenticate all users (humans, software processes or devices) engaged in wireless communication.

2. The network device should provide the capability to uniquely identify and authenticate all users (humans, software processes or devices) engaged in wireless communication.

3. Requirements for SLs

(1) SL 1 : **1201. 1**
(2) SL 2 : **1201. 2**
(3) SL 3 : **1201. 2**
(4) SL 4 : **1201. 2**

502. Access via untrusted networks

1. The network device supporting device access into a network should provide the capability to monitor and control all methods of access to the network device via untrusted networks.

2. The network device should provide the capability to deny access requests via untrusted networks unless explicitly approved by an assigned role.

3. Requirements for SLs

(1) SL 1 : **1202. 1**
(2) SL 2 : **1202. 1**
(3) SL 3 : **1202. 2**
(4) SL 4 : **1202. 2**

503. Mobile code

1. In the event that a network device utilizes mobile code technologies, the network device should provide the capability to enforce a security policy for the usage of mobile code technologies. The security policy should allow, at a minimum, the following actions for each mobile code technology used on the network device:

(1) Control execution of mobile code
(2) Control which users (human, software process, or device) are allowed to transfer mobile code from the network device
(3) Control the code execution based upon integrity checks on mobile code and prior to the code being executed

2. The network device should provide the capability to enforce a security policy that allows the device to control execution of mobile code based on the results of an authenticity check prior to the code being executed.

3. Requirements for SLs

(1) SL 1 : **1203. 1**
(2) SL 2 : **1203. 2**
(3) SL 3 : **1203. 2**
(4) SL 4 : **1203. 2**

504. Use of physical diagnostic and test interfaces

1. Network devices should protect against unauthorized use of the physical factory diagnostic and test interface(s).

2. Network devices should provide active monitoring of the device's diagnostic and test interface(s) and generate an audit log entry when attempts to access these interface(s) are detected.

3. Requirements for SLs

(1) SL 1 : Not applicable
(2) SL 2 : **1204. 1**
(3) SL 3 : **1204. 2**
(4) SL 4 : **1204. 2**

505. Protection from malicious code

1. The network device should provide for protection from malicious code.

2. Requirements for SLs

(1) SL 1 : **1205. 1**
(2) SL 2 : **1205. 1**
(3) SL 3 : **1205. 1**
(4) SL 4 : **1205. 1**

506. Support for updates

1. Network devices should support the ability to be updated and upgraded.

2. Network devices should validate the authenticity and integrity of any software update or upgrade prior to installation.

3. Requirements for SLs

(1) SL 1 : **1206. 1**
(2) SL 2 : **1206. 2**
(3) SL 3 : **1206. 2**
(4) SL 4 : **1206. 2**

507. Physical tamper resistance and detection

1. Network devices should provide tamper resistance and detection mechanisms to protect against unauthorized physical access into the device.

2. Network devices should be capable of automatically providing notification to a configurable set of recipients upon discovery of an attempt to make an unauthorized physical access. All notifications of tampering should be logged as part of the overall audit logging function.

3. Requirements for SLs

(1) SL 1 : Not applicable
(2) SL 2 : **1207. 1**
(3) SL 3 : **1207. 2**
(4) SL 4 : **1207. 2**

508. Provisioning product supplier roots of trust

1. Network devices should provide the capability to provision and protect the confidentiality, integrity, and authenticity of product supplier keys and data to be used as one or more “roots of trust” at the time of manufacture of the device.

2. Requirements for SLs

(1) SL 1 : Not applicable
(2) SL 2 : **1208. 1**
(3) SL 3 : **1208. 1**
(4) SL 4 : **1208. 1**

509. Provisioning asset owner roots of trust

1. Network devices should provide the capability to provision and protect the confidentiality, integrity, and authenticity of asset owner keys and data to be used as “roots of trust” and support the capability to provision without reliance on components that may be outside of the device’s security zone.

2. Requirements for SLs

(1) SL 1 : Not applicable
(2) SL 2 : **1209. 1**
(3) SL 3 : **1209. 1**
(4) SL 4 : **1209. 1**

510. Integrity of the boot process

1. Network devices should verify the integrity of the firmware, software, and configuration data needed for component's boot process prior to it being used in the boot process.

2. Network devices should use the component's product supplier roots of trust to verity the authenticity of the firmware, software, and configuration data needed for component's boot process prior to it being used in the boot process.

3. Requirements for SLs

(1) SL 1 : **1210. 1**
(2) SL 2 : **1210. 2**
(3) SL 3 : **1210. 2**
(4) SL 4 : **1210. 2**

511. Zone boundary protection

1. A network device at a zone boundary should provide the capability to monitor and control communications at zone boundaries to enforce the compartmentalization defined in the risk-based zones and conduits model.

2. The network component should provide the capability to deny network traffic by default and allow network traffic by exception.

3. The network component should provide the capability to protect against any communication through the system boundary (also termed island mode).

4. The network component should provide the capability to protect against any communication through the system boundary when there is an operational failure of the boundary protection mechanisms (also termed fail-close).

5. Requirements for SLs

(1) SL 1 : **1211. 1**
(2) SL 2 : **1211. 2**
(3) SL 3 : **1211. 4**
(4) SL 4 : **1211. 4**

512. General purpose, person-to-person communication restrictions

1. A network device at a zone boundary should provide the capability to protect against general purpose, person-to-person messages from being received from users or systems external to the system.

2. Requirements for SLs

(1) SL 1 : **1212. 1**
(2) SL 2 : **1212. 1**
(3) SL 3 : **1212. 1**
(4) SL 4 : **1212. 1** ⚓

ANNEX 1 MAPPING THE REQUIREMENTS TO SECURITY LEVEL *(2023)*

1. Common requirements for equipment cyber security

Table 4 SLs for Identification and authentication

Requirements	SL 1	SL 2	SL 3	SL 4	Reference
201. Human user identification and authentication					
201.1	O	O	O	O	IEC 62443 4-2 CR 1.1
201.2	X	O	O	O	IEC 62443 4-2 CR 1.1 RE 1
201.3	X	X	O	O	IEC 62443 4-2 CR 1.1 RE 2
202. Software process and device identification and authentication					
202.1	X	O	O	O	IEC 62443 4-2 CR 1.2
202.2	X	X	O	O	IEC 62443 4-2 CR 1.2 RE 1
203. Account management					
203.1	O	O	O	O	IEC 62443 4-2 CR 1.3
204. Identifier management					
204.1	O	O	O	O	IEC 62443 4-2 CR 1.4
205. Authenticator management					
205.1	O	O	O	O	IEC 62443 4-2 CR 1.5
205.2	X	X	O	O	IEC 62443 4-2 CR 1.5 RE 1
206. Strength of password-based authentication					
206.1	O	O	O	O	IEC 62443 4-2 CR 1.7
206.2	O	O	O	O	IEC 62443 4-2 CR 1.7
206.3	X	X	O	O	IEC 62443 4-2 CR 1.7 RE 1
206.4	X	X	X	O	IEC 62443 4-2 CR 1.7 RE 2
207. Public key infrastructure certificates					
207.1	X	O	O	O	IEC 62443 4-2 CR 1.8
208. Strength of public key authentication					
208.1	X	O	O	O	IEC 62443 4-2 CR 1.9
208.2	X	X	O	O	IEC 62443 4-2 CR 1.9 RE 1
209. Authenticator feedback					
209.1	O	O	O	O	IEC 62443 4-2 CR 1.10
210. Unsuccessful login attempts					
210.1	O	O	O	O	IEC 62443 4-2 CR 1.11
211. System use notification					
211.1	O	O	O	O	IEC 62443 4-2 CR 1.12
212. Strength of symmetric key authentication					
212.1	X	O	O	O	IEC 62443 4-2 CR 1.14

Table 5 SLs for Use control

Requirements	SL 1	SL 2	SL 3	SL 4	Reference
301. Authorization enforcement					
301.1	O	O	O	O	IEC 62443 4-2 CR 2.1
301.2	X	O	O	O	IEC 62443 4-2 CR 2.1 RE 1
301.3	X	O	O	O	IEC 62443 4-2 CR 2.1 RE 2
301.4	X	X	O	O	IEC 62443 4-2 CR 2.1 RE 3
301.5	X	X	X	O	IEC 62443 4-2 CR 2.1 RE 4
302. Wireless use control					
302.1	O	O	O	O	IEC 62443 4-2 CR 2.2
303. Session lock					
203.1	O	O	O	O	IEC 62443 4-2 CR 2.5
304. Remote session termination					
304.1	O	O	O	O	IEC 62443 4-2 CR 2.6
305. Concurrent session control					
305.1	X	X	O	O	IEC 62443 4-2 CR 2.7
306. Auditable events					
306.1	O	O	O	O	IEC 62443 4-2 CR 2.8
306.2	O	O	O	O	IEC 62443 4-2 CR 2.8
307. Audit storage capacity					
307.1	O	O	O	O	IEC 62443 4-2 CR 2.9
307.2	X	X	O	O	IEC 62443 4-2 CR 2.9 RE 1
308. Response to audit processing failures					
308.1	O	O	O	O	IEC 62443 4-2 CR 2.10
309. Timestamps					
309.1	O	O	O	O	IEC 62443 4-2 CR 2.11
309.2	X	O	O	O	IEC 62443 4-2 CR 2.11 RE 1
309.3	X	X	X	O	IEC 62443 4-2 CR 2.11 RE 2
310. Non-repudiation					
310.1	O	O	O	O	IEC 62443 4-2 CR 2.12
310.2	X	X	X	O	IEC 62443 4-2 CR 2.12 RE 1
311. Use control for portable and mobile devices					
311.1	O	O	O	O	IEC 62443 3-3 SR 2.3

Table 6 SLs for System integrity

Requirements	SL 1	SL 2	SL 3	SL 4	Reference
401. Communication integrity					
401.1	O	O	O	O	IEC 62443 4-2 CR 3.1
401.2	X	O	O	O	IEC 62443 4-2 CR 3.1 RE 1
402. Security functionality verification					
402.1	O	O	O	O	IEC 62443 4-2 CR 3.3
402.2	X	X	X	O	IEC 62443 4-2 CR 3.3 RE 1
403. Software and information integrity					
403.1	O	O	O	O	IEC 62443 4-2 CR 3.4
403.2	X	O	O	O	IEC 62443 4-2 CR 3.4 RE 1
403.3	X	X	O	O	IEC 62443 4-2 CR 3.4 RE 2
404. Input validation					
404.1	O	O	O	O	IEC 62443 4-2 CR 3.5
405. Deterministic output					
405.1	O	O	O	O	IEC 62443 4-2 CR 3.6
406. Error handling					
406.1	X	O	O	O	IEC 62443 4-2 CR 3.7
407. Session integrity					
407.1	X	O	O	O	IEC 62443 4-2 CR 3.8
408. Protection of audit information					
408.1	X	O	O	O	IEC 62443 4-2 CR 3.9
408.2	X	X	X	O	IEC 62443 4-2 CR 3.9 RE 1

Table 7 Data confidentiality

Requirements	SL 1	SL 2	SL 3	SL 4	Reference
501. Information confidentiality					
501.1	O	O	O	O	IEC 62443 4-2 CR 4.1
502. Information persistence					
502.1	X	O	O	O	IEC 62443 4-2 CR 4.2
502.2	X	X	O	O	IEC 62443 4-2 CR 4.2 RE 1
502.3	X	X	O	O	IEC 62443 4-2 CR 4.2 RE 2
503. Use of cryptography					
503.1	O	O	O	O	IEC 62443 4-2 CR 4.3

Table 8 Restricted data flow

Requirements	SL 1	SL 2	SL 3	SL 4	Reference
601. Network segmentation					
601.1	O	O	O	O	IEC 62443 4-2 CR 5.1

Table 9 Timely response to events

Requirements	SL 1	SL 2	SL 3	SL 4	Reference
701. Audit log accessibility					
701.1	O	O	O	O	IEC 62443 4-2 CR 6.1
701.2	X	X	O	O	IEC 62443 4-2 CR 6.1 RE 1
702. Continuous monitoring					
702.1	X	O	O	O	IEC 62443 4-2 CR 6.2

Table 10 Resource availability

Requirements	SL 1	SL 2	SL 3	SL 4	Reference
801. Denial of service protection					
801.1	O	O	O	O	IEC 62443 4-2 CR 7.1
801.2	X	O	O	O	IEC 62443 4-2 CR 7.1 RE 1
802. Resource management					
802.1	O	O	O	O	IEC 62443 4-2 CR 7.2
803. Control system backup					
803.1	O	O	O	O	IEC 62443 4-2 CR 7.3
803.2	X	O	O	O	IEC 62443 4-2 CR 7.3 RE 1
804. Control system recovery and reconstitution					
804.1	O	O	O	O	IEC 62443 4-2 CR 7.4
805. Network and security configuration settings					
805.1	O	O	O	O	IEC 62443 4-2 CR 7.6
805.2	X	X	O	O	IEC 62443 4-2 CR 7.6 RE 1
806. Least functionality					
806.1	O	O	O	O	IEC 62443 4-2 CR 7.7
807. Control system component inventory					
807.1	X	O	O	O	IEC 62443 4-2 CR 7.8

2. Additional requirements for equipment cyber security

Table 11 SLs for Application requirements

Requirements	SL 1	SL 2	SL 3	SL 4	Reference
201. Mobile code					
201.1	O	O	O	O	IEC 62443 4-2 SAR 2.4
201.2	X	O	O	O	IEC 62443 4-2 SAR 2.4 RE 1
202. Protection from malicious code					
202.1	O	O	O	O	IEC 62443 4-2 SAR 3.2

Table 12 SLs for Embeded device

Requirements	SL 1	SL 2	SL 3	SL 4	Reference
301. Mobile code					
301.1	O	O	O	O	IEC 62443 4-2 EDR 2.4
301.2	X	O	O	O	IEC 62443 4-2 EDR 2.4 RE 1
302. Use of physical diagnostic and test interfaces					
302.1	X	O	O	O	IEC 62443 4-2 EDR 2.13
302.2	X	X	O	O	IEC 62443 4-2 EDR 2.13 RE 1
303. Protection from malicious code					
303.1	X	O	O	O	IEC 62443 4-2 EDR 3.2
304. Support for updates					
304.1	O	O	O	O	IEC 62443 4-2 EDR 3.10
304.2	X	O	O	O	IEC 62443 4-2 EDR 3.10 RE 1
305. Physical tamper resistance and detection					
305.1	X	O	O	O	IEC 62443 4-2 EDR 3.11
305.2	X	X	O	O	IEC 62443 4-2 EDR 3.11 RE 1
306. Provisioning product supplier roots of trust					
306.1	X	O	O	O	IEC 62443 4-2 EDR 3.12
307. Provisioning asset owner roots of trust					
307.1	X	O	O	O	IEC 62443 4-2 EDR 3.13
308. Integrity of the boot process					
308.1	O	O	O	O	IEC 62443 4-2 EDR 3.14
308.2	X	O	O	O	IEC 62443 4-2 EDR 3.14 RE 1

Table 13 SLs for Host device

Requirements	SL 1	SL 2	SL 3	SL 4	Reference
401. Mobile code					
401.1	O	O	O	O	IEC 62443 4-2 HDR 2.4
401.2	X	O	O	O	IEC 62443 4-2 HDR 2.4 RE 1
402. Use of physical diagnostic and test interfaces					
402.1	X	O	O	O	IEC 62443 4-2 HDR 2.13
402.2	X	X	O	O	IEC 62443 4-2 HDR 2.13 RE 1
403. Protection from malicious code					
403.1	O	O	O	O	IEC 62443 4-2 HDR 3.2
403.2	X	O	O	O	IEC 62443 4-2 HDR 3.2 RE 1
404. Support for updates					
404.1	O	O	O	O	IEC 62443 4-2 HDR 3.10
404.2	X	O	O	O	IEC 62443 4-2 HDR 3.10 RE 1
405. Physical tamper resistance and detection					
405.1	X	O	O	O	IEC 62443 4-2 HDR 3.11
405.2	X	X	O	O	IEC 62443 4-2 HDR 3.11 RE 1
406. Provisioning product supplier roots of trust					
406.1	X	O	O	O	IEC 62443 4-2 HDR 3.12
407. Provisioning asset owner roots of trust					
407.1	X	O	O	O	IEC 62443 4-2 HDR 3.13
408. Integrity of the boot process					
408.1	O	O	O	O	IEC 62443 4-2 HDR 3.14
408.2	X	O	O	O	IEC 62443 4-2 HDR 3.14 RE 1

Table 14 SLs for Network device

Requirements	SL 1	SL 2	SL 3	SL 4	Reference
501. Wireless access management					
501.1	O	O	O	O	IEC 62443 4-2 NDR 1.6
501.2	X	O	O	O	IEC 62443 4-2 NDR 1.6 RE 1
502. Access via untrusted networks					
502.1	O	O	O	O	IEC 62443 4-2 NDR 1.13
502.2	X	X	O	O	IEC 62443 4-2 NDR 1.13 RE 1
503. Mobile code					
503.1	O	O	O	O	IEC 62443 4-2 NDR 2.4
503.2	X	O	O	O	IEC 62443 4-2 NDR 2.4 RE 1
504. Use of physical diagnostic and test interfaces					
504.1	X	O	O	O	IEC 62443 4-2 NDR 2.13
504.2	X	X	O	O	IEC 62443 4-2 NDR 2.13 RE 1
505. Protection from malicious code					
505.1	O	O	O	O	IEC 62443 4-2 NDR 3.2
506. Support for updates					
506.1	O	O	O	O	IEC 62443 4-2 NDR 3.10
506.2	X	O	O	O	IEC 62443 4-2 NDR 3.10 RE 1
507. Physical tamper resistance and detection					
507.1	X	O	O	O	IEC 62443 4-2 NDR 3.11
507.2	X	X	O	O	IEC 62443 4-2 NDR 3.11 RE 1
508. Provisioning product supplier roots of trust					
508.1	X	O	O	O	IEC 62443 4-2 NDR 3.12
509. Provisioning asset owner roots of trust					
509.1	X	O	O	O	IEC 62443 4-2 NDR 3.13
510. Integrity of the boot process					
510.1	O	O	O	O	IEC 62443 4-2 NDR 3.14
510.2	X	O	O	O	IEC 62443 4-2 NDR 3.14 RE 1
511. Zone boundary protection					
511.1	O	O	O	O	IEC 62443 4-2 NDR 5.2
511.2	X	O	O	O	IEC 62443 4-2 NDR 5.2 RE 1
511.3	X	X	X	O	IEC 62443 4-2 NDR 5.2 RE 2
511.4	X	X	X	O	IEC 62443 4-2 NDR 5.2 RE 3
512. General purpose, person-to-person communication restrictions					
512.1	O	O	O	O	IEC 62443 4-2 NDR 5.3

GUIDANCE FOR CONFORMITY CERTIFICATION OF MARITIME EQUIPMENT CYBER SECURITY

Published by
KR
36, Myeongji ocean city 9-ro, Gangseo-gu,
BUSAN, KOREA
TEL : +82 70 8799 7114
FAX : +82 70 8799 8999
Website : http://www.krs.co.kr