E27 (Apr 2022) Cyber resilience of on-board systems and equipment

1. General

1.1 Introduction

Technological evolution of vessels, ports, container terminals, etc. and increased reliance upon Operational Technology (OT) and Information Technology (IT) has created an increased possibility of cyber-attacks to affect business, personnel data, human safety, the safety of the ship, and also possibly threaten the marine environment. Safeguarding shipping from current and emerging threats must involve a range of controls that are continually evolving which would require incorporating security features in the equipment and systems at design and manufacturing stage. It is therefore necessary to establish a common set of minimum requirements to deliver systems and equipment that can be described as cyber resilient.

This document specifies unified requirements for cyber resilience of on-board systems and equipment.

1.2 Limitations

This UR does not cover environmental performance for the system hardware and the functionality of the software. In addition to this UR, following URs shall be applied:

- UR E10 for environmental performance for the system hardware
- UR E22 for safety of equipment for the functionality of the software

1.3 Scope

The requirements specified in this UR are applicable to computer based systems as defined in UR E26.

Navigation and radiocommunication systems may follow IEC 61162-460 instead of the requirements in this UR. See IACS UR E26 section 1.3

Note:

1. This Unified Requirement is to be uniformly implemented by IACS Societies on ships contracted for construction on or after 1 January 2024 and may be used for other ships as non-mandatory guidance. In order to allow sufficient time for non-mandatory pilot application of this UR, the application date of 1 January 2024 has been selected.

2. The “contracted for construction” date means the date on which the contract to build the vessel is signed between the prospective owner and the shipbuilder. For further details regarding the date of “contract for construction”, refer to IACS Procedural Requirement (PR) No. 29.

E27 (cont)

1.3.1 Information and Communication Technology (ICT)

Attention is made to additional IACS documents on Computer Based Systems and Cyber Resilience as follows:

IACS UR E22 “On board Use and Application of Computer based systems” includes requirements for design, construction, commissioning and maintenance of computer-based systems where they depend on software for the proper achievement of their functions. The requirements in E22 focus on the functionality of the software and on the hardware supporting the software which provide control, alarm, monitoring, safety or internal communication functions subject to classification requirements.

IACS UR E26 “Cyber resilience of Ships” includes requirements for cyber resilience of ships, with the purpose of providing technical means to stakeholders which would lead to cyber resilient ships.

IACS Recommendation 166 on Cyber Resilience: non-mandatory recommended technical requirements that stakeholders may reference and apply to assist with the delivery of cyber resilient ships, whose resilience can be maintained throughout their service life.

1.4 Definitions & Abbreviations

Attack surface: The set of all possible points where an unauthorized user can access a system and extract data. The attack surface comprises two categories: digital and physical. The digital attack surface encompasses all the hardware and software that connect to an organization’s network. These include applications, code, ports, servers and websites. The physical attack surface comprises all endpoint devices that an attacker can gain physical access to, such as desktop computers, hard drives, laptops, mobile phones, removable drives and carelessly discarded hardware.

Authentication: Provision of assurance that a claimed characteristic of an identity is correct.

Compensating countermeasure: An alternate solution to a countermeasure employed in lieu of or in addition to inherent security capabilities to satisfy one or more security requirements.

Computer Based System (CBS):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.

Computer Network: A group of two or more computer systems linked together.

Control: Means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be administrative, technical, management, or legal in nature.

Cyberattack: Any type of offensive cyber manoeuvre that targets IT and OT systems, computer networks, and/or personal computer devices and attempts to compromise, destroy or access company and ship systems and data.

E27 (cont)

Cyber incident: An event resulting from any offensive cyber manoeuvre, either intentional or unintentional, that targets or affects one or more CBS onboard, which actually or potentially results in adverse consequences to an onboard system, network and computer or the information that they process, store or transmit, and which may require a response action to mitigate the consequences. Cyber incidents include unauthorized access, misuse, modification, destruction or improper disclosure of the information generated, archived or used in onboard CBS or transported in the networks connecting such systems. Cyber incidents do not include system failures.

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

Defence in depth: Information Security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization.

Essential Systems: Computer Based System contributing to the provision of services essential for propulsion and steering, and safety of the ship. Essential services comprise "Primary Essential Services" and "Secondary Essential Services": Primary Essential Services are those services which need to be in continuous operation to maintain propulsion and steering; Secondary Essential Services are those services which need not necessarily be in continuous operation to maintain propulsion and steering but which are necessary for maintaining the vessel’s safety.

Firewall: A logical or physical barrier that monitors and controls incoming and outgoing network traffic controlled via predefined rules.

Firmware: 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.

Hardening: Hardening is the practice of reducing a system's vulnerability by reducing its attack surface.

Information Technology (IT): Devices, software and associated networking focusing on the use of data as information, as opposed to Operational Technology (OT).

Integrated system: System combining a number of interacting sub-system and/or equipment organized to achieve one or more specified purposes.

Network switch (Switch): A device that connects devices together on a computer network, by using packet switching to receive, process and forward data to the destination device.

Offensive cyber manoeuvre: Actions that result in denial, degradation, disruption, destruction, or manipulation of OT or IT systems.

Operational technology (OT): Devices, sensors, software and associated networking that monitor and control onboard systems. Operational technology systems may be thought of as focusing on the use of data to control or monitor physical processes.

OT system: Computer based systems, which provide control, alarm, monitoring, safety or internal communication functions**.**

E27
(cont)

Patches: Software designed to update installed software or supporting data to address security vulnerabilities and other bugs or improve operating systems or applications

Protocols: A common set of rules and signals that computers on the network use to communicate. Protocols allow to perform data communication, network management and security. Onboard networks usually implement protocols based on TCP/IP stacks or various field buses.

Recovery: Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cyber security event. The Recovery function support s timely return to normal operations to reduce the impact from a cyber security event.

System: Combination of interacting programmable devices and/or sub-systems organized to achieve one or more specified purposes

System Categories (I, II, III): System categories based on their effects on system functionality, which are defined in IACS UR E22.

System Integrator: The specific person or organization responsible for the integration of systems and products provided by suppliers into the system invoked by the requirements in the ship specifications and for providing the integrated system. The system integrator may also be responsible for integration of systems in the ship. This role shall be taken by the Shipyard unless an alternative organization is specifically contracted/assigned this responsibility.

Untrusted network: Any network outside the scope of applicability of this UR.

E27 (cont)

2. Security Philosophy

2.1 Systems and Equipment

2.1.1 A System can consist of group of hardware and software enabling safe, secure and reliable operation of a process. Typical example could be Engine control system, DP system, etc.

2.1.2 An Equipment may be one of the following:

- Network devices (i.e. routers, managed switches)
- Security devices (i.e. firewall, Intrusion Prevention System)
- Computers (i.e. workstation, servers)
- Automation devices (i.e. Programmable Logic Controllers)
- Virtual machine cloud-hosted

2.2 Cyber Resilience

The cyber resilience requirements in section 4 will be applicable for all systems in scope of UR E26 as applicable. Additional requirements related to interface with untrusted networks will only apply for systems where such connectivity is designed.

2.3 Compensating Countermeasures

2.3.1 Compensating countermeasure may be employed in lieu of or in addition to inherent security capabilities to satisfy one or more security requirements.
Compensating countermeasures should follow these principles:

Compensating countermeasure(s) should meet the intent and rigor of the original stated requirement. They should also be “above and beyond” other requirements (not simply in compliance with other requirements).

For type approval of a system, the compensating countermeasure(s) should be implemented in the CBS, i.e., not rely on barriers related to installation on board or operational procedures.

2.4 Essential Systems Availability

2.4.1 Security measures for Essential system shall not adversely affect the systems availability.

2.4.2 Implementation of security measures shall not cause loss of protection, loss of control, loss of view or loss of other essential functions which could result in health, safety and environmental consequences.

2.4.3 The system shall be adequately designed to allow the ship to continue its mission critical operations in a manner that ensures the confidentiality, integrity, and availability of the data necessary for safety of the vessel, its systems, personnel and cargo.

E27 (cont)

3. Documentation

3.1 System Documentation

Following documents shall be submitted to Classification society for review and approval in accordance with the requirements in Section 4:

a) Detailed list of equipment included in the system (see 3.2)

b) For each equipment, the involved hardware shall be detailed (i.e. motherboard, storage, interfaces (network, serial) and any connectivity)

c) A list of the following software including :
- Operating system/firmware
- Network services provided and managed by the operating systems
- Application Software (see 3.3)
- Databases
- Configuration files

d) Network or serial flows (source, destination, protocols, protocols details, physical implementation)

e) Network security equipment (which are to be considered and detailed as any other equipment). E.g. traffic management (firewalls, routers, etc) and packet management (IDS, etc)

f) Secure Development Lifecycle Document (see Section 5).

g) Plans for maintenance of system

h) Recovery Plan

i) System Test Plan

j) Description of how the system meets the applicable requirements in E27 (i.e. Operation Manual or User Manual, etc.)

k) Change Management Plan

3.2 Inventories

3.2.1 The following details shall be documented:

a) Name

b) Brand/Manufacturer (supplier)

c) Model or reference, some devices contain several references

d) Current Version of the operating system and embedded firmware (software version)and date implemented

E27
(cont)

3.3 Software Inventory

For software, the inventory shall contain at least the following information, for each software application program, operating system, firmware etc.:

a) The CBS where it is installed, a short description of its purpose with brief functional description and technical features (brand, manufacturer, model, main technical data);

b) Version information, license information with expiration dates and a log of updates;

c) Maintenance policy (e.g. on-site vs. remote, periodic vs. occasional, etc.) and responsible persons;

d) Access control policy (e.g. read, write and execution rights)with roles and responsibilities

E27
(cont)

4 System Requirements

This section specifies the required security capabilities for CBSs in the scope specified in section 1.3.

4.1 Required security capabilities

The following security capabilities are required for all CBSs in the scope specified in section 1.3.

Table 1

Sl No	Objective	Requirements
1	Human user identification and authentication	The CBS shall identify and authenticate all human users who can access the system directly or through interfaces (IEC 62443-3-3/SR 1.1)
2	Account management	The CBS shall provide the capability to support the management of all accounts by authorized users, including adding, activating, modifying, disabling and removing account (IEC 62443-3-3/SR 1.3)
3	Identifier management	The CBS shall provide the capability to support the management of identifiers by user, group and role. (IEC 62443-3-3/SR 1.4)
4	Authenticator management	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. (IEC 62443-3-3/SR 1.5)
5	Wireless access management	The CBS shall provide the capability to identify and authenticate all users (humans, software processes or devices) engaged in wireless communication (IEC 62443-3-3/SR 1.6)
6	Strength of password-based authentication	The CBS shall provide the capability to enforce configurable password strength based on minimum length and variety of character types. (IEC 62443-3-3/SR 1.7)
7	Authenticator feedback	The CBS shall obscure feedback during the authentication process. (IEC 62443-3-3/SR 1.10)
8	Authorization enforcement	On all interfaces, human users shall be assigned authorizations in accordance with the principles of segregation of duties and least privilege. (IEC 62443-3-3/SR 2.1)
9	Wireless use control	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 (IEC 62443-3-3/SR 2.2)
10	Use control for portable and mobile devices	When the CBS supports use of portable and mobile devices, the system shall include the capability to

E27
(cont)

		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 (IEC 62443-3-3/SR 2.3)
11	Mobile code	The CBS shall control the use of mobile code such as java scripts, ActiveX and PDF. (IEC 62443-3-3/SR 2.4)
12	Session lock	The CBS shall be able to prevent further access after a configurable time of inactivity or following activation of manual session lock. (IEC 62443-3-3/SR 2.5)
13	Auditable events	The CBS shall generate audit records relevant to security for at least the following events: access control, operating system events, backup and restore events, configuration changes, loss of communication. (IEC 62443-3-3/SR 2.8)
14	Audit storage capacity	The CBS shall provide the capability to allocate audit record storage capacity according to commonly recognized recommendations for log management. Auditing mechanisms shall be implemented to reduce the likelihood of such capacity being exceeded. (IEC 62443-3-3/SR 2.9)
15	Response to audit processing failures	The CBS shall provide the capability to prevent loss of essential services and functions in the event of an audit processing failure. (IEC 62443-3-3/SR 2.10)
16	Timestamps	The CBS shall timestamp audit records. (IEC 62443-3-3/SR 2.11)
17	Communication integrity	The CBS shall protect the integrity of transmitted information. Note: Cryptographic mechanisms shall be employed for wireless networks. (IEC 62443-3-3/SR 3.1)
18	Malicious code protection	The CBS shall provide capability to implement suitable protection measures to prevent, detect and mitigate the effects due to malicious code or unauthorized software. It shall have the feature for updating the protection mechanisms (IEC 62443-3-3/SR 3.2)
19	Security functionality verification	The CBS shall provide the capability to support verification of the intended operation of security functions and report when anomalies occur during maintenance (IEC 62443-3-3/SR 3.3)
20	Input validation	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. (IEC 62443-3-3/SR 3.5)
21	Deterministic output	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

E27
(cont)

		– Last-known value – Fixed value (IEC 62443-3-3/SR 3.6)
22	Information confidentiality	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. (IEC 62443-3-3/SR 4.1)
23	Use of cryptography	If cryptography is used, the CBS shall use cryptographic algorithms, key sizes and mechanisms according to commonly accepted security industry practices and recommendations. (IEC 62443-3-3/SR 4.3)
24	Audit log accessibility	The CBS shall provide the capability for accessing audit logs on read only basis by authorized humans and/or tools. (IEC 62443-3-3/SR 6.1)
25	Denial of service protection	The CBS shall provide the minimum capability to maintain essential functions during DoS events. (IEC 62443-3-3/SR 7.1)
26	Resource management	The CBS shall provide the capability to limit the use of resources by security functions to prevent resource exhaustion. (IEC 62443-3-3/SR 7.2)
27	System backup	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 (IEC 62443-3-3/SR 7.3)
28	System recovery and reconstitution	The CBS shall provide the capability to be recovered and reconstituted to a known secure state after a disruption or failure. (IEC 62443-3-3/SR 7.4)
29	Emergency power	The control system shall provide the capability to switch to and from an emergency power supply without affecting the existing security state or a documented degraded mode. (IEC 62443-3-3/SR 7.5)
30	Network and security configuration settings	The CBS traffic shall provide the capability to be configured according to recommended network and security configurations as described in guidelines provided by the control system supplier. The CBS shall provide an interface to the currently deployed network and security configuration settings. (IEC 62443-3-3/SR 7.6)
31	Least Functionality	The installation, the availability and the access rights of the following shall be limited to the strict needs of the functions provided by the system: - operating systems software components, processes and services - network services, ports, protocols, routes and hosts accesses and any software (IEC 62443-3-3/SR 7.7)

E27 (cont)

4.2 Additional security capabilities

The following additional security capabilities are required for CBSs with network communication to untrusted networks (i.e. interface to any networks outside the scope of UR E26).

Table 2

Sl No	Objective	Requirements
32	Multifactor authentication for human users	Multifactor authentication is required for human users when accessing the CBS from or via an untrusted network. (IEC 62443-3-3/SR 1.1, RE 2)
33	Software process and device identification and authentication	The system shall identify and authenticate software processes and devices (IEC 62443-3-3/SR 1.2)
34	Unsuccessful login attempts	The CBS shall enforce a limit of consecutive invalid login attempts from untrusted networks during a specified time period. (IEC 62443-3-3/SR 1.11)
35	System use notification	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. (IEC 62443-3-3/SR 1.12)
36	Access via Untrusted Networks	Any access to the CBS from or via untrusted networks shall be monitored and controlled. (IEC 62443-3-3/SR 1.13)
37	Explicit access request approval	The CBS shall deny access from or via untrusted networks unless explicitly approved by authorized personnel on board. (IEC 62443-3-3/SR 1.13, RE1)
38	Remote session termination	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. (IEC 62443-3-3/SR 2.6)
39	Cryptographic integrity protection	The CBS shall employ cryptographic mechanisms to recognize changes to information during communication with or via untrusted networks. (IEC 62443-3-3/SR 3.1, RE1)
40	Session integrity	The CBS shall protect the integrity of sessions. Invalid session IDs shall be rejected. (IEC 62443-3-3/SR 3.8)
41	Invalidation of session IDs after session termination	The system shall invalidate session IDs upon user logout or other session termination (including browser sessions). (IEC 62443-3-3/SR 3.8, RE1)

E27
(cont)

5 Product Design and Development Requirements

A Secure Development Lifecycle (SDLC) broadly addressing security aspects in following stages shall be followed for the development of systems or equipment

- Requirement analysis phase
- Design phase
- Implementation phase
- Verification phase
- Release phase
- Maintenance Phase
- End of life phase

A document, shall be produced that records how the security aspects have been addressed in above phases and shall at minimum integrate controlled processes as set out in below 5.2 to 5.7. The said document is required to be submitted to class for review and approval.

5.1 (IEC 62443-4-1/SM-8) The manufacturer shall have procedural and technical controls in place to protect private keys used for code signing from unauthorized access or modification. The manufacturer shall have QA process to test the updates before releasing

5.2 (IEC 62443-4-1/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:

a) The product version number(s) to which the security patch applies;

b) Instructions on how to apply approved patches manually and via an automated process;

c) Description of any impacts that applying the patch to the product can have, including reboot;

d) Instructions on how to verify that an approved patch has been applied; and

e) Risks of not applying the patch and mediations that can be used for patches that are not approved or deployed by the asset owner.

5.3 (IEC 62443-4-1/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:

a) Stating whether the product is compatible with the dependent component or operating system security update;

5.4 (IEC 62443-4-1/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 patch is authentic

5.5 (IEC 62443-4-1/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:

E27 (cont)

a) Security capabilities implemented by the product and their role in the defence in depth strategy;

b) Threats addressed by the defence in depth strategy; and

c) Product user mitigation strategies for known security risks associated with the product, including risks associated with legacy code.

5.6 (IEC 62443-4-1/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.

5.7 (IEC 62443-4-1/SG-3) A process shall be employed to create product user documentation that includes guidelines for hardening the product when installing and maintaining the product. The guidelines shall include, but are not limited to, instructions, rationale and recommendations for the following:

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

b) Integration of the product's application programming interfaces/protocols with user applications;

c) Applying and maintaining the product's defence in depth strategy

d) Configuration and use of security options/capabilities in support of local security policies, and for each security option/capability:

   i. its contribution to the product's defence in depth strategy

   ii. descriptions of configurable and default values that include how each affects security along with any potential impact each has on work practices; and

   iii. setting/changing/deleting its value;

e) 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;

f) Instructions and recommendations for periodic security maintenance activities;

g) Instructions for reporting security incidents for the product to the product supplier;

h) Description of the security best practices for maintenance and administration of the product.

E27
(cont)

Annex I

Requirements:

I. IACS UR E10: Test Specification for Type Approval

II. IACS UR E22: On board use and application of computer based systems

III. IACS UR E26: Cyber Resilience of Ships

Credits:

I. IACS Rec 166 (Corr.1 2020): Recommendation on Cyber Resilience

II. IEC 62443-3-3 (2013): Industrial communication networks – Network and system security. Part 3-3: System security requirements and security levels

III. IEC 62443-4-1 (2018): Security for industrial automation and control systems Part 4-1: Secure product development lifecycle requirements

IV. Implementing The CIRM Cyber Risk Code Of Practice For Vendors Of Marine Electronic Equipment And Services- GL-002

End of Document