E27 Cyber resilience of on-board systems and equipment

(Apr 2022 Withdrawn) (Rev.1 Sep 2023)

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

---

Note:

1. The Unified Requirement published in April 2022 was withdrawn before coming into force on 1 January 2024

2. Rev.1 to this UR is to be uniformly implemented by IACS Societies on ships contracted for construction on or after 1 July 2024 and may be used for other ships as non-mandatory guidance.

3. 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 Scope of applicability

The requirements specified in this UR are applicable to computer based systems specified in UR E26 for the following types of vessels:

Mandatory requirements for

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

Non-mandatory guidance to

a) Ships of war and troopships
b) Cargo ships less than 500 gross tonnage
c) Vessels not propelled by mechanical means
d) Wooden ships of primitive build
e) Passenger yachts (passengers not more than 12).
f) Pleasure yachts not engaged in trade
g) Fishing vessels
h) Site specific offshore installations (i.e. FPSOs, FSUs, etc)

For navigation and radiocommunication systems, the application of IEC 61162-460 or other equivalent standards in lieu of the required security capabilities in UR E27 section 4 may be accepted by the Society, on the condition that requirements in IACS UR E26 are complied with.

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 “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.

E27
(cont)

1.4 Definitions & Abbreviations

Attack surface: The set of all possible points where an unauthorized user can access a system, cause an effect on or extract data from. 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 connection between two or more computers for the purpose of communicating data electronically by means of agreed communication protocols.

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

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

E27 (cont)

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: A system combining a number of interacting sub-systems 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**.**

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.

Supplier: A manufacturer or provider of hardware and/or software products, system components or equipment (hardware or software) comprising of the application, embedded devices, network devices, host devices etc. working together as system or a subsystem. The Supplier is responsible for providing programmable devices, sub-systems or systems to the System Integrator.

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.

E27 (cont)

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. Until vessel delivery, 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.

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 Equipment may be one of the following:

- Network devices (i.e. routers, managed switches)
- Security devices (i.e. firewall, Intrusion Detection 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 Essential Systems Availability

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

2.3.2 Implementation of security measures shall not cause loss of safety functions , loss of control functions, loss of monitoring functions or loss of other functions which could result in health, safety and environmental consequences.

2.3.3 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.

2.4 Compensating Countermeasures

2.4.1 Compensating countermeasure may be employed in lieu of or in addition to inherent security capabilities to satisfy one or more security requirements.

Compensating countermeasure(s) shall meet the intent and rigor of the original stated requirement considering the referenced standards as well as the differences between each

E27 (cont)

requirement and the related items in the standards, and follow the principles specified in section 3.1.3.

3. Documentation

3.1 CBS Documentation

The following documents shall be submitted to Classification society for review and approval in accordance with the requirements in this UR. See also section 6.2.

3.1.1 CBS asset inventory

The CBS asset inventory shall include the information below.

- List of hardware components (e.g., host devices, embedded devices, network devices)Name
- Brand/manufacturer
- Model/type
- Short description of functionality/purpose
- Physical interfaces (e.g., network, serial)
- Name/type of system software (e.g., operating system, firmware)
- Version and patch level of system software
- Supported communication protocols

List of software components (e.g., application software, utility software)

- The hardware component where it is installed
- Brand/manufacturer
- Model/type
- Short description of functionality/purpose
- Version of software

3.1.2 Topology diagrams

The physical topology diagram shall illustrate the physical architecture of the system. It shall be possible to identify the hardware components in the CBS asset inventory. The diagram shall illustrate the following:

- All endpoints and network devices, including identification of redundant units
- Communication cables (networks, serial links), including communication with I/O units
- Communication cables to other networks or systems

The logical topology diagram shall illustrate the data flow between components in the system. The diagram shall illustrate the following:

- Communication endpoints (e.g. workstations, controllers, servers)
- Network devices (switches, routers, firewalls)
- Physical and virtual computers
- Physical and virtual communication paths
- Communication protocols

E27 (cont)

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

3.1.3 Description of security capabilities

This document shall describe how the CBS with its hardware and software components meets the required security capabilities in section 4.1.

Any network interfaces to other CBSs in the scope of applicability of UR E26 shall be described. The description shall include destination CBS, data flows, and communication protocols. If the System integrator has allocated the destination CBS to another security zone, components providing protection of the security zone boundary (see UR E26 section 4.2.2.1) shall be described in detail if delivered as part of the CBS.

Any network interfaces to other systems or networks outside the scope of applicability of UR E26 (untrusted networks) shall be described. The description shall specify compliance with the additional security capabilities in section 4.2, and include relevant procedures or instructions for the crew. Components providing protection of the security zone boundary (see UR E26 section 4.2.2.1) shall be described in detail if delivered as part of the CBS.

A separate chapter shall be designated for each requirement. All hardware and software components in the system shall be addressed in the description, as relevant.

If any requirement is not fully met, this shall be specified in the description, and compensating countermeasures shall be proposed. The compensating countermeasures should:

- Protect against the same threats as the original requirement
- Provide an equal level of protection as the original requirement
- Not be a security control that is required by other requirements in this UR
- Not introduce higher security risk

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

3.1.4 Test procedure of security capabilities

This document shall describe how to demonstrate by testing that the system complies with the requirements in section 4.1 and 4.2, including any compensating countermeasures. Demonstration of compliance by analytic evaluation may be specially considered. The procedure shall include a separate chapter for each applicable requirement and describe:

- Necessary test setup (i.e. to ensure the test can be repeated with the same expected result)
- Test equipment
- Initial condition(s)
- Test methodology, detailed test steps
- Expected results and acceptance criteria

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

E27 (cont)

3.1.5 Security configuration guidelines

This document shall describe recommended configuration settings of the security capabilities and specify default values. The objective is to ensure the security capabilities are implemented in accordance with UR E26 and any specifications by the System integrator (e.g. user accounts, authorisation, password policies, safe state of machinery, firewall rules, etc.)

The document shall serve as basis for verification of item no. 29 in section 4.1.

3.1.6 Secure development lifecycle documents

This documentation shall be submitted to the Society upon request and shall describe the supplier's processes and controls in accordance with requirements for secure development lifecycle in section 5. Software updates and patching shall be described. The document shall prepare the Society for survey as per section 6.3.4.

3.1.7 Plans for maintenance and verification of the CBS

This document shall be submitted to the Society upon request and shall include procedures for security-related maintenance and testing of the system. The document shall include instructions for how the user can verify correct operation of the system's security functions as required by item no.19 in section 4.1.

3.1.8 Information supporting the owner’s incident response and recovery plan

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

- Local independent control (see UR E26 sec. 4.4.2)
- Network isolation (see UR E26 sec. 4.4.3)
- Forensics by use of audit records (see UR E27 sec. 4.1 item no.13)
- Deterministic output (see UR E26 sec. 4.4.4 and UR E27 sec. 4.1 item no. 20)
- Backup (see UR E27 sec. 4.1 item no. 26)
- Restore (see UR E27 sec. 4.1 item no. 27)
- Controlled shutdown, reset, roll-back and restart (see UR E26 sec. 4.5.3)

3.1.9 Management of change plan

This document shall be submitted to the Society upon request. It is expected that this procedure is not specific for cyber security and is also required by UR E22.

3.1.10 Test reports

CBSs with Type approval certificate covering the security capabilities of this UR may be exempted from survey by the Society. However, test reports signed by the supplier shall be submitted to the Society, demonstrating that the supplier has completed design, construction, testing, configuration, and hardening as would otherwise be verified by the Society in survey (section 6.3).

E27
(cont)

4 System Requirements

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

The requirements in this section are based on the selected requirements in IEC 62443-3-3. To determine the full content, rationale and relevant guidance for each requirement, the reader should consult the referenced standard.

4.1 Required security capabilities

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

Table 1

Item No	Objective	Requirements
Protect against casual or coincidental access by unauthenticated entities		
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)
Protect against casual or coincidental misuse		
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)

E27
(cont)

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 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)
Protect the integrity of the CBS against casual or coincidental manipulation		
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)

E27
(cont)

20	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, – Last-known value, or – Fixed value (IEC 62443-3-3/SR 3.6)
Prevent the unauthorized disclosure of information via eavesdropping or casual exposure		
21	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)
22	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)
Monitor the operation of the CBS and respond to incidents		
23	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)
Ensure that the control system operates reliably under normal production conditions		
24	Denial of service protection	The CBS shall provide the minimum capability to maintain essential functions during DoS events. Note: It is acceptable that the CBS may operate in a degraded mode upon DoS events, but it shall not fail in a manner which may cause hazardous situations. Overload-based DoS events should be considered, i.e. where the networks capacity is attempted flooded, and where the resources of a computer is attempted consumed. (IEC 62443-3-3/SR 7.1)
25	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)
26	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)
27	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)
28	Alternative power source	The CBS shall provide the capability to switch to and from an alternative power source without affecting the existing security state or a documented degraded mode. (IEC 62443-3-3/SR 7.5)

E27
(cont)

29	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 supplier. The CBS shall provide an interface to the currently deployed network and security configuration settings. (IEC 62443-3-3/SR 7.6)
30	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 CBS: - 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)

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).

CBSs with communication traversing the boundaries of security zones shall also meet requirements for network segmentation and zone boundary protection in UR E26 section 4.2.1 and 4.2.2.

Table 2

Item No	Objective	Requirements
31	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)
32	Software process and device identification and authentication	The CBS shall identify and authenticate software processes and devices (IEC 62443-3-3/SR 1.2)
33	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)
34	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)
35	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)
36	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)

E27
(cont)

37	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)
38	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)
39	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)
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)

5 Secure Development Lifecycle 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 5.1 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, if applicable, from unauthorized access or modification.

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;

E27 (cont)

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.
IACS supplement: The manufacturer shall have QA process to test the updates before releasing.

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:

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

E27 (cont)

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 supplier;

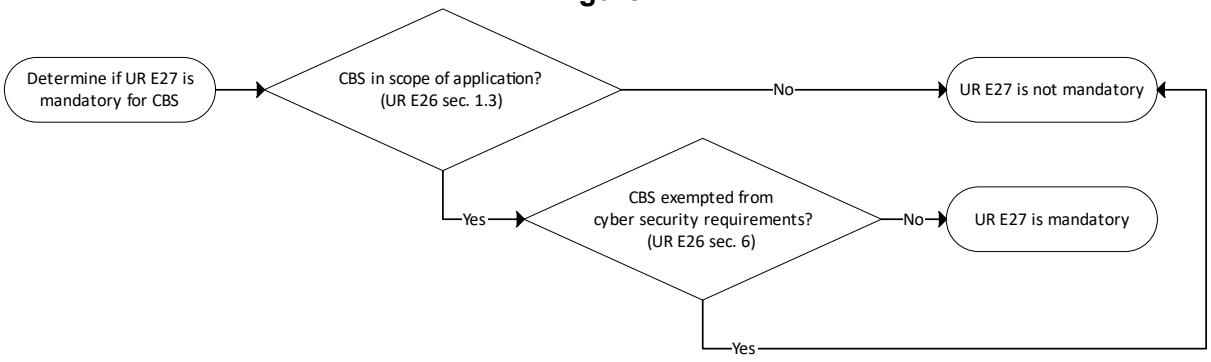
h) Description of the security best practices for maintenance and administration of the product.

6 Demonstration of compliance

6.1 Introduction

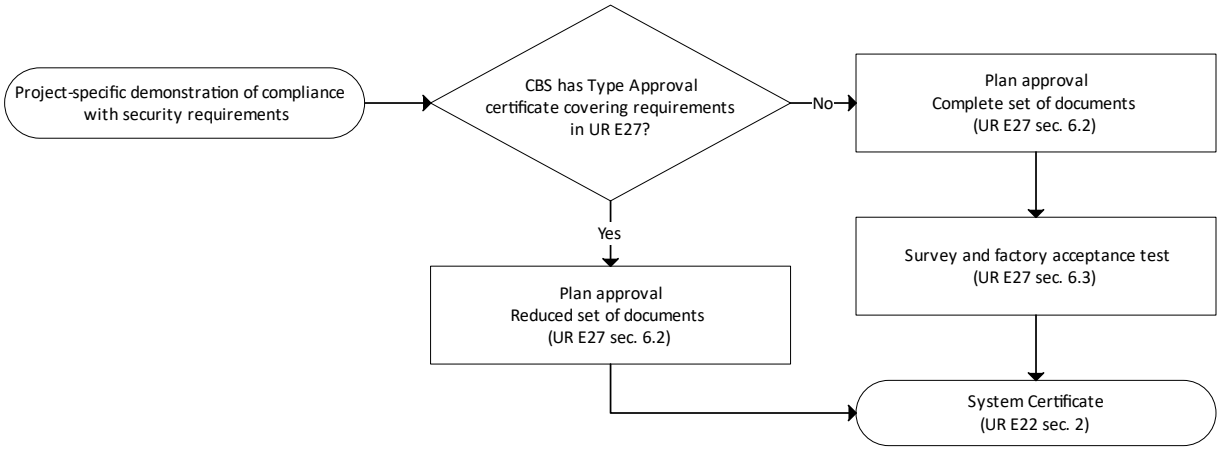
Suppliers shall in cooperation with the System integrator determine if UR E27 is mandatory for the CBS, see Figure 1.

Figure 1



Compliance with security requirements shall be demonstrated as indicated in Figure 2. This classification process is ship-specific and shall result in a System certificate.

Figure 2



E27 (cont)

Type approval is voluntary and applies for CBSs that are standard and routinely manufactured. See UR E22 for definition of System certification and Type approval.

The process in Figure 1 and Figure 2 applies also if other equivalent standards are applied for navigation and radiocommunication equipment (see section 1.3). In such case:

- the process in Figure 1 illustrates if the equivalent standard is mandatory (in lieu of UR E27)
- the process in Figure 2 illustrates that the certification process is lessened if the CBS has been type approved in accordance with the equivalent standard.

6.2 Plan approval

Plan approval is assessment of documents of a CBS intended for a specific vessel. The documents in section 3 are required to be submitted by the supplier. The documents shall enable the Society to verify compliance with requirements in this UR.

If the CBS holds a valid Type approval certificate covering the requirements of this UR, subject to approval by the Society, the supplier may submit a reduced set of vessel-specific documents to the Society (see Appendix II).

The approved version of the documents shall be included in the delivery of the CBS to the system integrator.

6.3 Survey and factory acceptance test

Survey and factory acceptance testing (FAT) is a vessel-specific verification activity required for CBSs that do not hold a valid Type approval certificate covering the requirements of this UR.

The objective of the survey and FAT is to demonstrate by testing and/or analytic evaluation that the CBS complies with applicable requirements in this UR. The survey and FAT shall be carried out at the supplier’s premises or at other works having the adequate apparatus for testing and inspection.

After completed plan approval and survey/FAT, the Society will issue a System certificate that shall accompany the CBS upon delivery to the system integrator.

The following subsections specify the survey and FAT activities.

6.3.1 General survey items

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

It shall also be demonstrated that the system to be delivered is correctly represented by the approved documentation. This shall be done by inspecting the system and comparing the components and arrangement/architecture with the asset inventory (section 3.1.1) and the topology diagrams (section 3.1.2).

E27
(cont)

6.3.2 Test of security capabilities

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

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

6.3.3 Correct configuration of security capabilities

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

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

6.3.4 Secure development lifecycle

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

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

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

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

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

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

The supplier shall present management system documentation substantiating that a process is established in the organization to ensure security updates are informed to the users. The information to the users shall include the items listed in section 5.2.

6.3.4.3 Dependent component security update documentation (IEC 62443-4-1/SUM-3)

The supplier shall present management system documentation, as required by section 5.3, substantiating that a process is established in the organization to ensure users are informed whether the system is compatible with updated versions of acquired software in the system (new versions/patches of operating system or firmware). The information shall address how to manage risks related to not applying the updated acquired software.

E27
(cont)

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

The supplier shall present management system documentation, as required by section 5.4, substantiating that a process is established in the organization ensuring that system security updates are made available to users, and describing how the user may verify the authenticity of the updated software.

6.3.4.5 Product defence in depth (IEC 62443-4-1/SG-1)

The supplier shall present management system documentation, as required by section 5.5, substantiating that a process is established in the organization to document a strategy for defence-in-depth measures to mitigate security threats to software in the CBS during installation, maintenance and operation.

Examples of threats could be installation of unauthorised software, weaknesses in the patching process, tampering with software in the operational phase of the ship.

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

The supplier shall present management system documentation, as required by section 5.6, substantiating that a process is established in the organization to document defence-in-depth measures expected to be provided by the external environment, such as physical arrangement, policies and procedures.

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

The supplier shall present management system documentation, as required by section 5.7, substantiating that a process is established in the organization to ensure that hardening guidelines are produced for the system.

The guidelines shall specify how to reduce vulnerabilities in the system by removal/prohibiting /disabling of unnecessary software, accounts, services, etc.

E27
(cont)

Appendix I

Requirements:

I. IACS UR E10: Test Specification for Type Approval

II. IACS UR E22: 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

E27 (cont)

Appendix II

The following table summarizes documents to be submitted by the supplier to the Society.

Document	Requirements	Class
CBS asset inventory (E27 sec.3.1.1)	To be incorporated in Vessel asset inventory (E26 sec.4.1.1)	Approve [1) 2)]
Topology diagrams (E27 sec.3.1.2)	Enabling System integrator to design security zones and conduits (E26 sec.4.2.1)	Approve [1) 2)]
Description of security capabilities (E27 sec.3.1.3)	Required security capabilities (E27 sec.4.1)	Approve [1)]
	Additional security capabilities, if applicable (E27 sec.4.2)	
Test procedure for security capabilities (E27 sec.3.1.4)	Required security capabilities (E27 sec.4.1)	Approve [1)]
	Additional security capabilities, if applicable (E27 sec.4.2)	
Security configuration guidelines (E27 sec.3.1.5)	Network and security configuration settings (E27 sec.4.1 item 29)	Info [1)]
Secure development lifecycle (E27 sec.3.1.6)	SDLC requirements (E27 sec.5)	Approve [1)]
Plans for maintenance and verification (E27 sec.3.1.7)	Security functionality verification (E27 sec.4.1 item 19)	Info [1)]
Information supporting incident response and recovery plans (E27 sec.3.1.8)	Auditable events (E27 sec.4.1 item 13)	Info [1)]
	Deterministic output (E27 sec.4.1 item 20)	Info [1)]
	System backup (E27 sec.4.1 item 26)	Info [1)]
	System recovery and reconstitution (E27 sec.4.1 item 27)	Info [1)]
Management of change plan (E27 sec.3.1.9)	Management of change process (E22)	Info [1)]
Test reports (E27 sec.3.1.10)	Configuration of security capabilities and hardening (E27 sec.3.1.5 and sec.5.7)	Info [2)]
Note 1: Required for CBS without type approved security capabilities Note 2: Required for CBS with type approved security capabilities		

End of Document