C C S Technical Information

(2024) Technical Information No.1 Total No.633
Jan.25,2024
(Total 1 pages + Annex)

To: Relevant shipowners, ship management companies, shipyards and designers, product manufacturer, related departments of the Headquarters of CCS, the Society's surveyors, Plan Approval Centers

Notice on IACS issuing UR E26(Rev.1) on Cyber Resilience of Ships

1. Background

In Nov, 2023, IACS issued UR E26 (Rev.1) on cyber resilience of ships. This revised UR will be applied to new ships contracted for construction on and after 1 July 2024. And the Unified Requirement published in April 2022 was withdrawn before coming into force on 1 January 2024.

2. Main contents

According to industry feedback, the following content has been revised on the basis of the original UR:

(1) The vessels in scope have been clarified, and the systems in scope have been optimized;
(2) The demonstration of compliance for each specified requirements have been added and summarized in section 5, clarifying the demonstrations and requirements on design, construction, commission and operation;
(3) The acceptance criteria of risk assessment for exclusion of CBS from the application of requirements have been optimized.

This notice is made public on CCS website (www.ccs.org.cn) and is distributed by CCS branches to all relevant stakeholders within their responsible areas. Please feel free to contact Science & Technology Innovation and Test Center of CCS for any inquiry (si@ccs.org.cn).

Annex: IACS UR E26 (Rev.1)

E26
(Apr 2022)
(Rev.1
Nov 2023
Complete
Revision)

Cyber resilience of ships

1. Introduction

Interconnection of computer systems on ships, together with the widespread use onboard of commercial-off-the-shelf (COTS) products, open the possibility for attacks to affect personnel data, human safety, the safety of the ship, and threaten the marine environment.

Attackers may target any combination of people and technology to achieve their aim, wherever there is a network connection or any other interface between onboard systems and the external world. Safeguarding ships, and shipping in general, from current and emerging threats involves a range of measures that are continually evolving.

It is then necessary to establish a common set of minimum functional and performance criteria to deliver a ship that can indeed be described as cyber resilient.

IACS considers that minimum requirements applied consistently to the full threat surface using a goal-based approach is necessary to make cyber resilient ships.

1.1 Structure of this UR

Table 1: Structure of this UR

Introductory Part	1 Introduction
	2 Definitions
	3 Goals and Organization of Requirements
Main Part	4 Requirements 4.1 Identify 4.2 Protect 4.3 Detect 4.4 Respond 4.5 Recover
	5 Demonstration of compliance 5.1 During design and construction phases 5.2 Upon ship commissioning 5.3 During the operational life of the ship
Supplementary Part	6 Risk assessment for exclusion of CBS from the application of requirements (required only when systems are excluded from application of this UR)
	Appendix I: Summary of actions and documents Appendix II: Summary of requirements and documents

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

E26 (cont)

regarding the date of “contract for construction”, refer to IACS Procedural Requirement (PR) No. 29.

1.2 Aim and purpose

The aim of this UR is to provide a minimum set of requirements for cyber resilience of ships, with the purpose of providing technical means to stakeholders which would lead to cyber resilient ships.

This UR targets the ship as a collective entity for cyber resilience and is intended as a base for the complementary application of other URs and industry standards addressing cyber resilience of onboard systems, equipment and components.

Minimum requirements for cyber resilience of on-board systems and equipment are given in IACS UR E27.

1.3 Scope of applicability

1.3.1 Vessels in scope

This UR is applicable to the following vessels:

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

This UR may be used as non-mandatory guidance to the following.

- Ships of war and troopships
- Cargo ships less than 500 GT
- Vessels not propelled by mechanical means
- Wooden ships of primitive build
- Passenger yachts (passengers not more than 12)
- Pleasure yachts not engaged in trade
- Fishing vessels
- Site specific offshore installations (i.e. FPSOs, FSUs, etc.)

E26 (cont)

1.3.2 Systems in scope

This UR applies to:

a) Operational Technology (OT) systems onboard ships, i.e. those CBSs using data to control or monitor physical processes that can be vulnerable to cyber incidents and, if compromised, could lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment.

In particular, the CBSs used for the operation of the following ship functions and systems, if present onboard, shall be considered:

- Propulsion
- Steering
- Anchoring and mooring
- Electrical power generation and distribution
- Fire detection and extinguishing systems
- Bilge and ballast systems, loading computer
- Watertight integrity and flooding detection
- Lighting (e.g. emergency lighting, low locations, navigation lights, etc.)
- Any required safety system whose disruption or functional impairing may pose risks to ship operations (e.g. emergency shutdown system, cargo safety system, pressure vessel safety system, gas detection system, etc.)

In addition, the following systems shall be included in the scope of applicability of this UR:

- Navigational systems required by statutory regulations
- Internal and external communication systems required by class rules and statutory regulations

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 UR E26 are complied with.

b) Any Internet Protocol (IP)-based communication interface from CBSs in scope of this UR to other systems. Examples of such systems are, but not limited to, the following:

- passenger or visitor servicing and management systems
- passenger-facing networks
- administrative networks
- crew welfare systems

E26 (cont)

- any other systems connected to OT systems, either permanently or temporarily (e.g. during maintenance).

The cyber incidents considered in this UR are events resulting from any offensive manoeuvre that targets OT systems onboard ships as defined in section 2.

1.3.3 System Category

System categories are defined in IACS UR E22 on the basis of the consequences of a system failure to human safety, safety of the vessel and/or threat to the environment.

1.3.4 IACS Documents on Computer Based Systems and Cyber Resilience

Attention is made to additional IACS documents on CBSs 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 E27 Cyber resilience of on-board systems and equipment includes requirements for cyber resilience for on-board systems and equipment.

IACS Recommendation 166 Recommendation 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. IACS Recommendation 166 on Cyber Resilience is intended for ships contracted for construction after its publication and may be used as a reference for ships already in service prior to its publication. For ships to which this UR applies as mandatory instrument, when both this UR and Recommendation 166 are used, should any difference in requirements addressing the same topic be found between the two instruments, the requirements in this UR shall prevail.

E26 (cont)

2. Definitions

In the purview of this UR, the following definitions apply:

Annual survey: See UR Z18

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 entity 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. CBSs onboard include IT and OT systems. A CBS may be a combination of subsystems connected via network. Onboard CBSs may be connected directly or via public means of communications (e.g. Internet) to ashore CBSs, other vessels' CBSs and/or other facilities.

Cyber incident: An event resulting from any offensive 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 cyber incidents arising from the disruption or impairment of operational technology (OT) used for the safe operation of a ship, which potentially lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment.

Essential services: Services 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.

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.

E26 (cont)

Logical network segment: The same as “Network segment”, but where two or more logical network segments share the same physical components.

Network: A connection between two or more computers for the purpose of communicating data electronically by means of agreed communication protocols.

Network segment: In the context of this UR, a network segment is an OSI layer-2 Ethernet segment (a broadcast domain).

Note on TCP/IP: Network address plan is prefixed by their IP addresses and the network mask. Communication between network segments is only possible by the use of routing service at network layer (OSI Layer 3).

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.

Physical network segment: The same as “Network segment”, but where physical components are not shared by other network segments.

Protocol: 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 fieldbuses.

Security zone: A collection of CBSs in the scope of applicability of this UR that meet the same security requirements. Each zone consists of a single interface or a group of interfaces, to which an access control policy is applied.

Shipowner/Company: The owner of the ship or any other organization or person, such as the manager, agent or bareboat charterer, who has assumed the responsibility for operation of the ship from the shipowner and who on assuming such responsibilities has agreed to take over all the attendant duties and responsibilities. The shipowner could be the Shipyard or systems integrator during initial construction. After vessel delivery, the shipowner may delegate some responsibilities to the vessel management company.

Special survey: See UR Z18

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 systems integrator.

Systems 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 systems 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.

E26 (cont)

3. Goals and organization of requirements

3.1 Primary goal

The primary goal is to support safe and secure shipping, which is operationally resilient to cyber risks.

Safe and secure shipping can be achieved through effective cyber risk management system. To support safe and secure shipping resilient to cyber risk, the following sub-goals for the management of cyber risk are defined in the five functional elements listed in section 3.2 below.

3.2 Sub-goals per functional element

1. Identify: Develop an organizational understanding to manage cybersecurity risk to onboard systems, people, assets, data, and capabilities.

2. Protect: Develop and implement appropriate safeguards to protect the ship against cyber incidents and maximize continuity of shipping operations.

3. Detect: Develop and implement appropriate measures to detect and identify the occurrence of a cyber incident onboard.

4. Respond: Develop and implement appropriate measures and activities to take action regarding a detected cyber incident onboard.

5. Recover: Develop and implement appropriate measures and activities to restore any capabilities or services necessary for shipping operations that were impaired due to a cyber incident.

These sub-goals and relevant functional elements should be concurrent and considered as parts of a single comprehensive risk management framework.

3.3 Organization of requirements

The requirements are organized according to a goal-based approach. Functional/technical requirements are given for the achievement of specific sub-goals of each functional element. The requirements are intended to allow a uniform implementation by stakeholders and to make them applicable to all types of vessels, in such a way as to enable an acceptable level of resilience and apply to all classed vessels/units regardless of operational risks and complexity of OT systems.

For each requirement, a rationale is given.

A summary of actions to be carried out and documentation to be made available is also given for each phase of the ship’s life and relevant stakeholders participating to such phase.

E26 (cont)

4. Requirements

This section contains the requirements to be satisfied in order to achieve the primary goal defined in 3.1, organized according to the five functional elements identified in 3.2.

The requirements shall be fulfilled by the stakeholders involved in the design, building and operation of the ship. Among them, the following stakeholders can be identified (see also section 2 for definitions):

- Shipowner/Company
- Systems integrator
- Supplier
- Classification Society

Whilst the above requirements may be fulfilled by these stakeholders, for the purposes of this UR, responsibility to fulfil them will lie with the stakeholder who has contracted with the Classification Society.

4.1 Identify

The requirements for the 'Identify' functional element are aimed at identifying: on one side, the CBSs onboard, their interdependencies and the relevant information flows; on the other side, the key resources involved in their management, operation and governance, their roles and responsibilities.

4.1.1 Vessel asset inventory

4.1.1.1 Requirement

An inventory of hardware and software (including application programs, operating systems, if any, firmware and other software components) of the CBSs in the scope of applicability of this UR and of the networks connecting such systems to each other and to other CBSs onboard or ashore shall be provided and kept up to date during the entire life of the ship.

4.1.1.2 Rationale

The inventory of CBSs onboard and relevant software used in OT systems, is essential for an effective management of cyber resilience of the ship, the main reason being that every CBS becomes a potential point of vulnerability. Cybercriminals can exploit unaccounted and out-of-date hardware and software to hack systems. Moreover, managing CBS assets enables Companies understand the criticality of each system to ship safety objectives.

4.1.1.3 Requirement details

The vessel asset inventory shall include at least the CBSs indicated in 1.3.2, if present onboard.

The inventory shall be kept updated during the entire life of the ship. Software and hardware modifications potentially introducing new vulnerabilities or modifying functional dependencies or connections among systems shall be recorded in the inventory.

E26 (cont)

If confidential information is included in the inventory (e.g. IP addresses, protocols, port numbers), special measures shall be adopted to limit the access to such information only to authorized people.

4.1.1.3.1 Hardware

For all hardware devices in the scope of applicability of this UR, the vessel asset inventory shall include at least the information in UR E27 section 3.1.1.

In addition, the vessel asset inventory may specify system category and security zone associated with the CBS.

4.1.1.3.2 Software

For all software in the scope of applicability of this UR (e.g., application program, operating system, firmware), the vessel asset inventory shall include at least the information in UR E27 section 3.1.1

The software of the CBSs in the scope of applicability of this UR shall be maintained and updated in accordance with the shipowner's process for management of software maintenance and update policy in the Ship cyber security and resilience program, see section 5.3.1.

4.1.1.4 Demonstration of compliance

4.1.1.4.1 Design phase

The systems integrator shall submit vessel asset inventory to the Society (ref. section 5.1.3).

The vessel asset inventory shall incorporate the asset inventories of all individual CBSs falling under the scope of this UR. Any equipment in the scope of this UR delivered by the systems integrator shall also be included in the vessel asset inventory.

4.1.1.4.2 Construction phase

The systems integrator shall keep the vessel asset inventory updated.

4.1.1.4.3 Commissioning phase

The systems integrator shall submit Ship cyber resilience test procedure (ref. section 5.2.1) and demonstrate to the Society that:

- Vessel asset inventory is updated and completed at delivery
- CBSs in the scope of applicability of this UR are correctly represented by the vessel asset inventory
- Software of the CBSs in the scope of applicability of this UR has been kept updated, e.g. by vulnerability scanning or by checking the software versions of CBSs while switched on.

4.1.1.4.4 Operation phase

For general requirements to surveys in the operation phase, see section 5.3.

E26 (cont)

The shipowner shall in the Ship cyber security and resilience program describe the process of management of change (MoC) for the CBSs in the scope of applicability of this UR, addressing at least the following requirements in this UR:

- Management of change (section 5.3)
- Hardware and software modifications (section 4.1.1.3)

The shipowner shall in the Ship cyber security and resilience program also describe the management of software updates, addressing at least the following requirements in this UR:

- Vulnerabilities and cyber risks (section 4.1.1.2 and 4.1.1.3)
- Security patching (section 4.2.6.3.2)

First annual survey

The shipowner shall present to the Society records or other documented evidence demonstrating implementation of the Ship cyber security and resilience program, i.e., that:

- The approved management of change process has been adhered to.
- Known vulnerabilities and functional dependencies have been considered for the software in the CBSs.
- The Vessel asset inventory has been kept updated.

Subsequent annual surveys

The shipowner shall upon request by the Society demonstrate implementation of the Ship cyber security and resilience program by presenting records or other documented evidence as specified for the first annual survey.

Special Survey

The shipowner shall demonstrate to the Society the activities in section 4.1.1.4.3 as per the Ship cyber resilience test procedure.

4.2 Protect

The requirements for the Protect functional element are aimed at the development and implementation of appropriate safeguards supporting the ability to limit or contain the impact of a potential incident.

4.2.1 Security Zones and Network Segmentation

4.2.1.1 Requirement

All CBSs in the scope of applicability of this UR shall be grouped into security zones with well-defined security policies and security capabilities. Security zones shall either be isolated (i.e. air gapped) or connected to other security zones or networks by means providing control of data communicated between the zones (e.g. firewalls/routers, simplex serial links, TCP/IP diodes, dry contacts, etc.)

E26 (cont)

Only explicitly allowed traffic shall traverse a security zone boundary.

4.2.1.2 Rationale

While networks may be protected by firewall perimeter and include Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) to monitor traffic coming in, breaching that perimeter is always possible. Network segmentation makes it more difficult for an attacker to perpetrate an attack throughout the entire network.

The main benefits of security zones and network segmentation are to reduce the extent of the attack surface, prevent attackers from achieving lateral movement through systems, and improve network performance. The concept of allocating the CBSs into security zones allows grouping the CBSs in accordance with their risk profile.

4.2.1.3 Requirement details

A security zone may contain multiple CBSs and networks, all of which shall comply with applicable security requirements given in this UR and UR E27.

The network(s) of a security zone shall be logically or physically segmented from other zones or networks. See also 4.2.6.3.

CBSs providing required safety functions shall be grouped into separate security zones and shall be physically segmented from other security zones.

Navigational and communication systems shall not be in same security zone as machinery or cargo systems. If navigation and/or radiocommunication systems are approved in accordance with other equivalent standard(s) (see section 1.3.2), these systems should be in a dedicated security zone.

Wireless devices shall be in dedicated security zones. See also 4.2.5.

Systems, networks or CBSs outside the scope of applicability of this UR are considered untrusted networks and shall be physically segmented from security zones required by this UR. Alternatively, it is accepted that such systems are part of a security zone if these OT-systems meet the same requirements as demanded by the zone.

It shall be possible to isolate a security zone without affecting the primary functionality of the CBSs in the zone, see also section 4.4.3.

4.2.1.4 Demonstration of compliance

4.2.1.4.1 Design phase

The systems integrator shall submit Zones and conduit diagram and the Cyber security design description (see 5.1.1 and 5.1.2).

The Zones and conduit diagram shall illustrate the CBSs in the scope of applicability of this UR, how they are grouped into security zones, and include the following information:

- Clear indication of the security zones

E26 (cont)

- Simplified illustration of each CBS in scope of applicability of this UR, and indication of the security zone in which the CBS is allocated, and indication of physical location of the CBS/equipment.

- Reference to the approved version of the CBS system topology diagrams provided by the suppliers (UR E27 section 3.1.2)

- Illustration of network communication between systems in a security zone

- Illustration of any network communication between systems in different security zones (conduits).

- Illustration of any communication between systems in a security zone and untrusted networks (conduits).

The systems integrator shall include the following information in the Cyber security design description:

- A short description of the CBSs allocated to the security zone. It shall be possible to identify each CBS in the Zones and conduit diagram.

- Network communication between CBSs in the same security zone. The description shall include purpose and characteristics (i.e. protocols and data flows) of the communication.

- Network communication between CBSs in different security zones. The description shall include purpose and characteristics (i.e. protocols and data flows) of the communication. The description shall also include zone boundary devices and specify the traffic that is permitted to traverse the zone boundary (e.g. firewall rules).

- Any communication between CBSs in security zones and untrusted networks. The description shall include discrete signals, serial communication, and the purpose and characteristics (i.e. protocols and data flows) of IP-based network communication. The description shall also include zone boundary devices and specify the traffic that is permitted to traverse the zone boundary (e.g. firewall rules).

4.2.1.4.2 Construction phase

The systems integrator shall keep the Zones and conduit diagram updated.

4.2.1.4.3 Commissioning phase

The systems integrator shall submit Ship cyber resilience test procedure (ref. section 5.2.1) and demonstrate to the Society that:

- the security zones on board are implemented in accordance with the approved documents (i.e. zones and conduit diagram, cyber security design description, asset inventory, and relevant documents provided by the supplier). This may be done by e.g., inspection of the physical installation, network scanning and/or other methods providing the Surveyor assurance that the installed equipment is grouped in security zones according to the approved design.

E26 (cont)

- security zone boundaries allow only the traffic that has been documented in the approved Cyber security description. This may be done by e.g., evaluation of firewall rules or port scanning.

4.2.1.4.4 Operation phase

For general requirements to surveys in the operation phase, see section 5.3.

The shipowner shall in the Ship cyber security and resilience program describe the management of security zone boundary devices (e.g., firewalls), addressing at least the following requirements in this UR:

- Principle of Least Functionality (section 4.2.2.1)
- Explicitly allowed traffic (section 4.2.1.1)
- Protection against denial of service (DoS) events (section 4.2.2.1)
- Inspection of security audit records (section 4.3.1.3)

First annual survey

The shipowner shall demonstrate to the Society that the Zones and conduit diagram has been kept updated and present records or other documented evidence demonstrating implementation of the Ship cyber security and resilience program, i.e., that security zone boundaries are managed in accordance with the above requirements.

Subsequent annual surveys

The shipowner shall upon request by the Society demonstrate implementation of the Ship cyber security and resilience program by presenting records or other documented evidence as specified for the first annual survey.

Special survey

The shipowner shall demonstrate to the Society the activities in section 4.2.1.4.3 as per the Ship cyber resilience test procedure.

4.2.2 Network protection safeguards

4.2.2.1 Requirement

Security zones shall be protected by firewalls or equivalent means as specified in section 4.2.1.

The networks shall also be protected against the occurrence of excessive data flow rate and other events which could impair the quality of service of network resources.

The CBSs in scope of this UR shall be implemented in accordance with the principle of Least Functionality, i.e. configured to provide only essential capabilities and to prohibit or restrict the use of non-essential functions, where unnecessary functions, ports, protocols and services are disabled or otherwise prohibited.

E26 (cont)

4.2.2.2 Rationale

Network protection covers a multitude of technologies, rules and configurations designed to protect the integrity, confidentiality and availability of networks. The threat environment is always changing, and attackers are always trying to find and exploit vulnerabilities.

There are many layers to consider when addressing network protection. Attacks can happen at any layer in the network layers model, so network hardware, software and policies must be designed to address each area.

While physical and technical security controls are designed to prevent unauthorized personnel from gaining physical access to network components and protect data stored on or in transit across the network, procedural security controls consist of security policies and processes that control user behaviour.

4.2.2.3 Requirement details

The design of network shall include means to meet the intended data flow through the network and minimize the risk of denial of service (DoS) and network storm/high rate of traffic. Estimation of data flow rate shall at least consider the capacity of network, data speed requirement for intended application and data format.

4.2.2.4 Demonstration of compliance

4.2.2.4.1 Design phase

No requirements.

4.2.2.4.2 Construction phase

No requirements.

4.2.2.4.3 Commissioning phase

The systems integrator shall submit Ship cyber resilience test procedure (ref. section 5.2.1) and demonstrate the following to the Society:

- Test denial of service (DoS) attacks targeting zone boundary protection devices, as applicable.
- Test denial of service (DoS) to ensure protection against excessive data flow rate, originating from inside each network segment. Such denial of service (DoS) tests shall cover flooding of network (i.e., attempt to consume the available capacity on the network segment), and application layer attack (i.e., attempt to consume the processing capacity of selected endpoints in the network)
- Test e.g. by analytic evaluation and port scanning that unnecessary functions, ports, protocols and services in the CBSs have been removed or prohibited in accordance with hardening guidelines provided by the suppliers. See UR E27 section 5.7 and 6.3.4.7.

The second and third tests may be omitted if performed during the certification of CBSs as per section 5.2.1.

E26 (cont)

4.2.2.4.4 Operation phase

For general requirements to surveys in the operation phase, see section 5.3.

Special survey

Subject to modifications of the CBSs, the shipowner shall demonstrate to the Society the activities in section 4.2.2.4.3 as per the Ship cyber resilience test procedure.

4.2.3 Antivirus, antimalware, antispam and other protections from malicious code

4.2.3.1 Requirement

CBSs in the scope of applicability of this UR shall be protected against malicious code such as viruses, worms, trojan horses, spyware, etc.

4.2.3.2 Rationale

A virus or any unwanted program that enters a user's system without his/her knowledge can self-replicate and spread, perform unwanted and malicious actions that end up affecting the system's performance, user's data/files, and/or circumvent data security measures.

Antivirus, antimalware, antispam software will act as a closed door with a security guard fending off the malicious intruding viruses performing a prophylactic function. It detects potential virus and then works to remove it, mostly before the virus gets to harm the system.

Common means for malicious code to enter CBSs are electronic mail, electronic mail attachments, websites, removable media (for example, universal serial bus (USB) devices, diskettes or compact disks), PDF documents, web services, network connections and infected laptops.

4.2.3.3 Requirement details

Malware protection shall be implemented on CBSs in the scope of applicability of this UR. On CBSs having an operating system for which industrial-standard anti-virus and anti-malware software is available and maintained up-to-date, anti-virus and/or anti-malware software shall be installed, maintained and regularly updated, unless the installation of such software impairs the ability of CBS to provide the functionality and level of service required (e.g. for Cat.II and Cat.III CBSs performing real-time tasks).

On CBSs where anti-virus and anti-malware software cannot be installed, malware protection shall be implemented in the form of operational procedures, physical safeguards, or according to manufacturer's recommendations.

4.2.3.4 Demonstration of compliance

4.2.3.4.1 Design phase

The systems integrator shall include the following information in the Cyber security design description:

- For each CBS, summary of the approved mechanisms provided by the supplier for protection against malicious code or unauthorized software.

E26 (cont)

- For CBSs with anti-malware software, information about how to keep the software updated.

- Any operational conditions or necessary physical safeguards to be implemented in the shipowner's management system.

4.2.3.4.2 Construction phase

The systems integrator shall ensure that malware protection is kept updated during the construction phase.

4.2.3.4.3 Commissioning phase

The systems integrator shall submit Ship cyber resilience test procedure (ref. section 5.2.1) and demonstrate the following to the Society:

- Approved anti-malware software or other compensating countermeasures is effective (test e.g., with a trustworthy anti-malware test file).

The above tests may be omitted if performed during the certification of CBSs as per section 5.2.1.

4.2.3.4.4 Operation phase

For general requirements to surveys in the operation phase, see section 5.3.

The shipowner shall in the Ship cyber security and resilience program describe the management of malware protection, addressing at least the following requirements in this UR:

- Maintenance/update (section 4.2.3.3)

- Operational procedures, physical safeguards (section 4.2.3.3)

- Use of mobile, portable, removable media (section 4.2.4.3.4 and 4.2.7.3)

- Access control (section 4.2.4)

First annual survey

The shipowner shall present to the Society records or other documented evidence demonstrating implementation of the Ship cyber security and resilience program, i.e., that:

- Any anti-malware software has been maintained and updated.

- Procedures for use of portable, mobile or removable devices have been followed.

- Policies and procedures for access control have been followed.

- Physical safeguards are maintained.

E26 (cont)

Subsequent annual surveys

The shipowner shall upon request by the Society demonstrate implementation of the Ship cyber security and resilience program by presenting records or other documented evidence as specified for the first annual survey.

Special survey

The shipowner shall demonstrate to the Society the activities in section 4.2.3.4.3 as per the Ship cyber resilience test procedure.

4.2.4 Access control

4.2.4.1 Requirement

CBSs and networks in the scope of applicability of this UR shall provide physical and/or logical/digital measures to selectively limit the ability and means to communicate with or otherwise interact with the system itself, to use system resources to handle information, to gain knowledge of the information the system contains or to control system components and functions. Such measures shall be such as not to hamper the ability of authorized personnel to access CBS for their level of access according to the least privilege principle.

4.2.4.2 Rationale

Attackers may attempt to access the ship's systems and data from either onboard the ship, within the company, or remotely through connectivity with the internet. Physical and logical access controls to cyber assets, networks etc. should then be implemented to ensure safety of the ship and its cargo.

Physical threats and relevant countermeasures are also considered in the ISPS Code. Similarly, the ISM Code contains guidelines to ensure safe operation of ships and protection of the environment. Implementation of ISPS and ISM Codes may imply inclusion in the Ship Security Plan (SSP) and Safety Management System (SMS) of instructions and procedures for access control to safety critical assets.

4.2.4.3 Requirement details

Access to CBSs and networks in the scope of applicability of this UR and all information stored on such systems shall only be allowed to authorized personnel, based on their need to access the information as a part of their responsibilities or their intended functionality.

4.2.4.3.1 Physical access control

CBSs of Cat.II and Cat.III shall generally be located in rooms that can normally be locked or in controlled space to prevent unauthorized access, or shall be installed in lockable cabinets or consoles. Such locations or lockable cabinets/consoles shall be however easy to access to the crew and various stakeholders who need to access to CBSs for installation, integration, operation, maintenance, repair, replacement, disposal etc. so as not to hamper effective and efficient operation of the ship.

E26 (cont)

4.2.4.3.2 Physical access control for visitors

Visitors such as authorities, technicians, agents, port and terminal officials, and shipowner representatives shall be restricted regarding access to CBSs onboard whilst on board, e.g. by allowing access under supervision.

4.2.4.3.3 Physical access control of network access points

Access points to onboard networks connecting Cat.II and/or Cat.III CBSs shall be physically and/or logically blocked except when connection occurs under supervision or according to documented procedures, e.g. for maintenance.

Independent computers isolated from all onboard networks, or other networks, such as dedicated guest access networks, or networks dedicated to passenger recreational activities, shall be used in case of occasional connection requested by a visitor (e.g. for printing documents).

4.2.4.3.4 Removable media controls

A policy for the use of removable media devices shall be established, with procedures to check removable media for malware and/or validate legitimate software by digital signatures and watermarks and scan prior to permitting the uploading of files onto a ship's system or downloading data from the ship's system. See also 4.2.7.

4.2.4.3.5 Management of credentials

CBSs and relevant information shall be protected with file system, network, application, or database specific Access Control Lists (ACL). Accounts for onboard and onshore personnel shall be left active only for a limited period according to the role and responsibility of the account holder and shall be removed when no longer needed.

Note: CBSs shall identify and authenticate human users as per item No.1 in Table 1 of UR E27. In other words, it is not necessary to "uniquely" identify and authenticate all human users

Onboard CBSs shall be provided with appropriate access control that fits to the policy of their Security Zone but does not adversely affect their primary purpose. CBSs which require strong access control may need to be secured using a strong encryption key or multi-factor authentication.

Administrator privileges shall be managed in accordance with the policy for access control, allowing only authorized and appropriately trained personnel full access to the CBS, who as part of their role in the company or onboard need to log on to systems using these privileges.

4.2.4.3.6 Least privilege principle

Any human user allowed to access CBS and networks in the scope of applicability of this UR shall have only the bare minimum privileges necessary to perform its function.

The default configuration for all new account privileges shall be set as low as possible. Wherever possible, raised privileges shall be restricted only to moments when they are needed, e.g. using only expiring privileges and one-time-use credentials. Accumulation of privileges over time shall be avoided, e.g. by regular auditing of user accounts.

E26 (cont)

4.2.4.4 Demonstration of compliance

4.2.4.4.1 Design phase

The systems integrator shall include the following information in the Cyber security design description:

- Location and physical access controls for the CBSs. Devices providing Human Machine Interface (HMI) for operators needing immediate access need not enforce user identification and authentication provided they are located in an area with physical access control. Such devices shall be specified.

4.2.4.4.2 Construction phase

The systems integrator shall prevent unauthorised access to the CBSs during the construction phase.

4.2.4.4.3 Commissioning phase

The systems integrator shall submit Ship cyber resilience test procedure (ref. section 5.2.1) and demonstrate the following to the Society:

- Components of the CBSs are located in areas or enclosures where physical access can be controlled to authorised personnel.

- User accounts are configured according to the principles of segregation of duties and least privilege and that temporary accounts have been removed (may be omitted based on certification of CBSs as per section 5.2.1)

4.2.4.4.4 Operation phase

For general requirements to surveys in the operation phase, see section 5.3.

The shipowner shall in the Ship cyber security and resilience program describe the management of logical and physical access, addressing at least the following requirements in this UR:

- Physical access control (section 4.2.4.3.1)

- Physical access control for visitors (section 4.2.3.4.2)

- Physical access control of network access points (section 4.2.4.3.3)

- Management of credentials (section 4.2.4.3.5)

- Least privilege policy (section 4.2.4.3.6)

The shipowner shall in the Ship cyber security and resilience program describe the management of confidential information, addressing at least the following requirements in this UR:

- Confidential information (section 4.1.1.3)

- Information allowed to authorized personnel (section 4.2.4.3)

E26 (cont)

- Information transmitted on the wireless network (section 4.2.5.3)

First annual survey

The shipowner shall present to the Society records or other documented evidence demonstrating implementation of the Ship cyber security and resilience program, i.e., that:

- Personnel are authorized to access the CBSs in accordance with their responsibilities.
- Only authorised devices are connected to the CBSs.
- Visitors are given access to the CBSs according to relevant policies and procedures.
- Physical access controls are maintained and applied.
- Credentials, keys, secrets, certificates, relevant CBS documentation, and other sensitive information is managed and kept confidential according to relevant policies and procedures.

Subsequent annual surveys

The shipowner shall upon request by the Society demonstrate implementation of the Ship cyber security and resilience program by presenting records or other documented evidence as specified for the first annual survey.

4.2.5 Wireless communication

4.2.5.1 Requirement

Wireless communication networks in the scope of this UR shall be designed, implemented and maintained to ensure that:

- Cyber incidents will not propagate to other control systems
- Only authorised human users will gain access to the wireless network
- Only authorised processes and devices will be allowed to communicate on the wireless network
- Information in transit on the wireless network cannot be manipulated or disclosed

4.2.5.2 Rationale

Wireless networks give rise to additional or different cybersecurity risks than wired networks. This is mainly due to less physical protection of the devices and the use of the radio frequency communication.

Inadequate physical access control may lead to unauthorised personnel gaining access to the physical devices, which in turn could lead to circumventing logical access restrictions or deployment of rogue devices on the network.

Signal transmission by radio frequency introduces risks related to jamming as well as eavesdropping which in turn could cater for attacks such as Piggybacking or Evil twin attacks (see https://us-cert.cisa.gov/ncas/tips/ST05-003).

E26 (cont)

4.2.5.3 Requirement details

Cryptographic mechanisms such as encryption algorithms and key lengths in accordance with industry standards and best practices shall be applied to ensure integrity and confidentiality of the information transmitted on the wireless network.

Devices on the wireless network shall only communicate on the wireless network (i.e. they shall not be “dual-homed”)

Wireless networks shall be designed as separate segments in accordance with 4.2.1 and protected as per 4.2.2.

Wireless access points and other devices in the network shall be installed and configured such that access to the network can be controlled.

The network device or system utilizing wireless communication shall provide the capability to identify and authenticate all users (humans, software processes or devices) engaged in that communication.

4.2.5.4 Demonstration of compliance

4.2.5.4.1 Design phase

The systems integrator shall include the following information in the Cyber security design description:

- Description of wireless networks in the scope of applicability of this UR and how these are implemented as separate security zones. The description shall include zone boundary devices and specify the traffic that is permitted to traverse the zone boundary (e.g. firewall rules)

4.2.5.4.2 Construction phase

The systems integrator shall prevent unauthorised access to the wireless networks during the construction phase.

4.2.5.4.3 Commissioning phase

The systems integrator shall submit Ship cyber resilience test procedure (ref. section 5.2.1) and demonstrate the following to the Society:

- Only authorised devices can access the wireless network.

- Secure wireless communication protocol is used as per approved documentation by the respective supplier (demonstrate e.g. by use of a network protocol analyser tool).

The above tests may be omitted if performed during the certification of CBSs as per section 5.2.1.

4.2.5.4.4 Operation phase

For general requirements to surveys in the operation phase, see section 5.3.

E26 (cont)

Special survey

Subject to modifications of the wireless networks in the scope of applicability of this UR, the shipowner shall demonstrate to the Society the activities in section 4.2.5.4.3 as per the Ship cyber resilience test procedure.

4.2.6 Remote access control and communication with untrusted networks

4.2.6.1 Requirement

CBSs in scope of this UR shall be protected against unauthorized access and other cyber threats from untrusted networks.

4.2.6.2 Rationale

Onboard CBSs have become increasingly digitalized and connected to the internet to perform a wide variety of legitimate functions. The use of digital systems to monitor and control onboard CBSs makes them vulnerable to cyber incidents. Attackers may attempt to access onboard CBSs through connectivity with the internet and may be able to make changes that affect a CBS's operation or even achieve full control of the CBS, or attempt to download information from the ship's CBS. In addition, since use of legacy IT and OT systems that are no longer supported and/or rely on obsolete operating systems affects cyber resilience, special care should be put to relevant hardware and software installations on board to help maintain a sufficient level of cyber resilience when such systems can be remotely accessed, also keeping in mind that not all cyber incidents are a result of a deliberate attack.

4.2.6.3 Requirement details

User's manual shall be delivered for control of remote access to onboard IT and OT systems. Clear guidelines shall identify roles and permissions with functions.

For CBSs in the scope of applicability of this UR, no IP address shall be exposed to untrusted networks.

Communication with or via untrusted networks requires secure connections (e.g. tunnels) with endpoint authentication, protection of integrity and authentication and encryption at network or transport layer. Confidentiality shall be ensured for information that is subject to read authorization.

4.2.6.3.1 Design

CBSs in the scope of applicability of this UR shall:

- have the capability to terminate a connection from the onboard connection endpoint. Any remote access shall not be possible until explicitly accepted by a responsible role on board.

- be capable of managing interruptions during remote sessions so as not to compromise the safe functionality of OT systems or the integrity and availability of data used by OT systems.

- provide a logging function to record all remote access events and retain for a period of time sufficient for offline review of remote connections, e.g. after detection of a cyber incident.

E26 (cont)

4.2.6.3.2 Additional requirements for remote maintenance

When remote access is used for maintenance, the following requirements shall be complied with in addition to those in 4.2.6.3.1:

- Documentation shall be provided to show how they connect and integrate with the shore side.

- Security patches and software updates shall be tested and evaluated before they are installed to ensure they are effective and do not result in side effects or cyber events that cannot be tolerated. A confirmation report from the software supplier towards above shall be obtained, prior to undertaking remote update.

- Suppliers shall provide plans for- and make security updates available to the shipowner, see UR E27 section 5.2, 5.3 and 5.4.

- At any time, during remote maintenance activities, authorized personnel shall have the possibility to interrupt and abort the activity and roll back to a previous safe configuration of the CBS and systems involved.

- Multi-factor authentication is required for any access by human users to CBS's in scope from an untrusted network.

- After a configurable number of failed remote access attempts, the next attempt shall be blocked for a predetermined length of time.

- If the connection to the remote maintenance location is disrupted for some reason, access to the system shall be terminated by an automatic logout function.

4.2.6.4 Demonstration of compliance

4.2.6.4.1 Design phase

The systems integrator shall include the following information in the Cyber security design description:

- Identification of each CBS in the scope of applicability of this UR that can be remotely accessed or that otherwise communicates through the security zone boundary with untrusted networks.

- For each CBS, a description of compliance with requirements in 4.2.6.3, as applicable

4.2.6.4.2 Construction phase

The systems integrator shall ensure that any communication with untrusted networks is only temporarily enabled and used in accordance with the requirements of this section.

4.2.6.4.3 Commissioning phase

The systems integrator shall submit Ship cyber resilience test procedure (ref. section 5.2.1) and demonstrate the following to the Society:

- Communication with untrusted networks is secured in accordance with UR E27 section 4.2 and that the communication protocols cannot be negotiated to a less secure version (demonstrate e.g., by use of a network protocol analyzer tool).

E26 (cont)

- Remote access requires multifactor authentication of the remote user.
- A limit of unsuccessful login attempts is implemented, and that a notification message is provided for the remote user before session is established.
- Remote connections must be explicitly accepted by responsible personnel on board.
- Remote sessions can be manually terminated by personnel on board or that the session will automatically terminate after a period of inactivity.
- Remote sessions are logged (see UR E27 section 4.1 item 13).
- Instructions or procedures are provided by the respective product suppliers (see UR E27 section 3.1.3).

4.2.6.4.4 Operation phase

For general requirements to surveys in the operation phase, see section 5.3.

The shipowner shall in the Ship cyber security and resilience program describe the management of remote access and communication with/via untrusted networks, addressing at least the following requirements in this UR:

- User's manual (section 4.2.6.3)
- Roles and permissions (section 4.2.6.3)
- Patches and updates (section 4.2.6.3.2)
- Confirmation prior to undertaking remote software update (section 4.2.6.3.2)
- Interrupt, abort, roll back (section 4.2.6.3.2)

First annual survey

The shipowner shall present to the Society records or other documented evidence demonstrating implementation of the Ship cyber security and resilience program, i.e., that:

- Remote access sessions have been recorded or logged and carried out as per relevant policies and user manuals.
- Installation of security patches and other software updates have been carried out in accordance with Management of change procedures and in cooperation with the supplier.

Annual survey

The shipowner shall upon request by the Society demonstrate implementation of the Ship cyber security and resilience program by presenting records or other documented evidence as specified for the first annual survey.

E26 (cont)

Special survey

The shipowner shall demonstrate to the Society the activities in section 4.2.6.4.3 as per the Ship cyber resilience test procedure.

4.2.7 Use of Mobile and Portable Devices

4.2.7.1 Requirement

The use of mobile and portable devices in CBSs in the scope of applicability of this UR shall be limited to only necessary activities and be controlled in accordance with UR E27 section 4.1 item 10. For any CBS that cannot fully meet these requirements, the interface ports shall be physically blocked.

4.2.7.2 Rationale

It is generally known that CBSs can be impaired due to malware infection via a mobile or a portable device. Therefore, connection of mobile and portable devices should be carefully considered. In addition, mobile equipment that is required to be used for the operation and maintenance of the ship should be under the control of the shipowner.

4.2.7.3 Requirement details

Mobile and portable devices shall only be used by authorised personnel. Only authorised devices may be connected to the CBSs. All use of such devices shall be in accordance with the shipowner's policy for use of mobile and portable devices, taking into account the risk of introducing malware in the CBS.

4.2.7.4 Demonstration of compliance

4.2.7.4.1 Design phase

The systems integrator shall include the following information in the Cyber security design description:

- Any CBSs in the scope of applicability that do not meet the requirements in UR E27 section 4.1 item 10, i.e., that shall have protection of interface ports by physical means such as port blockers.

4.2.7.4.2 Construction phase

The systems integrator shall ensure that use of physical interface ports in the CBSs is controlled in accordance with UR E27 section 4.1 item 10, and that any use of such devices follows procedures to prevent malware from being introduced in the CBS.

4.2.7.4.3 Commissioning phase

The systems integrator shall submit Ship cyber resilience test procedure (ref. section 5.2.1) and demonstrate to the Society that capabilities to control use of mobile and portable devices are implemented correctly, the following countermeasures shall be demonstrated as relevant:

- Use of mobile and portable devices is restricted to authorised users
- Interface ports can only be used by specific device types

E26 (cont)

- Files cannot be transferred to the system from such devices
- Files on such devices will not be automatically executed (by disabling autorun)
- Network access is limited to specific MAC or IP addresses
- Unused interface ports are disabled
- Unused interface ports are physically blocked

4.2.7.4.4 Operation phase

For general requirements to surveys in the operation phase, see section 5.3.

The shipowner shall in the Ship cyber security and resilience program describe the management of mobile and portable devices, addressing at least the following requirements in this UR:

- Policy and procedures (section 4.2.4.3.4)
- Physical block of interface ports (section 4.2.7.1)
- Use by authorized personnel (section 4.2.7.3)
- Connect only authorized devices (section 4.2.7.3)
- Consider risk of introducing malware (section 4.2.7.3)

First annual survey

The shipowner shall present to the Society records or other documented evidence demonstrating implementation of the Ship cyber security and resilience program, i.e., that:

- The use of mobile, portable or removable media is restricted to authorised personnel and follows relevant policies and procedures.
- Only authorised devices are connected to the CBSs.
- Means to restrict use of physical interface ports are implemented as per approved design documentation.

Subsequent annual surveys

The shipowner shall upon request by the Society demonstrate implementation of the Ship cyber security and resilience program by presenting records or other documented evidence as specified for the first annual survey.

Special survey

The shipowner shall demonstrate to the Society the activities in section 4.2.7.4.3 as per the Ship cyber resilience test procedure.

E26
(cont)

4.3 Detect

The requirements for the Detect functional element are aimed at the development and implementation of appropriate means supporting the ability to reveal and recognize anomalous activity on CBSs and networks onboard and identify cyber incidents.

4.3.1 Network operation monitoring

4.3.1.1 Requirement

Networks in scope of this UR shall be continuously monitored, and alarms shall be generated if malfunctions or reduced/degraded capacity occurs.

4.3.1.2 Rationale

Cyber-attacks are becoming increasingly sophisticated, and attacks that target vulnerabilities that were unknown at the time of construction could result in incidents where the vessel is ill-prepared for the threat. To enable an early response to attacks targeting these types of unknown vulnerabilities, technology capable of detecting unusual events is required. A monitoring system that can detect anomalies in networks and that can use post-incident analysis provides the ability to appropriately respond and further recover from a cyber event.

4.3.1.3 Requirement details

Measures to monitor networks in the scope of applicability of this UR shall have the following capabilities:

- Monitoring and protection against excessive traffic
- Monitoring of network connections
- Monitoring and recording of device management activities
- Protection against connection of unauthorized devices
- Generate alarm if utilization of the network's bandwidth exceeds a threshold specified as abnormal by the supplier. See UR E22 section 7.2.1.

Intrusion detection systems (IDS) may be implemented, subject to the following:

- The IDS shall be qualified by the supplier of the respective CBS
- The IDS shall be passive and not activate protection functions that may affect the performance of the CBS
- Relevant personnel should be trained and qualified for using the IDS

4.3.1.4 Demonstration of compliance

4.3.1.4.1 Design phase

No requirements.

E26
(cont)

4.3.1.4.2 Construction phase

No requirements.

4.3.1.4.3 Commissioning phase

The systems integrator shall specify in the Ship cyber resilience test procedure and demonstrate to the Society the network monitoring and protection mechanisms in the CBSs.

- Test that disconnected network connections will activate alarm and that the event is recorded.
- Test that abnormally high network traffic is detected, and that alarm and audit record is generated. This test may be carried on together with the test in section 4.4.4.4.3.
- Demonstrate that the CBS will respond in a safe manner to network storm scenarios, considering both unicast and broadcast messages (see also 4.2.2.4.3)
- Demonstrate generation of audit records (logging of security-related events)
- If Intrusion detection systems are implemented, demonstrate that this is passive and will not activate protection functions that may affect intended operation of the CBSs.

The above tests may be omitted if performed during the certification of CBSs as per section 5.2.1.

Any Intrusion detection systems in the CBSs in scope of applicability to be implemented shall be subject to verification by the Society. Relevant documentation shall be submitted for approval, and survey/tests shall be carried out on board.

4.3.1.4.4 Operation phase

For general requirements to surveys in the operation phase, see section 5.3.

The shipowner shall in the Ship cyber security and resilience program describe the management activities to detect anomalies in the CBSs and networks, addressing at least the following requirements in this UR:

- Reveal and recognize anomalous activity (section 4.3)
- Inspection of security audit records (section 4.3.1.3)
- Instructions or procedures to detect incidents (section 4.4.1.1)

The above activities may be addressed together with incident response in section 4.4.1.

<u>First annual survey</u>

The shipowner shall present to the Society records or other documented evidence demonstrating implementation of the Ship cyber security and resilience program, i.e., that:

- The CBSs are routinely monitored for anomalies by inspection of security audit records and investigation of alerts in the CBSs.

E26 (cont)

Subsequent annual surveys

The shipowner shall upon request by the Society demonstrate implementation of the Ship cyber security and resilience program by presenting records or other documented evidence as specified for the first annual survey.

Special survey

Subject to modifications of the CBSs, the shipowner shall demonstrate to the Society the activities in section 4.3.1.4.3 as per the Ship cyber resilience test procedure.

4.3.2 Verification and diagnostic functions of CBS and networks

4.3.2.1 Requirement

CBSs and networks in the scope of applicability of this UR shall be capable to check performance and functionality of security functions required by this UR. Diagnostic functions shall provide adequate information on CBSs integrity and status for the use of the intended user and means for maintaining their functionality for a safe operation of the ship.

4.3.2.2 Rationale

The ability to verify intended operation of the security functions is important to support management of cyber resilience in the lifetime of the ship. Tools for diagnostic functions may comprise automatic or manual functions such as self-diagnostics capabilities of each device, or tools for network monitoring (such as ping, traceroute, ipconfig, netstat, nslookup, Wireshark, nmap, etc.).

It should be noted however that execution of diagnostic functions may sometimes impact the operational performance of the CBS.

4.3.2.3 Requirement details

CBSs and networks' diagnostics functionality shall be available to verify the intended operation of all required security functions during test and maintenance phases of the ship.

4.3.2.4 Demonstration of compliance

4.3.2.4.1 Design phase

No requirements.

4.3.2.4.2 Construction phase

No requirements.

4.3.2.4.3 Commissioning phase

The systems integrator shall submit Ship cyber resilience test procedure (ref. section 5.2.1) and demonstrate to the Society the effectiveness of the procedures for verification of security functions provided by the suppliers.

The above tests may be omitted if performed during the certification of CBSs as per section 5.2.1.

E26 (cont)

4.3.2.4.4 Operation phase

For general requirements to surveys in the operation phase, see section 5.3.

The shipowner shall in the Ship cyber security and resilience program describe the management activities to verify correct operation of the security functions in the CBSs and networks, addressing at least the following requirements in this UR:

- Test and maintenance periods (section 4.3.2.3)
- Periodic maintenance (section 5.3.3)

First annual survey

The shipowner shall present to the Society records or other documented evidence demonstrating implementation of the Ship cyber security and resilience program, i.e., that:

- The security functions in the CBSs are periodically tested or verified.

Subsequent annual surveys

The shipowner shall upon request by the Society demonstrate implementation of the Ship cyber security and resilience program by presenting records or other documented evidence as specified for the first annual survey.

4.4 Respond

The requirements for the Respond functional element are aimed at the development and implementation of appropriate means supporting the ability to minimize the impact of cyber incidents, containing the extension of possible impairment of CBSs and networks onboard.

4.4.1 Incident response plan

4.4.1.1 Requirement

An incident response plan shall be developed by the shipowner covering relevant contingencies and specifying how to react to cyber security incidents. The Incident response plan shall contain documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of incidents against CBSs in the scope of applicability of this UR.

4.4.1.2 Rationale

An incident response plan is an instrument aimed to help responsible persons respond to cyber incidents. As such, the Incident response plan is as effective as it is simple and carefully designed. When developing the Incident response plan, it is important to understand the significance of any cyber incident and prioritize response actions accordingly.

Means for maintaining as much as possible the functionality and a level of service for a safe operation of the ship, e.g. transfer active execution to a standby redundant unit, should also be indicated. Designated personnel ashore should be integrated with the ship in the event of a cyber incident.

E26 (cont)

4.4.1.3 Requirement details

The various stakeholders involved in the design and construction phases of the ship shall provide information to the shipowner for the preparation of the Incident Response Plan to be placed onboard at the first annual Survey. The Incident Response Plan shall be kept up-to-date (e.g. upon maintenance) during the operational life of the ship.

The Incident response plan shall provide procedures to respond to detected cyber incidents on networks by notifying the proper authority, reporting needed evidence of the incidents and taking timely corrective actions, to limit the cyber incident impact to the network segment of origin.

The incident response plan shall, as a minimum, include the following information:

- Breakpoints for the isolation of compromised systems;
- A description of alarms and indicators signalling detected ongoing cyber events or abnormal symptoms caused by cyber events;
- A description of expected major consequences related to cyber incidents;
- Response options, prioritizing those which do not rely on either shut down or transfer to independent or local control, if any.
- Independent and local control information for operating independently from the system that failed due to the cyber incident, as applicable;

The Incident response plan shall be kept in hard copy in the event of complete loss of electronic devices enabling access to it.

4.4.1.4 Demonstration of compliance

4.4.1.4.1 Design phase

The systems integrator shall include the following information in the Cyber security design description:

- References to information provided by the suppliers (see UR E27 section 3.1.8) that may be applied by the shipowner to establish plans for incident response.

4.4.1.4.2 Construction phase

No requirements.

4.4.1.4.3 Commissioning phase

No requirements.

4.4.1.4.4 Operation phase

For general requirements to surveys in the operation phase, see section 5.3.

The shipowner shall in the Ship cyber security and resilience program describe incident response plans. The plans shall cover the CBSs in scope of applicability of this UR and shall address at least the following requirements in this UR:

E26 (cont)

- Description of who, when and how to respond to cyber incidents in accordance with requirements of section 4.4.1
- Procedures or instructions for local/manual control in accordance with requirements in section 4.4.2
- Procedures or instructions for isolation of security zones in accordance with requirements in section 4.4.3
- Description of expected behaviour of the CBSs in the event of cyber incidents in accordance with requirements in section 4.4.4.

First annual survey

The shipowner shall present to the Society records or other documented evidence demonstrating implementation of the Ship cyber security and resilience program, i.e., that:

- The incident response plans are available for the responsible personnel onboard.
- Procedures or instructions for local/manual controls are available for responsible personnel onboard.
- Procedures or instructions for disconnection/isolation of security zones are available for responsible personnel onboard.
- Any cyber incidents have been responded to in accordance with the incident response plans.

Subsequent annual surveys

The shipowner shall upon request by the Society demonstrate implementation of the Ship cyber security and resilience program by presenting records or other documented evidence as specified for the first annual survey.

4.4.2 Local, independent and/or manual operation

4.4.2.1 Requirement

Any CBS needed for local backup control as required by SOLAS II-1 Regulation 31 shall be independent of the primary control system. This includes also necessary Human Machine Interface (HMI) for effective local operation.

4.4.2.2 Rationale

Independent local controls of machinery and equipment needed to maintain safe operation is a fundamental principle for manned vessels. The objective of this requirement has traditionally been to ensure that personnel can cope with failures and other incidents by performing manual operations in close vicinity of the machinery. Since incidents caused by malicious cyber events should also be considered, this principle of independent local control is no less important.

4.4.2.3 Requirement details

The CBS for local control and monitoring shall be self-contained and not depend on communication with other CBS for its intended operation.

E26 (cont)

If communication to the remote control system or other CBS's is arranged by networks, segmentation and protection safeguards as described in 4.2.1 and 4.2.2 shall be implemented. This implies that the local control and monitoring system shall be considered a separate security zone. Notwithstanding the above, special considerations can be given to CBSs with different concepts on case by case basis

The CBS for local control and monitoring shall otherwise comply with requirements in this UR.

4.4.2.4 Demonstration of compliance

4.4.2.4.1 Design phase

The systems integrator shall include the following information in the Cyber security design description:

- Description of how the local controls specified in SOLAS II-1 Reg.31 are protected from cyber incidents in any connected remote or automatic control systems.

4.4.2.4.2 Construction phase

No requirements.

4.4.2.4.3 Commissioning phase

The systems integrator shall submit Ship cyber resilience test procedure (ref. section 5.2.1) and demonstrate to the Society that the required local controls in the scope of applicability of this UR needed for safety of the ship can be operated independently of any remote or automatic control systems. The tests shall be carried out by disconnecting all networks from the local control system to other systems/devices.

The above tests may be omitted if performed during the certification of CBSs as per section 5.2.1.

4.4.2.4.4 Operation phase

For general requirements to surveys in the operation phase, see section 5.3.

Special survey

Subject to modifications of the CBSs, the shipowner shall demonstrate to the Society the activities in section 4.4.2.4.3 as per the Ship cyber resilience test procedure.

4.4.3 Network isolation

4.4.3.1 Requirement

It shall be possible to terminate network-based communication to or from a security zone.

4.4.3.2 Rationale

In the event that a security breach has occurred and is detected, it is likely that the incident response plan includes actions to prevent further propagation and effects of the incident. Such actions could be to isolate network segments and control systems supporting essential functions.

E26 (cont)

4.4.3.3 Requirement details

Where the Incident Response Plan indicates network isolation as an action to be done, it shall be possible to isolate security zones according to the indicated procedure, e.g. by operating a physical ON/OFF switch on the network device or similar actions such as disconnecting a cable to the router/firewall. There shall be available instructions and clear marking on the device that allows the personnel to isolate the network in an efficient manner.

Individual system's data dependencies that may affect function and correct operation, including safety, shall be identified, clearly showing where systems must have compensations for data or functional inputs if isolated during a contingency.

4.4.3.4 Demonstration of compliance

4.4.3.4.1 Design phase

The systems integrator shall include the following information in the Cyber security design description:

- specification of how to isolate each security zone from other zones or networks. The effects of such isolation shall also be described, demonstrating that the CBSs in a security zone do not rely on data transmitted by IP-networks from other zones or networks.

4.4.3.4.2 Construction phase

No requirements.

4.4.3.4.3 Commissioning phase

The systems integrator shall submit Ship cyber resilience test procedure (ref. section 5.2.1) and demonstrate to the Society by disconnecting all networks traversing security zone boundaries, that the CBSs in the security zone will maintain adequate operational functionality without network communication with other security zones or networks.

The above tests may be omitted if performed during the certification of CBSs as per section 5.2.1.

4.4.3.4.4 Operation phase

For general requirements to surveys in the operation phase, see section 5.3.

Special survey

Subject to modifications of the CBSs, the shipowner shall demonstrate to the Society the activities in section 4.4.3.4.3 as per the Ship cyber resilience test procedure.

4.4.4 Fallback to a minimal risk condition

4.4.4.1 Requirement

In the event of a cyber incident impairing the ability of a CBS or network in the scope of applicability of this UR to provide its intended service, the affected system or network shall fall back to a minimal risk condition, i.e. bring itself in a stable, stopped condition to reduce the risk of possible safety issues.

E26 (cont)

4.4.4.2 Rationale

The ability of a CBS and integrated systems to fallback to one or more minimal risk conditions to be reached in case of unexpected or unmanageable failures or events is a safety measure aimed to keep the system in a consistent, known and safe state.

Fallback to a minimal risk condition usually implies the capability of a system to abort the current operation and signal the need for assistance, and may be different depending on the environmental conditions, the voyage phase of the ship (e.g. port depart/arrival vs. open sea passage) and the events occurred.

4.4.4.3 Requirement details

As soon as a cyber incident affecting the CBS or network is detected, compromising the system's ability to provide the intended service as required, the system shall fall back to a condition in which a reasonably safe state can be achieved. Fall-back actions may include:

- bringing the system to a complete stop or other safe state;
- disengaging the system;
- transferring control to another system or human operator;
- other compensating actions.

Fall-back to minimum risk conditions shall occur in a time frame adequate to keep the ship in a safe condition.

The ability of a system to fall back to a minimal risk condition shall be considered from the design phase by the supplier and the systems integrator.

4.4.4.4 Demonstration of compliance

4.4.4.4.1 Design phase

The systems integrator shall include the following information in the Cyber security design description:

- Specification of safe state for the control functions in the CBSs in the scope of applicability of this UR.

4.4.4.4.2 Construction phase

No requirements.

4.4.4.4.3 Commissioning phase

The systems integrator shall submit Ship cyber resilience test procedure (ref. section 5.2.1) and demonstrate to the Society that CBSs in the scope of applicability of this UR respond to cyber incidents in a safe manner (as per section 4.4.4.4.1), e.g. by maintaining its outputs to essential services and allowing operators to carry out control and monitoring functions by alternative means. The tests shall at least include denial of service (DoS) attacks and may be done together with related test in section 4.3.1.4.3.

E26 (cont)

The above tests may be omitted if performed during the certification of CBSs as per section 5.2.1.

4.4.4.4.4 Operation phase

For general requirements to surveys in the operation phase, see section 5.3.

Special survey

Subject to modifications of the CBSs, the shipowner shall demonstrate to the Society the activities in section 4.4.4.4.3 as per the Ship cyber resilience test procedure.

4.5 Recover

The requirements for the Recover functional element are aimed at the development and implementation of appropriate means supporting the ability to restore CBSs and networks onboard affected by cyber incidents.

4.5.1 Recovery plan

4.5.1.1 Requirement

A recovery plan shall be made by the shipowner to support restoring CBSs under the scope of applicability of this UR to an operational state after a disruption or failure caused by a cyber incident. Details of where assistance is available and by whom shall be part of the recovery plan.

4.5.1.2 Rationale

Incident response procedures are an essential part of system recovery. Responsible personnel should consider carefully and be aware of the implications of recovery actions (such as wiping of drives) and execute them carefully.

It should be noted, however, that some recovery actions may result in the destruction of evidence that could provide valuable information on the causes of an incident.

Where appropriate, external cyber incident response support should be obtained to assist in preservation of evidence whilst restoring operational capability.

4.5.1.3 Requirement details

The various stakeholders involved in the design and construction phases of the ship shall provide information to the shipowner for the preparation of the recovery plan to be placed onboard at the first annual Survey. The recovery plan shall be kept up-to-date (e.g. upon maintenance) during the operational life of the ship.

Recovery plans shall be easily understandable by the crew and external personnel and include essential instructions and procedures to ensure the recovery of a failed system and how to get external assistance if the support from ashore is necessary. In addition, software recovery medium or tools essential for recovery on board shall be available.

When developing recovery plans, the various systems and subsystems involved shall be specified. The following recovery objectives shall also be specified:

E26 (cont)

(l) System recovery: methods and procedures to recover communication capabilities shall be specified in terms of Recovery Time Objective (RTO). This is defined as the time required to recover the required communication links and processing capabilities.

(2) Data recovery: methods and procedures to recover data necessary to restore safe state of OT systems and safe ship operation shall be specified in terms of Recovery Point Objective (RPO). This is defined as the longest period of time for which an absence of data can be tolerated.

Once the recovery objectives are defined, a list of potential cyber incidents shall be created, and the recovery procedure developed and described. Recovery plans shall include, or refer to the following information;

(l) Instructions and procedures for restoring the failed system without disrupting the operation from the redundant, independent or local operation.

(2) Processes and procedures for the backup and secure storage of information.

(3) Complete and up-to-date logical network diagram.

(4) The list of personnel responsible for restoring the failed system.

(5) Communication procedure and list of personnel to contact for external technical support including system support vendors, network administrators, etc.

(6) Current configuration information for all components.

The operation and navigation of the ship shall be prioritized in the plan in order to help ensure the safety of onboard personnel.

Recovery plans in hard copy onboard and ashore shall be available to personnel responsible for cyber security and who are tasked with assisting in cyber incidents.

4.5.1.4 Demonstration of compliance

4.5.1.4.1 Design phase

The systems integrator shall include the following information in the Cyber security design description:

- references to information provided by the suppliers (see UR E27 section 3.1.8) that may be applied by the shipowner to establish plans to recover from cyber incidents.

4.5.1.4.2 Construction phase

No requirements.

4.5.1.4.3 Commissioning phase

The systems integrator shall submit Ship cyber resilience test procedure (ref. section 5.2.1) and demonstrate to the Society the effectiveness of the procedures and instructions provided by the suppliers to respond to cyber incidents as specified in section 4.5.2 and 4.5.3.

E26 (cont)

The above tests may be omitted if performed during the certification of CBSs as per section 5.2.1.

4.5.1.4.4 Operation phase

For general requirements to surveys in the operation phase, see section 5.3.

The shipowner shall in the Ship cyber security and resilience program describe incident recovery plans. The plans shall cover the CBSs in scope of applicability of this UR and shall address at least the following requirements in this UR:

- Description of who, when and how to restore and recover from cyber incidents in accordance with requirements in sections 4.5.1

- Policy for backup addressing frequency, maintenance and testing of the backups, considering acceptable downtime, availability of alternative means for control, vendor support arrangements and criticality of the CBSs in accordance with requirements in section 4.5.2.

- Reference to user manuals or procedures for backup, shutdown, reset, restore and restart of the CBSs in accordance with requirements in section 4.5.2 and 4.5.3.

First annual survey

The shipowner shall present to the Society records or other documented evidence demonstrating implementation of the Ship cyber security and resilience program, i.e., that:

- Instructions and/or procedures for incident recovery are available for the responsible personnel onboard.

- Equipment, tools, documentation, and/or necessary software and data needed for recovery is available for the responsible personnel onboard.

- Backup of the CBSs have been taken in accordance with the policies and procedures.

- Manuals and procedures for shutdown, reset, restore and restart are available for the responsible personnel onboard.

Subsequent annual surveys

The shipowner shall upon request by the Society demonstrate implementation of the Ship cyber security and resilience program by presenting records or other documented evidence as specified for the first annual survey.

4.5.2 Backup and restore capability

4.5.2.1 Requirement

CBSs and networks in the scope of applicability of this UR shall have the capability to support back-up and restore in a timely, complete and safe manner. Backups shall be regularly maintained and tested.

E26 (cont)

4.5.2.2 Rationale

In general, the purpose of a backup and restore strategy should protect against data loss and reconstruct the database after data loss. Typically, backup administration tasks include the following: Planning and testing responses to different kinds of failures; Configuring the database environment for backup and recovery; Setting up a backup schedule; Monitoring the backup and recovery environment; Creating a database copy for long-term storage; Moving data from one database or one host to another, etc.

4.5.2.3 Requirement details

4.5.2.3.1 Restore capability

CBSs in the scope of applicability of this UR shall have backup and restore capabilities to enable the ship to safely regain navigational and operational state after a cyber incident.

Data shall be restorable from a secure copy or image.

Information and backup facilities shall be sufficient to recover from a cyber incident.

4.5.2.3.2 Backup

CBSs and networks in the scope of applicability of this UR shall provide backup for data. The use of offline backups shall also be considered to improve tolerance against ransomware and worms affecting online backup appliances.

Backup plans shall be developed, including scope, mode and frequency, storage medium and retention period.

4.5.2.4 Demonstration of compliance

4.5.2.4.1 Design phase

No requirements.

4.5.2.4.2 Construction phase

No requirements.

4.5.2.4.3 Commissioning phase

The systems integrator shall submit Ship cyber resilience test procedure (ref. section 5.2.1) and demonstrate to the Society the procedures and instructions for backup and restore provided by the suppliers for CBSs in the scope of applicability of this UR.

The above tests may be omitted if performed during the certification of CBSs as per section 5.2.1.

4.5.2.4.4 Operation phase

For general requirements to surveys in the operation phase, see section 5.3.

E26 (cont)

Special survey

Subject to modifications of the CBSs, the shipowner shall demonstrate to the Society the activities in section 4.5.2.4.3 as per the Ship cyber resilience test procedure.

4.5.3 Controlled shutdown, reset, roll-back and restart

4.5.3.1 Requirement

CBS and networks in the scope of applicability of this UR shall be capable of controlled shutdown, reset to an initial state, roll-back to a safe state and restart from a power-off condition in such state, in order to allow fast and safe recovery from a possible impairment due to a cyber incident.

Suitable documentation on how to execute the above-mentioned operations shall be available to onboard personnel.

4.5.3.2 Rationale

Controlled shutdown consists in turning a CBS or network off by software function allowing other connected systems to commit/rollback pending transactions, terminating processes, closing connections, etc. leaving the entire integrated system in a safe and known state. Controlled shutdown is opposed to hard shutdown, which occurs for example when the computer is forcibly shut down by interruption of power.

While in the case of some cyber incidents hard shutdowns may be considered as a safety precaution, controlled shutdown is preferable in case of integrated systems to keep them in a consistent and known state with predictable behaviour. When standard shutdown procedures are not done, data or program and operating system files corruption may occur. In case of OT systems, the result of corruption can be instability, incorrect functioning or failure to provide the intended service.

The reset operation would typically kick off a soft boot, instructing the system to go through the process of shutting down, clear memory and reset devices to their initialized state. Depending on system considered, the reset operation might have different effects.

Rollback is an operation which returns the system to some previous state. Rollbacks are important for data and system integrity, because they mean that the system data and programs can be restored to a clean copy even after erroneous operations are performed. They are crucial for recovering from crashes ad cyber incidents, restoring the system to a consistent state.

Restarting a system and reloading a fresh image of all the software and data (e.g. after a rollback operation) from a read-only source appears to be an effective approach to recover from unexpected faults or cyber incidents. Restart operations should be however controlled in particular for integrated systems, where unexpected restart of a single component can result in inconsistent system state or unpredictable behaviour.

4.5.3.3 Requirement details

CBS and networks in the scope of applicability of this UR shall be capable of:

- controlled shutdown allowing other connected systems to commit/rollback pending transactions, terminating processes, closing connections, etc. leaving the entire integrated system in a safe, consistent and known state.

E26 (cont)

- resetting themselves, instructing the system to go through the process of shutting down, clear memory and reset devices to their initialized state.

- rolling back to a previous configuration and/or state, to restore system integrity and consistency.

- restarting and reloading a fresh image of all the software and data (e.g. after a rollback operation) from a read-only source. Restart time shall be compatible with the system's intended service and shall not bring other connected systems, or the integrated system it is part of, to an inconsistent or unsafe state.

Documentation shall be available to onboard personnel on how to execute the above-mentioned operations in case of a system affected by a cyber incident.

4.5.3.4 Demonstration of compliance

4.5.3.4.1 Design phase

The systems integrator shall include the following information in the Cyber security design description:

- references to product manuals or procedures describing how to safely shut down, reset, restore and restart the CBSs in the scope of applicability of this UR.

4.5.3.4.2 Construction phase

No requirements.

4.5.3.4.3 Commissioning phase

The systems integrator shall submit Ship cyber resilience test procedure (ref. section 5.2.1) and demonstrate to the Society that manuals or procedures are established for shutdown, reset and restore of the CBSs in the scope of applicability of this UR. These manuals/procedures shall be provided to the shipowner.

The above tests may be omitted if performed during the certification of CBSs as per section 5.2.1.

4.5.3.4.4 Operation phase

For general requirements to surveys in the operation phase, see section 5.3.

Special survey

Subject to modifications of the CBSs, the shipowner shall demonstrate to the Society the activities in section 4.5.3.4.3 as per the Ship cyber resilience test procedure.

E26 (cont)

5. Demonstration of compliance

Evaluation of compliance with requirements in this UR shall be carried out by the Society by assessment of documentation and survey in the relevant phases as specified in the following subsections.

Documentation to be submitted by suppliers to the Society is specified in UR E27. The approved versions of this documentation shall also be provided by the suppliers to the systems integrator as specified in UR E27 section 6.2

Documents to be provided by the systems integrator are listed in section 5.1 and 5.2.

Documents to be provided by the shipowner are listed in section 5.3.

Upon delivery of the ship, the systems integrator shall provide below documentation to the shipowner:

- Documentation of the CBSs provided by the suppliers (see UR E27 section 6.2)
- Documentation produced by the systems integrator (see sections 5.1 and 5.2)

See also appendix I and appendix II for a summary of the documents.

5.1 During design and construction phases

The supplier shall demonstrate compliance to the Society by following the certification process specified in UR E27 section 6.

The systems integrator shall demonstrate compliance by submitting documents in the following subsections to the Society for assessment.

During the design and construction phases, modifications to the design shall be carried out in accordance with the management of change (MoC) requirements in UR E22.

5.1.1 Zones and conduit diagram

The content of this document is specified in section 4.2.1.4.1.

5.1.2 Cyber security design description (CSDD)

The content of this document is specified in subsections “Design phase” for each requirement in section 4.

5.1.3 Vessel asset inventory

The content of this document is specified in section 4.1.1.

5.1.4 Risk assessment for the exclusion of CBSs

The content of this document is specified in section 6.

E26 (cont)

5.1.5 Description of compensating countermeasures

If any CBS in the scope of applicability of this UR has been approved with compensating countermeasures in lieu of a requirement in UR E27, this document shall specify the respective CBS, the lacking security capability, as well as provide a detailed description of the compensating countermeasures. See also UR E27 section 3.1.3 requiring that the supplier describes such compensating countermeasures in the system documentation.

5.2 Upon ship commissioning

Before final commissioning of the ship, the systems integrator shall:

1. Submit updated design documentation to the Society (as-built versions of the documents in section 5.1)

2. Submit Ship cyber resilience test procedure to the Society describing how to demonstrate compliance with this UR by testing and/or analytic evaluation.

3. Carry out testing, witnessed by the Society, in accordance with the approved Ship cyber resilience test procedure.

5.2.1 Ship cyber resilience test procedure

The content of this document is specified for the Commissioning phase in each subsection “Demonstration of compliance” in section 4.

For each CBS, the required inherent security capabilities and configuration thereof are verified and tested in the certification process of each CBS (see UR E27). Testing of such security functions may be omitted if specified in the respective subsection "Commissioning phase", on the condition that these security functions have been successfully tested during the certification of the CBS as per UR E27. Nevertheless, all tests shall be included in the Ship cyber resilience test procedure and the decision to omit tests will be taken by the Society. Tests may generally not be omitted if findings/comments are carried over from the certification process to the commissioning phase, if the respective requirements have been met by compensating countermeasures, or due to other reasons such as modifications of the CBS after the certification process.

The Ship cyber resilience test procedure shall also specify how to test any compensating countermeasures described in section 5.1.2.

The Ship cyber resilience test procedure shall include means to update status and record findings during the testing, and specify the following information:

- 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

E26 (cont)

Before submitting the Ship cyber resilience test procedure to the Society, the systems integrator shall verify that the information is updated and placed under change management; that it is aligned with the latest configurations of CBSs and networks connecting such systems together onboard the ship and to other CBSs not onboard (e.g., ashore); and that the tests documented are sufficiently detailed as to allow verification of the installation and operation of measures adopted for the fulfilment of relevant requirements on the final configuration of CBSs and networks onboard.

The systems integrator shall document verification tests or assessments of security controls and measures in the fully integrated ship, maintaining change management for configurations, and noting in the documented test results where safety conditions may be affected by specific circumstances or failures addressed in the Ship cyber resilience test procedure.

The testing shall be carried out on board in accordance with the approved Ship cyber resilience test procedure after other commissioning activities for the CBSs are completed. The Society may request execution of additional tests.

5.3 During the operational life of the ship

After the ship has been delivered to the shipowner, the shipowner shall manage technical and organisational security countermeasures by establishing and implementing processes as specified in this UR.

Modifications to the CBSs in scope of applicability of this UR shall be carried out in accordance with the management of change (MoC) requirements in UR E22. This includes keeping documentation of the CBSs up to date.

The shipowner, with the support of suppliers, shall keep the Ship cyber resilience test procedure up to date and aligned with the CBSs onboard the ship and the networks connecting such systems to each other and to other CBSs not onboard (e.g. ashore). The shipowner shall update the Ship cyber resilience test procedure considering the changes occurred on CBSs and networks onboard, possible emerging risks related to such changes, new threats, new vulnerabilities and other possible changes in the ship’s operational environment.

The shipowner shall prepare and implement operational procedures, provide periodic training and carry out drills for the onboard personnel and other concerned personnel ashore to familiarize them with the CBSs onboard the ship and the networks connecting such systems to each other and to other CBSs not onboard (e.g. ashore), and to properly manage the measures adopted for the fulfilment of requirements.

The shipowner, with the support of supplier, shall keep the measures adopted for the fulfilment of requirements up to date, e.g. by periodic maintenance of hardware and software of CBSs onboard the ship and the networks connecting such systems.

The shipowner shall retain onboard a copy of results of execution of tests and an updated Ship cyber resilience test procedure and make them available to the Classification Society.

5.3.1 First annual survey

In due time before the first annual survey of the ship, the shipowner shall submit to the Society a Ship cyber security and resilience program documenting management of cyber security and cyber resilience of the CBSs in the scope of applicability of this UR.

E26 (cont)

The Ship cyber security and resilience program shall include policies, procedures, plans and/or other information documenting the processes/activities specified in subsections “Demonstration of compliance” in section 4 of this UR.

After the Society has approved the Ship cyber security and resilience program, the shipowner shall in the first annual survey demonstrate compliance by presenting records or other documented evidence of implementation ofthe processes described in the approved Ship cyber security and resilience program.

Change of vessel management company will require a new verification of the Ship cyber security and resilience program.

5.3.2 Subsequent annual surveys

In the subsequent annual surveys of the ship, the shipowner shall upon request by the Society demonstrate implementation of the Ship cyber security and resilience program.

5.3.3 Special survey

Upon renewal of the ship’s classification certificate, the shipowner shall carry out testing witnessed by the Society in accordance with the Ship cyber resilience test procedure. Certain security safeguards shall be demonstrated at Special survey whereas other need only be carried out upon request by the Society based on modifications to the CBSs as specified in subsections “Operation phase” in section 4 of this UR.

E26 (cont)

6 Risk assessment for exclusion of CBS from the application of requirements

6.1 Requirement

A risk assessment shall be carried out in case any of the CBSs falling under the scope of applicability of this UR is excluded from the application of relevant requirements. The risk assessment shall provide evidence of the acceptable risk level associated to the excluded CBSs.

6.2 Rationale

Exclusion of a CBS falling under the scope of applicability of this UR from the application of relevant requirements needs to be duly justified and documented. Such exclusion can be accepted by the Classification Society only if evidence is given that the risk level associated to the operation of the CBS is under an acceptable threshold by means of specific risk assessment.

The risk assessment shall be based on available knowledge bases and experience on similar designs, if any, considering the CBS category, connectivity and the functional requirements and specifications of the ship and of the CBS. Cyber threat information from internal and external sources may be used to gain a better understanding of the likelihood and impact of cybersecurity events.

6.3 Requirement details

Risk assessment shall be made and kept up to date by the System integrator during the design and building phase considering possible variations of the original design and newly discovered threats and/or vulnerabilities not known from the beginning.

During the operational life of the ship, the shipowner shall update the risk assessment considering the constant changes in the cyber scenario and new weaknesses identified in CBS onboard in a process of continuous improvement. Should new risks be identified, the shipowner shall update existing, or implement new risk mitigation measures.

Should the changes in the cyber scenario be such as to elevate the risk level associated to the CBS under examination above the acceptable risk threshold, the shipowner shall inform the Classification Society and submit the updated risk assessment for evaluation.

The envisaged operational environments for the CBS under examination shall be analyzed in the risk assessment to discern the likelihood of cyber incidents and the impact they could have on the human safety, the safety of the vessel or the marine environment, taking into account the category of the CBS. The attack surface shall be analyzed, taking into account the connectivity of the CBS, possible interfaces for portable devices, logical access restrictions, etc.

Emerging risks related to the specific configuration of the CBS under examination shall be also identified. In the risk assessment, the following elements shall be considered:

- Asset vulnerabilities;
- Threats, both internal and external;

E26 (cont)

- Potential impacts of cyber incidents affecting the asset on human safety, safety of the vessel and/or threat to the environment;
- Possible effects related to integration of systems, or interfaces among systems, including systems not onboard (e.g. if remote access to onboard systems is provided).

6.4 Acceptance criteria

Exclusion of a CBS falling under the scope of applicability of this UR from the application of relevant requirements can be accepted by the Classification Society only if assurance is given that the operation of the CBS has no impact on the safety of operations regarding cyber risk. The said exclusion may be accepted for a CBS which does not fully meet the additional criteria listed below but is provided with a rational explanation together with evidence and is found satisfactory by the Classification Society. The Classification Society may also require submittal of additional documents to consider the said exclusion.

The following criteria shall be met to exclude a system from the scope of applicability of this UR:

a) The CBS shall be isolated (i.e, have no IP-network connections to other systems or networks)

b) The CBS shall have no accessible physical interface ports. Unused interfaces shall be logically disabled. It shall not be possible to connect unauthorised devices to the CBS

c) The CBS must be located in areas to which physical access is controlled

d) The CBS shall not be an integrated control system serving multiple ship functions as specified in the scope of applicability of this UR (see section 1.3)

The following additional criteria should be considered for the evaluation of risk level acceptability:

a) The CBS should not serve ship functions of category III ;

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

c) The attack surface for the CBS is minimized, having considered its complexity, connectivity, physical and logical access points, including wireless access points;

E26
(cont)

Appendix I – Summary of actions and documents

Legend:

Submit	The stakeholder shall submit the document to the Class society for verification and approval of compliance with requirements in this UR
Maintain	The stakeholder shall keep the document updated in accordance with procedure for management of change (MoC). Updated document and change management records shall be submitted to the Class society as per UR E22.
Demonstrate	The stakeholder shall demonstrate compliance to the Class society in accordance with the approved document.
1st AS	First annual survey
AS	Annual survey
SS	Special survey

E26 (cont)

Document (E26)	Systems integrator			Shipowner			
	Design	Construction	Commissioning	Operation	1st AS	AS	SS
Approved supplier documentation [5]		Maintain	Maintain	Maintain			
Zones and conduit diagram [5.1.1]	Submit	Maintain	Maintain	Maintain			
Cyber security design description [5.1.2]	Submit	Maintain	Maintain	Maintain			
Vessel asset inventory [5.1.3]	Submit	Maintain	Maintain	Maintain			
Risk assessment for the exclusion of CBSs [5.1.4] NOTE 1	Submit	Maintain	Maintain	Maintain			
Description of compensating countermeasures [5.1.5] NOTE 1	Submit	Maintain	Maintain	Maintain			
Ship cyber resilience test procedure [5.2.1]		Submit	Demonstrate	Maintain			Demonstrate
Ship cyber security and resilience program [5.3.1] - Management of change (MoC) [4.1.1.4.4] - Management of software updates [4.1.1.4.4] - Management of firewalls [4.2.1.4.4] - Management of malware protection [4.2.3.4.4] - Management of access control [4.2.4.4.4] - Management of confidential information [4.2.4.4.4] - Management of remote access [4.2.6.4.4] - Management of mobile and portable devices [4.2.7.4.4] - Detection of security anomalies [4.3.1.4.4] - Verification of security functions [4.3.2.4.4] - Incident response plans [4.4.1.4.4] - Recovery plans [4.5.1.4.4]				Maintain	Submit	Demonstrate	
NOTE 1: If applicable							

E26 (cont) Appendix II – Summary of requirements and documents

Vessel asset inventory (section 4.1.1)		
CBS security capabilities	Provide documentation of product security updates Provide documentation of dependent component security updates Provide security updates	E27 (5.2) E27 (5.3) E27 (5.4)
CBS documentation	CBS asset inventory Management of change plan	E27 (3.1.1) E27 (3.1.9)
Vessel design documentation	Vessel asset inventory	E26 (4.1.1.4.1)
Ship cyber security and resilience program	Management of change	E26 (4.1.1.4.4)
	Management of software updates	E26 (4.1.1.4.4)

Security zones and network segmentation (section 4.2.1)		
CBS security capabilities		
CBS documentation	Topology diagrams	E27 (3.1.2)
Vessel design documentation	Zones and conduit diagram Design description Ship cyber resilience test procedure	E26 (4.2.1.4.1) E26 (4.2.1.4.1) E26 (4.2.1.4.3)
Ship cyber security and resilience program	Management of security zone boundary devices (e.g., firewalls)	E26 (4.2.1.4.4)

Network protection safeguards (section 4.2.2)		
CBS security capabilities	Denial of service (DoS) protection (item 24) Deterministic output (item 20)	E27 (4.1)
CBS documentation	Description of security capabilities Test procedure for security capabilities	E27 (3.1.3) E27 (3.1.4)
Vessel design documentation	Ship cyber resilience test procedure	E26 (4.2.2.4.3)
Ship cyber security and resilience program		

E26
(cont)

Antivirus, antimalware, antispam and other protections from malicious code (section 4.2.3)		
CBS security capabilities	Malicious code protection (#18)	E27 (4.1)
CBS documentation	Description of security capabilities Test procedure for security capabilities	E27 (3.1.3) E27 (3.1.4)
Vessel design documentation	Design description Ship cyber resilience test procedure	E26 (4.2.3.4.1) E26 (4.2.3.4.3)
Ship cyber security and resilience program	Management of malware protection	E26 (4.2.3.4.4)

Access control (section 4.2.4)		
CBS security capabilities	Human user id. and auth. (#1) Account management (#2) Identifier management (#3) Authenticator management (#4) Authorisation enforcement (#8)	E27 (4.1)
CBS documentation	Description of security capabilities Test procedure for security capabilities	E27 (3.1.3) E27 (3.1.4)
Vessel design documentation	Design description Ship cyber resilience test procedure	E26 (4.2.4.4.1) E26 (4.2.4.4.3)
Ship cyber security and resilience program	Management of confidential information	E26 (4.2.4.4.4)
	Management of logical and physical access	E26 (4.2.4.4.4)

Wireless communication (section 4.2.5)		
CBS security capabilities	Wireless access management (#5) Wireless use control (#9)	E27 (4.1)
CBS documentation	Description of security capabilities Test procedure for security capabilities	E27 (3.1.3) E27 (3.1.4)
Vessel design documentation	Design description Ship cyber resilience test procedure	E26 (4.2.5.4.1) E26 (4.2.5.4.3)
Ship cyber security and resilience program		

E26
(cont)

Remote access control and communication with untrusted networks (section 4.2.6)		
CBS security capabilities	Multifactor authentication (#31) Process / device id. and auth. (#32) Unsuccessful login attempts (#33) System use notification (#34) Access via untrusted networks (#35) Explicit access request approval (#36) Remote session termination (#37) Cryptographic integrity protection (#38) Input validation (#39) Session integrity (#40) Invalidation of session ID (#41)	E27 (4.2)
CBS documentation	Description of security capabilities Test procedure for security capabilities	E27 (3.1.3) E27 (3.1.4)
Vessel design documentation	Design description Ship cyber resilience test procedure	E26 (4.2.6.4.1) E26 (4.2.6.4.3)
Ship cyber security and resilience program	Management of remote access and communication with/via untrusted networks	E26 (4.2.6.4.4)

Use of mobile and portable devices (section 4.2.7)		
CBS security capabilities	Use control for portable devices (#10)	E27 (4.1)
CBS documentation	Description of security capabilities Test procedure for security capabilities	E27 (3.1.3) E27 (3.1.4)
Vessel design documentation	Design description Ship cyber resilience test procedure	E26 (4.2.7.4.1) E26 (4.2.7.4.3)
Ship cyber security and resilience program	Management of mobile and portable devices	E26 (4.2.7.4.4)

E26
(cont)

Network operation monitoring (section 4.3.1)		
CBS security capabilities	Use control for portable devices (#10) Auditable events (#13) Denial of service (DoS) protection (#24)	E27 (4.1)
	Alarm excessive bandwidth use	E22 (7.2.1)
CBS documentation	Description of security capabilities Test procedure for security capabilities	E27 (3.1.3) E27 (3.1.4)
Vessel design documentation	Ship cyber resilience test procedure	E26 (4.3.1.4.3)
Ship cyber security and resilience program	Incident response plans	E26 (4.3.1.4.4)

Verification and diagnostic functions of CBS and networks (section 4.3.2)		
CBS security capabilities	Security function verification (#19)	E27 (4.1)
CBS documentation	Description of security capabilities Test procedure for security capabilities Plans for maintenance and verification	E27 (3.1.3) E27 (3.1.4) E27 (3.1.7)
Vessel design documentation	Ship cyber resilience test procedure	E26 (4.3.2.4.3)
Ship cyber security and resilience program	Verification of security functions	E26 (4.3.2.4.4)

Incident response plan (section 4.4.1)		
CBS security capabilities		
CBS documentation	Description of security capabilities Test procedure for security capabilities Information supporting incident response and recovery plans	E27 (3.1.3) E27 (3.1.4) E27 (3.1.8)
Vessel design documentation	Design description Ship cyber resilience test procedure	E26 (4.4.1.4.1) E26 (4.4.1.4.3)
Ship cyber security and resilience program	Incident response plans	E26 (4.4.1.4.4)

E26
(cont)

Local, independent and/or manual operation (section 4.4.2)		
CBS security capabilities		
CBS documentation	Description of security capabilities Test procedure for security capabilities Information supporting incident response and recovery plans	E27 (3.1.3) E27 (3.1.4) E27 (3.1.8)
Vessel design documentation	Design description Ship cyber resilience test procedure	E26 (4.4.2.4.1) E26 (4.4.2.4.3)
Ship cyber security and resilience program	Incident response plans	E26 (4.4.1.4.4)

Network isolation (section 4.4.3)		
CBS security capabilities		
CBS documentation	Description of security capabilities Test procedure for security capabilities Information supporting incident response and recovery plans	E27 (3.1.3) E27 (3.1.4) E27 (3.1.8)
Vessel design documentation	Design description Ship cyber resilience test procedure	E26 (4.4.3.4.1) E26 (4.4.3.4.3)
Ship cyber security and resilience program	Incident response plans	E26 (4.4.1.4.4)

Fallback to a minimal risk condition (section 4.4.4)		
CBS security capabilities	Deterministic output (#20)	E27 (4.1)
CBS documentation	Description of security capabilities Test procedure for security capabilities Information supporting incident response and recovery plans	E27 (3.1.3) E27 (3.1.4) E27 (3.1.8)
Vessel design documentation	Design description Ship cyber resilience test procedure	E26 (4.4.4.4.1) E26 (4.4.4.4.3)
Ship cyber security and resilience program	Incident response plans	E26 (4.4.1.4.4)

E26
(cont)

Recovery plan (section 4.5.1)		
CBS security capabilities		
CBS documentation	Description of security capabilities Test procedure for security capabilities Information supporting incident response and recovery plans	E27 (3.1.3) E27 (3.1.4) E27 (3.1.8)
Vessel design documentation	Design description Ship cyber resilience test procedure	E26 (4.5.1.4.1) E26 (4.5.1.4.3)
Ship cyber security and resilience program	Recovery plans	E26 (4.5.1.4.4)

Backup and restore capability (section 4.5.2)		
CBS security capabilities	System backup (#26) System recovery and reconstitution (#27)	E27 (4.1)
CBS documentation	Description of security capabilities Test procedure for security capabilities Information supporting incident response and recovery plans	E27 (3.1.3) E27 (3.1.4) E27 (3.1.8)
Vessel design documentation	Ship cyber resilience test procedure	E26 (4.5.2.4.3)
Ship cyber security and resilience program	Recovery plan	E26 (4.5.1.4.4)

Controlled shutdown, reset, restore and restart (section 4.5.3)		
CBS security capabilities	System recovery and reconstitution (#27)	E27 (4.1)
CBS documentation	Description of security capabilities Test procedure for security capabilities Information supporting incident response and recovery plans	E27 (3.1.3) E27 (3.1.4) E27 (3.1.8)
Vessel design documentation	Design description Ship cyber resilience test procedure	E26 (4.5.3.4.1) E26 (4.5.3.4.3)
Ship cyber security and resilience program	Recovery plans	E26 (4.5.1.4.4)

E26
(cont)

Risk assessment for exclusion of CBS from the application of requirements (section 6)		
CBS security capabilities		
CBS documentation		
Vessel design documentation	Risk assessment for the exclusion of CBSs	E26 (5.1.4)
Ship cyber security and resilience program		

End of document