E26 Cyber resilience of ships

(Apr 2022)

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 Test plan for performance evaluation and testing 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: Summary of Actions and Documents

Note:

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

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

E26
(cont)

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.

As long as on-board systems and equipment are part of a computer-based systems in the scope of applicability of this UR and are not considered as individual entities, for such systems and equipment more stringent requirements than those enforced in IACS UR E27 may be required as per IACS UR E27 additional system requirements to support the fulfilment of this UR.

1.3 Scope of applicability

This UR applies to:

a) Operational Technology (OT) systems onboard ships, i.e. those computer-based systems (CBS) 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
- Cargo handling system (limited to safety-related elements)
- Bilge and ballast systems, loading/unloading control systems, loading computer
- Boiler control system
- Scrubber control system and other systems needed for compliance with class or international regulations to prevent pollution to the environment
- Watertight integrity and flooding detection
- Lighting (e.g. emergency lighting, low locations, navigation lights, etc.)
- Any other OT system whose disruption or functional impairing may pose risks to ship operations (e.g. LNG monitoring and control system, relevant 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, standard such as IEC 61162-460 or IEC 63154 can be used as alternatives to this UR, as long as the application of such standards

E26 (cont)

provides equivalent or greater cyber resilience as obtained from the application of the requirements contained in this UR. In any case, requirements under section 4 shall be 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
- 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.

1.3.1 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.

1.3.2 IACS Documents on Computer Based Systems and Cyber Resilience

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

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

IACS UR 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:

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

Authentication: Provision of assurance that a claimed characteristic of an 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.

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

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.

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

Demilitarized zone (DMZ): A physical or logical perimeter network segment that contains and exposes an organization's external-facing services to an external network. Its purpose is to enforce the internal network's security policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the internal networks from outside attacks.

Essential System: Computer Based System contributing to the provision of services essential for propulsion and steering, and safety of the ship. Essential services comprise

E26 (cont)

"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).

Initial Authenticator Content: Factory default authentication credentials (e.g.: initial passwords, tokens, etc.) to allow for initial installation and configuration of system.

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

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

Note on TCP/IP: Logical networks are hosted on the same physical network but segmented and managed at the data link or network layers (OSI Layer 2 and 3).

Network segment: A collection of nodes that share the same network address plan. A network segment is 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". The physical components are not shared by other network segments.

Note on TCP/IP: Segmentation breaks networks down into multiple physical segments or subnets. The incoming and outgoing packets are controlled. The connections and data exchanges are allowed or blocked at both network layer (OSI Layer 3) and application level (OSI Layer 7). Both traffic management and packet filtering can be managed by a single software or hardware equipment.

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 connected CBSs in the scope of applicability of this UR that require the same access control policy. Each zone consists of a single interface or a group of interfaces, to which an access control policy is applied.

Ship Designer/Shipyard: The person or organization:

- implementing the process of evolving the ship specifications given by the Shipowner into a complete ship project, including management of concept, contract and detail design, and/or

E26 (cont)

- in charge of ship construction and responsible for fulfilling during ship construction the requirements of applicable rules and regulations and implementing the specifications of ship design, and/or

- responsible for the integration of systems and products provided by Suppliers into an integrated system.

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 Owner could be the Shipyard or System Integrator (Builder or Shipyard) during initial construction. After vessel delivery, the owner may delegate some responsibilities to the vessel operating company.

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

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

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

Virtual Private Network (VPN): A virtual network, built on top of existing physical networks, that provides a secure communications tunnel for data transmitted between networks or devices utilizing tunnelling, security controls and endpoint address translation giving the impression of a dedicated line.

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. Criteria for performance evaluation and testing are also given.

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 under the responsibility of 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
- Ship Designer/Shipyard
- System Integrator
- Supplier
- 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 Inventory of CBSs and networks onboard

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 inventory of CBSs onboard shall include at least the CBSs indicated in 1.3 a) and b), if present onboard.

The inventory shall be 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.

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.

E26
(cont)

4.1.1.3.1 Hardware

For hardware, the inventory shall contain at least the following information:

1. For each CBS, a short description of its purpose with brief functional description and technical features (brand, manufacturer, model, main technical data);

2. A block diagram identifying the logical and physical connections among various CBSs onboard and between CBSs and external devices or networks, the topology of networks connecting CBSs and the intended function of each node;

3. For network devices such as switches, routers, hubs, gateways etc., a description of the connected subnetworks, IP ranges, MAC addresses of nodes connected (or addresses/identifiers specific to the protocols used in the network)

4. The main features of each network (e.g. protocols used) and communication data flows (e.g. data flow diagram) in all intended operation modes;

5. A map describing the physical layout of each digital network connecting the CBSs onboard, including the physical location of the CBSs onboard and the physical location of network access points.

Based on the information above, a system category and security zone may also be associated to the CBS and recorded in the inventory.

4.1.1.3.2 Software

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

1. The CBS where it is installed, a short description of its purpose, technical features (brand, manufacturer, model, main technical data) and specific function;

2. Version information, license information with initial installation and expiration dates and a log of updates;

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

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

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

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 control policy and security capabilities. Security zones shall either be isolated (i.e. air gapped) or connected to other security zones or networks by means

E26 (cont)

providing control of data communicated between the zones (e.g. firewalls/routers, simplex serial links, TCP/IP diodes, dry contacts, etc.)

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 the 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 systems 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.

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

Other OT-systems or CBSs outside the scope of applicability of this UR shall be physically segmented from security zones required by this UR. Alternatively, it is accepted that other OT-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 manually isolate a security zone without affecting the primary functionality of the CBSs in the zone.

In the definition of security control policies, the functions allowed to access or operate on the network shall be associated to technical procedures and roles.

4.2.2 Network protection safeguards

4.2.2.1 Requirement:

Networks connecting CBSs in the scope of applicability of this UR 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

E26
(cont)

use of non-essential functions, where unnecessary functions, ports, protocols and services are disabled or otherwise prohibited.

4.2.2.2 Rationale:

Network protection covers a multitude of technologies, rules and configurations designed to protect the integrity, confidentiality and availability of computer 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 for limiting data flow rate 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.

4.2.3 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 all the malicious intruding viruses performing a prophylactic function. It detects any 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 anti-malware software shall be installed, maintained and regularly updated, unless the installation of such software impairs

E26 (cont)

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.

4.2.4 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. shall 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. The requirements in this article may be considered as the technical foundation for instructions and procedures deriving from the application of ISPS and ISM Code.

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, authorized processes and devices, 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 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, maintenance, repair, replacement, disposal etc. so as not to hamper effective and efficient operation of the ship.

4.2.4.3.2 Physical access control for visitors

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

E26
(cont)

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.

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 allowing full access to system configuration settings and all data shall only be given to appropriately trained personnel, who as part of their role in the company or onboard, need to log onto systems using these privileges. Administrator privileges shall be removed when the person concerned is no longer onboard. In any case, use of administrator privileges shall always be limited to functions requiring such access.

4.2.4.3.6 Least privilege policy

Any user, program, or process 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. Processes having access to systems and networks onboard shall operate at privilege levels no higher than necessary to accomplish their intended task.

The default configuration for all new account or process 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 and process accounts.

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:

E26 (cont)

- 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).

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.

4.2.6 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 a lot cyber resilience,

E26 (cont)

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 application of this UR, no IP address shall be exposed to untrusted networks. It shall not be possible to route packets directly to security zones from 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.

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.

- Patches and 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.

- A support plan shall be developed and made available to all stakeholders involved.

- 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.

E26 (cont)

- When an access attempt is failed, next attempt is not to be started for a predetermined length of time. When the number of failed access attempts reached to a predetermined value, the authentication function shall be blocked.

- 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.

4.2.7 Use of Mobile and Portable Devices

4.2.7.1 Requirement:

The connection of mobile and portable devices to CBSs in the scope of applicability of this UR and of the networks connecting such systems shall be physically or logically blocked except when connecting for operation of the ship or maintenance.

Wireless connected mobile and portable devices shall be compliant with requirements of 4.2.5.

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 shall be carefully considered. In addition, mobile equipment that is required to be used for the operation and maintenance of the ship shall be under the control of the Shipowner.

4.2.7.3 Requirement details

Mobile and portable devices for ship's operational use shall be recorded on inventory list. When mobile and portable devices are used for maintenance, it is necessary to describe the maintenance information in the inventory list. Information about connection ports for mobile and portable devices equipped in CBSs shall be included in the inventory list, including the connection ports used for maintenance.

Blockers for removable media shall be used on physically accessible computers and network ports other than independent computers mentioned in 4.2.4.3.3.

For connection ports for mobile and portable devices used for onboard operation by the ship's crew or for maintenance by the supplier, measures shall be taken to prevent connection other than the predetermined equipment. Information about the connection ports shall be included in inventory list.

Ports to which physical or logical blocks have been applied shall be clearly indicated.

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.

E26
(cont)

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
- Monitoring or protection against connection of unauthorized devices

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

4.3.2 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 security functions during test and maintenance phases of the ship.

Diagnostic functions continuously monitoring excessive network traffic as well as status of network connections and devices during normal operation of the CBS and related networks shall be implemented. Diagnostic functions shall alert the responsible crew if anomalies are detected.

E26
(cont)

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 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 shall be integrated with the ship in the event of a cyber incident.

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;

E26 (cont)

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

4.4.2 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 shall 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.

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.

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

4.4.3 Network isolation

4.4.3.1 Requirement:

It shall be possible to manually or automatically terminate network-based communication to or from a network segment.

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.

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 physical network segments 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.

E26 (cont)

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.

4.4.4 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.

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;
- 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 Shipyard / Ship Designer / System Integrator.

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 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.

E26
(cont)

4.5.1.2 Rationale:

Incident response procedures are an essential part of system recovery. Responsible personnel shall 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, professional cyber incident response support shall 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:

(1) 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;

(1) 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.

E26 (cont)

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.

4.5.2 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.

4.5.2.2 Rationale:

In general, the purpose of a backup and restore strategy shall 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 quickly and 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.

4.5.3 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.

E26 (cont)

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 shall 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.

- 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.

E26
(cont)

5. Test Plan for performance evaluation and testing

Performance evaluation and testing are aimed to verify the effective implementation of measures adopted for the fulfilment of requirements in this UR.

Performance evaluation and testing are mainly based on the design, development, maintenance and implementation of a Test Plan, which is the essential instrument intended to support and ground testing and verification activities. It evolves during different phases of the ship's life and involves different stakeholders.

The Test Plan shall be used as an instrument and a reference for the verification of the actual and effective implementation of measures adopted for the fulfilment of requirements in this UR. Additional or alternative tests may also be executed. Simulated cyber incidents can be intentionally induced for testing purposes.

This section indicates how the Test Plan shall be designed, implemented and maintained in the different phases of the ship's life in order to include all necessary information. Responsibilities related to these actions are also indicated.

This section does not contain requirements on how to conduct surveys. Survey requirements will be developed separately.

The following information shall be produced during the different phases of the ship's life for the design, development, maintenance and implementation of a Test Plan:

5.1 During design and construction phases:

a. The Supplier shall design and document testing procedures suitable to verify the performance of measures adopted to fulfil relevant requirements (Test Plan), for what pertains the systems or equipment supplied to the Shipyard or System Integrator for integration in the CBSs in the scope of applicability of this UR and networks connecting such systems to each other and to other CBSs onboard or ashore.

b. The Supplier shall maintain a test report where results of execution of the tests described in the Test Plan, following the relevant testing procedures, are recorded, to be provided to the Shipyard, where test results are recorded.

c. The Shipyard or System Integrator shall incorporate the documentation provided by the Supplier into an overall Test Plan for the CBSs in the scope of applicability of this UR and networks connecting such systems to each other and to other CBSs onboard or ashore.

d. The Shipyard or System Integrator shall design and document testing procedures suitable to verify the performance of measures adopted to fulfil relevant requirements (Test Plan), for what pertains the whole integrated CBSs in the scope of applicability of this UR and networks connecting such systems to each other and to other CBSs onboard or ashore. Testing procedures shall include functional tests, failure tests and a description of alarms and other monitoring means used to signal normal conditions, warnings and alerts.

e. The Shipyard or System Integrator shall maintain a test report where results of execution of tests described in the Test Plan, following the relevant testing procedure, are recorded, to be provided to the incoming Shipowner and to the Class Society upon ship commissioning, where test results are recorded. The Classification Society shall witness the execution of tests and may request execution of additional tests.

E26 (cont)

f. Testing procedures shall be described in the Test Plans in such a way as to make it possible for a third party, upon commissioning of the ship and during its service, to reproduce onboard the intended test conditions, execute the tests and verify test results, and make it possible a comparison between the results obtained and those obtained by the Supplier and/or the Shipyard/System Integrator.

g. The Supplier and the Shipyard shall keep Test Plans up to date and aligned with the actual implementation and installation of CBSs onboard.

5.2 Upon ship commissioning:

a. The Shipyard and the incoming Shipowner shall together verify that the information contained in the final version of the Test Plan 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 in the Test Plan 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.

b. The Shipyard 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 Test Plan.

c. The final Test Plans updated according to the actual CBSs configuration and implementation onboard shall be made available to the Classification Society. The Classification Society may request execution of additional tests.

5.3 During the operational life of the ship:

a. The Shipowner, with the support of Systems Integrator and Suppliers, shall keep the Test Plan 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 Test Plan 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.

b. 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.

c. The Shipowner, with the support of System Integrator and 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.

d. The Shipowner shall retain onboard a copy of results of execution of tests and an updated Test Plan and make them available to the Classification Society.

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. A concise list of excluded applications of relevant requirements is to be generated and maintained with the CBS documents onboard the ship (e.g. the execution of test plans and any relevant updated test plans).

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 and connectivity grade 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 Shipyard during the design and building phase and kept up to date 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.

A concise list of excluded applications of relevant requirements is to be generated and maintained with the CBS documents onboard the ship (e.g. the execution of test plans and any relevant updated test plans). The Class Society may accept or reject the exclusion of the CBS from the application of the requirements in this UR.

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 grade 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;

E26 (cont)

- Threats, both internal and external;
- 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 evidence 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 criteria as per a) to l) 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 to submit additional documents to consider the said exclusion.

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

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

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

c) The CBS, considered in its function and role in the integrated system it is part of, cannot be affected by cyber incidents vectored by other CBSs or network devices, nor it can propagate the effect of a cyber incident to other CBSs or network devices;

d) The CBS must not serve essential services or multiple ship services;

e) The CBS must be located in areas using controlled access;

f) The connections of CBS to other CBSs have been duly investigated, understood and documented. In particular, the CBS shall not be connected to other CBSs or devices by IP-based networks;

g) The CBS shall not have available physical interfaces that can be used by uncontrolled/unsecure removable devices;

h) The software installed on the CBS has been duly identified and evidence is given of the purpose, name, version, provider and maintainer of each software application, operating system and firmware (as applicable);

i) The CBS is subject to a maintenance policy and such policy does not imply any permanent or temporary connection to untrusted networks, or use of uncontrolled/unsecure removable devices;

j) The CBS provides means for checking at any time its functional integrity and the quality of service provided, including checks on hardware and software integrity;

k) The CBS provides suitable interfaces allowing a human operator to take local manual control, and such interfaces do not widen its attack surface (see also point (b)).

l) The Incident Response Plan and Recovery Plan contain indications on how to treat the CBS in case of cyber incidents occurring on the ship.

E26
(cont)

Appendix – Summary of actions and documents

Legend*

Approve	The document shall be submitted to Class Society for approval
Check	The Surveyor shall verify the availability and update status of the document
Info	The document shall be submitted to Class Society for information
Maintain	The indicated stakeholder shall keep the document up to date and aligned with the actual implementation of CBSs, networks and risk mitigation measures
Make avail	The indicated stakeholder shall make documentation available to the Surveyor
Provide	The indicated stakeholder shall provide the documentation and make it available to other concerned stakeholders

* “document” refers to the document in the left column of the row in the table below.

N: The documents listed in the table below can be grouped in less numerous compound documents according to criteria of affinity and homogeneity of contents, provided that clearly separated and recognizable sections are included in the compound document, each corresponding to one of the original documents in the list.

Document	Reference Requirement	Phase	Supplier	Shipyard System Integrator	Shipowner Company	Class
Identify						
Inventory of hardware and software 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	Inventory of CBSs and software onboard	**Design**	Provide			Approve
		Construction		Maintain		Info
		Commissioning		Provide		Approve
		Operation			Maintain	
		Survey			Make avail.	Check

E26 (cont)

Document	Reference Requirement	Phase	Supplier	Shipyard System Integrator	Shipowner Company	Class
Protect						
Documentation of the product, equipment or component supplied to construct network segregation, including a diagram of zones and conduits and the configuration of traffic filtering/shaping rules	Network segmentation / segregation	**Design**	Provide			Approve
		Construction		Maintain		Info
		Commissioning		Provide		Info
		Operation			Maintain	
		Survey			Make avail.	Check
Documentation on network protection measures including a test plan to verify the implemented control	Network protection sefaguards	**Design**	Provide			Info
		Construction		Maintain		Info
		Commissioning		Provide		Approve
		Operation			Maintain	
		Survey			Make avail.	Check
Antivirus, antimalware and antispam software installed or other security measures applied	Antivirus, antimalware, antispam and other protections from malicious code	**Design**	Provide			Approve
		Construction		Maintain		Info
		Commissioning		Provide		Info
		Operation			Maintain	
		Survey			Make avail.	Check
Installation locations, physical access restrictions, credential management policy, removable media access points	Physical and logical access control	**Design**	Provide			Info
		Construction		Maintain		Approve
		Commissioning		Provide		Info
		Operation			Maintain	
		Survey			Make avail.	Check
Wireless networks diagrams, security capabilities, connection with other networks	Wireless communication	**Design**	Provide			Approve
		Construction		Maintain		Info
		Commissioning		Provide		Info
		Operation			Maintain	
		Survey			Make avail.	Check

E26 (cont)

Document	Reference Requirement	Phase	Supplier	Shipyard System Integrator	Shipowner Company	Class
Remote connection policies and procedures, roles and responsibilities	Remote access control and remote maintenance	**Design**	Provide			Info
		Construction		Maintain		Info
		Commissioning		Provide		Info
		Operation			Maintain	
		Survey			Make avail.	Check
Policies and procedures on use of mobile and portable devices, roles and responsibilities	Use of Mobile and Portable Devices	**Design**	Provide			Info
		Construction		Maintain		Info
		Commissioning		Provide		Approve
		Operation			Maintain	
		Survey			Make avail.	Check
Detect						
Description on how to monitor networks, test plan; plans for training and drills	Network operation monitoring	**Design**	Provide			Info
		Construction		Maintain		Info
		Commissioning		Provide		approve
		Operation			Maintain	
		Survey			Make avail.	Check
Monitoring, alarm and diagnostic functions of CBS and network devices	Diagnostic functions of CBS and networks	**Design**	Provide			Info
		Construction		Maintain		Info
		Commissioning		Provide		Info
		Operation			Maintain	
		Survey			Make avail.	Check
Respond						
Alarms and other means used to signal cyber incidents and procedures to respond to such incidents; plans for training and drills	Incident response plan	**Design**	Provide			Approve
		Construction		Maintain		Info
		Commissioning		Provide		Info
		Operation			Maintain	
		Survey			Make avail.	Check

E26 (cont)

Document	Reference Requirement	Phase	Supplier	Shipyard System Integrator	Shipowner Company	Class
Instructions on how to activate local independent and/or manual operation (part of the Incident response plan)	Local, independent and/or manual operation	**Design**	Provide			Info
		Construction		Maintain		Info
		Commissioning		Provide		Info
		Operation			Maintain	
		Survey			Make avail.	Check
Instructions to allow personnel to isolate the network in an efficient manner (part of the Incident response plan)	Network isolation	**Design**	Provide			Approve
		Construction		Maintain		Info
		Commissioning		Provide		Info
		Operation			Maintain	
		Survey			Make avail.	Check
Minimal risk conditions to be reached in case of unexpected or unmanageable failures or cyber events including procedures to be followed in case of request for human operator's takeover	Fallback to a minimal risk condition	**Design**	Provide			Approve
		Construction		Maintain		Info
		Commissioning		Provide		Info
		Operation			Maintain	
		Survey			Make avail.	Check
Recover						
Instructions and procedures for the recovery of a failed system; how to get external assistance and support from ashore; plans for training and drills	Recovery plan	**Design**	Provide			Info
		Construction		Maintain		Info
		Commissioning		Provide		Approve
		Operation			Maintain	
		Survey			Make avail.	Check
Procedures and operations for backup and restoration of data and software; plans for training and drills	Backup and restore capability	**Design**	Provide			Info
		Construction		Maintain		Info
		Commissioning		Provide		Info
		Operation			Maintain	
		Survey			Make avail.	Check

E26
(cont)

Document	Reference Requirement	Phase	Supplier	Shipyard System Integrator	Shipowner Company	Class
Documentation on how to execute controlled shutdown, reset to an initial state, roll-back to a safe state and restart from scratch to allow fast and safe recovery	Controlled shutdown, reset, roll-back and restart	**Design**	Provide			Approve
		Construction		Maintain		Info
		Commissioning		Provide		Info
		Operation			Maintain	
		Survey			Make avail.	Check
Performance evaluation and testing						
Test Plans describing testing procedures in such a way as to make it possible for the Surveyor or other third party to reproduce onboard the intended test conditions, execute the tests and verify test results, and make it possible a comparison between the results obtained and those obtained by the Supplier and/or the Shipyard/System Integrator. Testing procedures shall include a description of functional tests, failure tests, alarms and other monitoring means used to signal normal conditions, warnings and alerts.	Performance evaluation and testing	**Design**	Provide			Approve
		Construction		Maintain		Info
		Commissioning		Provide		Info
		Operation			Maintain	
		Survey			Make avail.	Check
Risk Assessment						
Risk assessment for supplied products, equipment or components aimed at identification of cyber risks and relevant mitigation measures, including a concise list of excluded applications of relevant requirements.	Risk assessment for exclusion of CBS from the application of requirements	**Design**	Provide			Approve
		Construction		Maintain		Info
		Commissioning		Provide		Approve
		Operation			Maintain	
		Survey			Make avail.	Check

End of document