

## **REVIEW OF AMENDMENTS IN RELATION TO PREVIOUS EDITION OF THE RULES**

### **RULES FOR THE CLASSIFICATION OF SHIPS**

#### *Part 1 - GENERAL REQUIREMENTS*

#### *Chapter 6 – Requirements for additional class notations*

All major changes in respect to Rules for the classification of ships, Part 1 – General requirements, Chapter 6 – Requirements for additional class notations, edition January 2025, throughout the text are shaded (if any).

Items not being indicated as corrected have not been changed.

The grammar and print errors have been corrected throughout the Rules and are not subject to above indication of changes.

The subject Chapter of the Rules includes the requirements of the following international Organisations:

**International Maritime Organization (IMO)**

**Resolutions:** A.446(XI), as amended by Res. A.497(XII), and as further amended by Res. A.897(21)  
A.1207(34) Survey Guidelines Under the Harmonized System of Survey and Certification (HSSC), 2025  
MSC.521(106), Amendments to the International Convention for the Safety of Life at Sea, 1974 (Chapter XV)

**Codes:** MSC.527(106), International Code of Safety for Ships Carrying Industrial Personnel (IP Code)

**Circulars:** MSC.1/Circ.1680, Unified interpretations of SOLAS Regulation XV/5.1 and paragraph 3.5 of part 1 of the International Code of Safety for Ships Carrying Industrial Personnel (IP Code) on the Harmonization of the Industrial Personnel Safety Certificate with SOLAS Safety Certificates

**International Association of Classification Societies (IACS):**

**Unified Requirements (UR):**  
E10 (Rev. 10, Aug. 2024), E26 (Rev.1, 2023), E27 (Rev.1, 2023)

**Unified Interpretations (UI):**  
SC 303 (July 2024)

**Recommendations (Rec.):**  
Rec. 190 (June 2025)

## Chapter 6      **REQUIREMENTS FOR ADDITIONAL CLASS NOTATIONS**

### Contents:

	Page
<b>1    ADDITIONAL CLASS NOTATIONS.....</b>	<b>1</b>
1.1    GENERAL.....	1
<b>2    BATTERY SYSTEM (BAT).....</b>	<b>2</b>
2.1    GENERAL.....	2
2.2    TECHNICAL REQUIREMENTS.....	2
2.3    RISK ASSESSMENT, BATTERY LOCATION, VENTILATION, GAS DETECTION AND FIRE SAFETY.....	4
2.4    CERTIFICATION, TESTING AND INSPECTION.....	5
<b>3    CRUDE OIL WASHING (COW).....</b>	<b>7</b>
3.1    GENERAL.....	7
3.2    PIPING.....	7
3.3    TANK WASHING MACHINES.....	8
3.4    PUMPS FOR CRUDE OIL WASHING SYSTEM.....	9
3.5    STRIPPING SYSTEM.....	9
<b>4    IN-WATER SURVEY (IWS).....</b>	<b>11</b>
4.1    GENERAL.....	11
4.2    TECHNICAL REQUIREMENTS.....	11
<b>5    ASPHALT CARRIERS.....</b>	<b>12</b>
5.1    GENERAL.....	12
5.2    GENERAL REQUIREMENTS.....	12
<b>6    CYBER RESILIENCE.....</b>	<b>14</b>
6.1    GENERAL.....	14
6.2    CYBER RESILIENCE OF SHIP.....	14
6.3    CYBER RESILIENCE OF ON-BOARD SYSTEMS AND EQUIPMENT.....	34
6.4    TECHNICAL DOCUMENTATION.....	45
6.5    PERIODICAL CLASS SURVEYS.....	45
<b>7    SHIPS CARRYING INDUSTRIAL PERSONNEL.....</b>	<b>46</b>
7.1    GENERAL.....	46
7.2    APPLICATION.....	46
7.3    REQUIREMENTS FOR THE ASSIGNMENT.....	46
7.4    TECHNICAL DOCUMENTATION.....	48
7.5    PERIODICAL CLASS SURVEYS.....	48
<b>8    TRANSHIPPING UNITS.....</b>	<b>49</b>
8.1    GENERAL.....	49
8.2    APPLICATION.....	49
8.3    REQUIREMENTS FOR THE ASSIGNMENT.....	49
8.4    TECHNICAL DOCUMENTATION.....	49
8.5    PERIODICAL CLASS SURVEYS.....	49
<b>9    MOBILE STORAGE UNITS.....</b>	<b>51</b>
9.1    GENERAL.....	51
9.2    APPLICATION.....	51
9.3    REQUIREMENTS FOR THE ASSIGNMENT.....	51
9.4    TECHNICAL DOCUMENTATION.....	51
9.5    PERIODICAL CLASS SURVEYS.....	51

# 1 ADDITIONAL CLASS NOTATIONS

## 1.1 GENERAL

**1.1.1** This section of this Chapter of the *Rules for the classification of ships* (hereafter referred to as: the Rules) of **CROATIAN REGISTER OF SHIPPING** (hereinafter referred to as: the *Register*) is prescribing technical requirements for some of additional characters of class or descriptive class notes, as referenced to in the *Rules for the classification of ships, Part 1 – General requirements, Chapter 1 – General information, 4*.

**1.1.2** The assignment of additional characters of class or descriptive class notes to a new ship is subject to compliance with the general rule requirements laid down in the *Rules for the classification of ships, Part 1 – General requirements, Chapter 1 – General information*, and with the additional requirements laid down in the corresponding Section of this Chapter.

## 2 BATTERY SYSTEM (BAT)

### 2.1 GENERAL

**2.1.1** The additional character of class **BAT** - **BATTERY SYSTEM** may be assigned to ships using battery systems complying to below specified requirements.

Technical documentation to be submitted to the *Register* for the purpose of the first assignment of subject character of class is listed in the *Rules for the classification of ships, Part 1 – General requirements, Chapter 2 – Survey during construction and initial survey*.

Requirements for periodical class surveys, for the purpose of maintaining subject character of class are included in the *Rules, Part 1 – General requirements, Chapter 5 – Surveys of ships in service*.

### 2.2 TECHNICAL REQUIREMENTS

**2.2.1** Requirements in this item applies to the lithium-ion, lithium metal and lithium polymer battery types. Requirements concerning conventional types of batteries are prescribed in the *Rules for the classification of ships, Part 12 – Electrical equipment, Section 13*.

**2.2.2** Since battery technologies are under constant development, additional battery types may be considered and additional requirements, other than these stated here, may be required.

Alternative battery designs, other than stated here, may be considered on case-to-case basis by the *Register* provided that the safety and reliability of such design will be at least at equivalent level to those specified here.

**2.2.3** Definitions and explanations:

- .1 **Battery cell** – smallest unit of a battery.
- .2 **Battery cell block** – group of battery cells connected together in parallel configuration with or without protective devices and monitoring circuitry.
- .3 **Battery module** – group of battery cells connected together in series and/or parallel configuration with or without protective devices and monitoring circuitry.
- .4 **Battery pack** – energy storage device, which is comprised of one or more battery cells or battery modules electrically connected. Battery pack has a monitoring circuitry which provides information to a battery system. Battery pack may incorporate a protective housing and be provided with terminals or other interconnection arrangement.
- .5 **Battery system** – system which comprises of one or more battery cells, battery modules or battery packs. Battery system has a Battery Management System and may also have cooling or heating units.
- .6 **Battery Management System (BMS)** – electronic system associated with a battery which has functions to cut off in case of

overcharge, overcurrent, over discharge and overheating. It monitors and/or manages its state, calculates secondary data, reports that data and/or controls its environment to influence the battery's safety, performance and/or service life. The function of the BMS can be assigned to the battery pack or to equipment that uses the battery.

- .7 **Energy Management System (EMS)** – system providing monitoring and control of energy capacities.
- .8 **Battery string** – a number of battery cells or modules connected in series with the same voltage level as the battery system.
- .9 **Battery space (Compartment)** – The space in which the battery system is physically located.
- .10 **State of Charge (SOC)** – available capacity in a battery expressed as a percentage of rated capacity.
- .11 **State of Health (SOH)** – an indication of the general condition of a battery compared to its ideal conditions (e.g. a new battery). The unit of SOH are percent points (100% means battery's condition matches the battery's specifications).
- .12 **Thermal Runaway** – uncontrolled intensive increase in the temperature of a cell driven by exothermic reaction.
- .13 **Rated capacity** – capacity value of a cell or battery determined under specified conditions and declared by the manufacturer.

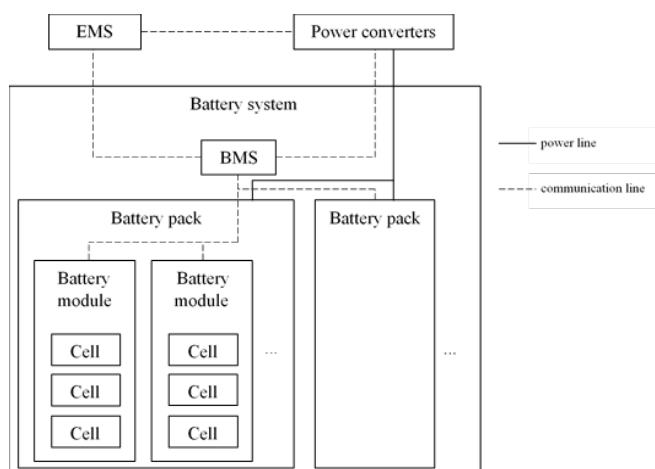
**2.2.4** Apart from the list of documentation to be submitted for the purpose of the assignment of subject additional character of class stated in the *Rules for the classification of ships, Part 1 – General requirements, Chapter 2 – Survey during construction and initial survey, 1.2.17*, the *Register* may request additional documentation to be submitted, where it proves necessary.

- 2.2.5** Following documentation is to be kept onboard:
- .1 Operation manual and maintenance manual.
  - .2 Battery system firefighting procedure.
  - .3 Battery system operation and maintenance logs.

#### Battery system

**2.2.6** Typical battery system configuration is shown in the Figure 2.2.6-1. Battery system configuration may vary from manufacturer to manufacturer.

**Figure 2.2.6-1**  
Typical battery system configuration



**2.2.7** Battery system is to be designed so that the capacity of the system is sufficient for the intended use of the vessel, taking into account aging deterioration of the battery capacity.

**2.2.8** Exposed battery casing shall be constructed of durable, flame-retardant, materials that are suitable for use in the marine environment and resistant to electrolyte spillage.

**2.2.9** Minimum degree of protection (IP) of batteries depends on the location of installation but shall be no less than IP 44.

**2.2.10** Battery system is to be provided with Battery Management System (BMS) and external emergency shut-down arrangement.

**2.2.11** If the battery system is used as a main source of power, then two independent battery systems shall be provided. If the battery system is used as emergency source of power, then it is not to be installed in the same space as the emergency switchboard.

**2.2.12** Battery cells of different physical characteristics, chemistry composition and electrical parameters are not to be used in the same electrical circuit.

**2.2.13** Battery system's outgoing circuits are to be protected against overload and short-circuit.

**2.2.14** If batteries are used for supplying power to propulsion and steering, then the system is to be arranged so that the power to these services is maintained or immediately restored in case of supply failure.

**2.2.15** Arrangements shall be provided to disconnect the less essential consumers automatically and gradually in the event of the battery system overload. This load shedding may be carried out in one or several steps.

**2.2.16** Battery system is to be provided with means for local operation, independent of remote operation and with disconnecting switch for maintenance purposes.

### Power converters

**2.2.17** Power converters are to be certified and fulfil the requirements set in the *Rules for the classification of ships, Part 12 – Electrical equipment, Sections 2 and 12*.

**2.2.18** Power converters are to be able to communicate to and be able to operate within limits set by BMS and EMS.

**2.2.19** Power converters shall be provided with over-voltage and undervoltage protection.

**2.2.20** Power converters exceeding 50 kVA shall be provided with an independent emergency stop function.

**2.2.21** Power converters shall alarm charging/discharging failure on continuously manned station.

**2.2.22** In the case of charging of battery system via shore-connection, means shall be provided to cut off the shore power automatically or manually. Shore-connection is to be executed in such manner so that the human operator cannot come in contact with any live connection.

### Control, monitoring, alarm, and safety systems

**2.2.23** Control, monitoring, alarm, and safety systems are to have self-check functions. In the event of failure, an alarm is to be activated.

**2.2.24** Safety system is to be designed to minimize the impact of failures and shall be constructed on fail-safe principle.

**2.2.25** Safety system sensors are to be independent from other sensors.

**2.2.26** Sensors are to be designed to withstand the local environment. The enclosure of the sensor and the cable entry are to be appropriate to the space in which they are located. Any malfunction in the sensors is to be detectable.

**2.2.27** Energy Management System (EMS) is to be installed that shall provide reliable measure of available energy and power taking into consideration the SOH and SOC. EMS is responsible for load reduction to prevent battery system overload.

**2.2.28** EMS is to be certified. EMS is considered to be a computer system of category III and is to comply with requirements from the *Rules for the classification of ships, Part 12 – Electrical equipment, Chapter 2.10*. EMS may be a part of vessel's Power Management System (PMS).

### Battery management system (BMS)

**2.2.29** Battery Management System (BMS) is to be certified. BMS is considered to be a computer system of category II or III (exact categorization depends on the intended use of the battery system) and is to comply with requirements from the *Rules for the classification of ships, Part 12 – Electrical equipment, Chapter 2.10*.

**2.2.30** BMS is to have following functions:

- Provide limits to the power converters for charging and discharging.
- Provide protection of the battery system in case of overcurrent, overvoltage, undervoltage and overtemperature.
- Provide battery cell and module balancing.

**2.2.31** BMS is to be continuously powered by a source of power other than battery monitored by it, and an alarm shall be provided in the event of power supply failure.

**2.2.32** BMS is to monitor the battery cell voltage, temperature, and battery string current. BMS shall provide following information on local control panel and on continuously manned station:

- Battery system voltage.
- Battery cell voltage (including minimum, maximum, and average).
- Battery cell temperature (including minimum, maximum, and average).
- Battery string current.
- Ambient and/or battery space temperature.
- State of Charge (SOC) of the batteries (also to be provided to EMS).
- State of Health (SOH) of the batteries (also to be provided to EMS).
- Battery charging/discharging status.

### Alarms

**2.2.33** Any abnormal condition of the battery system is to initiate an audible and visual alarm at continuously manned station and/or navigation bridge. For vessels without centralized alarm system, battery alarms are to be presented on the navigation bridge.

**2.2.34** Battery alarms shall consist of following alarms:

- Battery shutdown.
- Other safety/protection functions.
- Failure of safety/protection functions.
- Battery cell high temperature.
- Ambient or battery space low/high temperature.
- Battery cell overvoltage/undervoltage.
- Battery cell voltage imbalance.
- Battery string overcurrent.
- Ventilation status alarms.
- Minimum SOC.
- Gas detection.
- Charging/discharging fault.

**2.2.35** Battery system warnings that can develop into safety hazards are to be alarmed before reaching hazardous levels (e.g. high ambient temperature).

**2.2.36** Minimum level of SOC is to be determined with regards to vessels operation purpose.

### Safety system

**2.2.37** Activation of safety system is to give an alarm. Safety system is to be executed in the fail-safe principle. Failure of the safety system's protection functions is to give an alarm.

**2.2.38** Thermal protection device, independent of the BMS, that shall disconnect the battery in case of high temperature is to be provided for battery modules.

**2.2.39** Battery cell or battery module/pack case is to be provided with a pressure relief mechanism to prevent rupture or explosion.

**2.2.40** External emergency shutdown arrangement mentioned in 4.2.1.6 is to be located outside battery space. If

the battery system is used for propulsion, then an additional emergency shutdown arrangement from navigation bridge is to be provided.

**2.2.41** Other safety functions shall be implemented if battery design comprises additional safety hazards.

**2.2.42** Safety mechanism is to be provided that will not allow manual override of safety functions.

## 2.3 RISK ASSESSMENT, BATTERY LOCATION, VENTILATION, GAS DETECTION AND FIRE SAFETY

### Risk assessment

**2.3.1** Risk assessment is to be carried out in the design phase in order to identify all potential hazards and uncertainties of the proposed battery system design and installation on the vessel. Risk assessment should include measures to avoid and/or mitigate risks.

**2.3.2** Risk assessment shall be used to determine:

- Development of dangerous (toxic and corrosive) gases.
- Electrolyte spillage.
- Electric shock.
- Fire and water hazards.
- Explosion hazards.
- Battery room entry hazards and procedures.
- Battery thermal runaway, short-circuit, overcurrent, overvoltage.
- External heat hazards.
- Battery space ventilation rate and loss of ventilation.
- Charging facilities.
- Loss of propulsion.
- Gas detection system.
- Fire detection system.
- Fire-fighting methods.

**2.3.3** Battery system fire-fighting procedure is to be provided which shall cover all the necessary steps for successful fire suppression and extinguishment and will include all necessary precautions to avoid any personnel injuries.

**2.3.4** Risk assessment is part of documentation that is subject to approval.

**2.3.5** Identified risks and means to mitigate risks are to be included in the operating manual.

### Battery spaces, ventilation, gas detection

**2.3.6** Risk assessment is to be carried to determine whether the battery system needs to be installed in designated battery room, sufficient ventilation capacities, selection of gas detection and fire safety systems.

**2.3.7** Batteries > 25 kWh are to be installed inside battery rooms or inside battery boxes on open deck, provided that the battery boxes can ensure battery's service environment.

**2.3.8** Batteries < 25 kWh may be installed inside battery boxes located in engine room, provided that the battery boxes can ensure battery's service environment.

**2.3.9** Battery boxes' mechanical degree of protection shall correspond to the requirements of the installed location (the *Rules for the classification of ships, Part 12 – Electrical equipment, Chapter 2.4*).

**2.3.10** Battery boxes, as well as battery rooms shall be fitted with temperature sensor(s).

**2.3.11** Battery spaces are not to be located forward of the collision bulkhead, nor in the accommodation spaces.

**2.3.12** Battery rooms are not to contain any equipment supporting essential services with the exemption of cables of the battery system itself.

**2.3.13** Battery rooms are not to contain any other equipment that are not part of battery system with the exemption of safety and fire protection equipment used for the battery system itself.

**2.3.14** Battery rooms are not to contain any heat sources.

**2.3.15** Batteries are to be installed in locations where they will not be exposed to excessive temperatures, liquid splashing or spraying, shocks and vibrations.

**2.3.16** Battery rooms and battery boxes are to be mechanically ventilated. Ventilation ducts are to be made of steel or equivalent material. Ventilation ducts used for battery system ventilation cannot be used to ventilate other spaces. Ventilation shall have capacity for at least two air changes per hour.

**2.3.17** Battery rooms and battery boxes are to be equipped with appropriate emergency exhaust ventilation that shall vent the gases that may occur during an abnormal situation. Ventilation fan is to be of non-sparking type and provide six air changes per hour. Intake and exhaust ventilation ducts are to be from/to a safe location on the open deck.

**2.3.18** Emergency exhaust ventilation is to be activated automatically upon detection of dangerous gases from the batteries. Facilities for local and remote (from continuously manned station) operation of this ventilation are to be provided.

**2.3.19** Battery spaces are to be provided with gas detection system of approved type which will be appropriately suited for the used battery chemistry. Gas detection system is to provide an alarm to continuously manned station in case of 30% LEL and emergency exhaust ventilation is to be started automatically. In the case of 60% LEL, all unprotected electrical circuits in the battery space must be de-energized.

**2.3.20** Battery spaces are to be provided with a gas-tight door with alarm to the continuously manned station, or self-closing gas-tight door without hold-back arrangement.

**2.3.21** Means to disconnect the battery system outside of the protected space are to be provided in case of fire in battery space or machinery space of category A.

#### Fire safety

**2.3.22** Fixed fire detection and alarm system is to be provided for battery system. This system is to be according to the *Rules for the classification of ships, Part 12 – Electrical equipment*, and the *Rules for the classification of ships, Part 17 – Fire protection*.

**2.3.23** Battery spaces are categorized as auxiliary machinery spaces and are subject to fire protection requirements for those spaces.

**2.3.24** Battery spaces are to be fitted with fixed fire extinguishing system that is appropriate to be used with regards to battery chemistry. Battery manufacturer's recommendations shall be taken into account. This system is to be according to the *Rules for the classification of ships, Part 17 – Fire protection*.

**2.3.25** In addition to fixed fire extinguishing system, portable fire extinguishers are to be used – at least two dry powder or CO<sub>2</sub> extinguishers, with capacity of not less than 5 kg, near every battery system installation.

**2.3.26** Depending on battery chemistry and design used, flammable gases may be produced in the battery space. In this case the battery space is to be classified as a hazardous area as per IEC 60079 series and additional precautions shall be taken accordingly.

**2.3.27** Additional firefighting equipment or cooling means may be required with regard to characteristics of battery fire.

## 2.4 CERTIFICATION, TESTING AND INSPECTION

### Certification and testing

**2.4.1** The battery system  $\geq 25$  kWh shall be type approved, with testing carried out according to requirements from IEC 61619:2017, IEC 61620:2017 and Electrical and electronic equipment type testing (refer to IACS UR E10, also). Type testing is to be witnessed by the surveyor of the *Register*. For type testing information see Table 2.4.1-1.

**2.4.2** For battery system  $< 25$  kWh, manufacturer test certificates are required.

**2.4.3** Batteries that have failed propagation test are not allowed for use.

**2.4.4** Electrical equipment is to be suitable for use in the marine environment and fulfil the requirement of the *Rules for the classification of ships, Part 12 – Electrical Equipment, Section 2*.

**Table 2.4.1-1**  
Battery system type testing

No.	Test	Test unit	Type test	Routine test	Reference
1.	External short-circuit test	Cell	x	-	IEC 62619, 7.2.1
2.	Impact test	Cell	x	-	IEC 62619, 7.2.2
3.	Drop test	Cell	x	-	IEC 62619, 7.2.3
4.	Thermal abuse test	Cell	x	-	IEC 62619, 7.2.4
5.	Overcharge test	Cell	x	-	IEC 62619, 7.2.5
6.	Forced discharge test	Cell	x	-	IEC 62619, 7.2.6
7.	Internal short-circuit test	Battery system	x	-	IEC 62619, 7.3.2
8.	Propagation test	Battery system	x	-	IEC 62619, 7.3.3
9.	Overcharge control of voltage	Battery system	x	-	IEC 62619, 8.2.2
10.	Overcharge control of current	Battery system	x	-	IEC 62619, 8.2.3
11.	Overheating control	Battery system	x	-	IEC 62619, 8.2.4
12.	Capacity validation	Battery system	x	-	IEC 62620, 6.3.1
13.	Battery system type testing	Battery system	x	-	IACS UR E10
14.	Battery system unit testing	Battery system	-	x	IACS UR E10, 1, 2, 3, 9, 10
15.	Battery system safety function tests	Battery system	x	x	Specification

**2.4.5** Performance tests of the battery system are to be carried out according to the Testing program that is to be submitted for approval.

**2.4.6** Additional tests may be required if hazards are recognized by the Risk assessment or if seemed necessary by the *Register*.

### Inspection

**2.4.7** Battery system is to be inspected during manufacturing, during installation onboard and after installation onboard.

**2.4.8** Inspection during installation of battery system onboard is to include:

- Inspection of battery boxes or battery rooms.
- Inspection of cable routing.
- Inspection of fire division.
- Inspection of ventilation system.
- Inspection of gas detection system.
- Inspection of fire detection system.
- Inspection of fire-extinguishing system.
- Inspection of temperature sensors.
- Inspection of safe type of electrical equipment.

**2.4.9** Inspection after installation of battery system onboard is to include:

- Interface testing of battery system.

- Insulation resistance test.
- Test of battery system's protection and safety functions.
- Testing of alarms and indication.
- Testing of fire detection, gas detection, ventilation, etc. as far as applicable.
- Charging and discharging capacities.

**2.4.10** Battery system is to be periodically surveyed to ensure that the system is in satisfactory condition.

**2.4.11** At each annual survey of the vessel with additional character of class **BAT** assigned, items listed in the *Rules for the classification of ships, Part 1 – General requirements, Chapter 5 – Surveys of ships in service*, must be checked.

**2.4.12** Any modification or alteration of installed battery system, besides replacing spare parts and batteries, is not allowed prior to the approval of the *Register*.

## 3 CRUDE OIL WASHING (COW)

### 3.1 GENERAL

**3.1.1** The additional character of class COW - CRUDE OIL WASHING may be assigned to an oil tanker with installed Crude oil washing system and complying with the below specified requirements.

Technical documentation to be submitted to the Register for the purpose of the first assignment of the subject character of class is listed in the *Rules for the classification of ships, Part 1 - General requirements, Chapter 2 - Surveys during construction and initial survey*.

Requirements for periodical class surveys, for the purpose of maintaining subject character of class are included in the *Rules for the classification of ships, Part 1 - General requirements, Chapter 5 - Surveys of ships in service*.

**3.1.2** Ships carrying crude oil having 20,000 tons deadweight and above are to be fitted with cargo tank cleaning system using crude oil washing arrangement complying with MARPOL 73/78, Annex I, Reg. 33 and Reg. 35, which refers to "Revised Specifications for the Design, Operation and Control of Crude Oil Washing Systems", adopted by IMO Res. A.446(XI), as amended by A.497(XII) and as further amended by A.897(21).

**3.1.3** The crude oil washing system shall fully comply with the requirements of IMO Resolution A.446(XI), as amended by IMO Resolution A.497(XII) and as further amended by IMO Resolution A.897(21) within one year after the tanker was first engaged in the trade of carrying crude oil or by the end of the third voyage carrying crude oil suitable for crude oil washing, whichever occurs later (see 5.2).

**3.1.4** Every oil tanker operating with the crude oil washing system shall be provided with an Operations and Equipment Manual detailing the system and equipment and specifying operational procedures, to the satisfaction of the Register.

**3.1.5** Every oil tanker fitted with a cargo tank cleaning system using crude oil washing shall be provided with an inert gas system, according to the *Rules for the classification of ships, Part 17 - Fire protection*.

### 3.2 PIPING

**3.2.1** The crude oil washing pipes and all valves incorporated in the supply piping system shall be of steel or other equivalent material and shall be of adequate strength having regard to the pressure to which they may be subjected, and shall be properly jointed and supported. Piping is to comply with the requirements of the *Rules for the classification of ships, Part 8 - Piping*.

**3.2.2** The crude oil washing system shall consist of permanent piping and shall be independent of the fire mains and of any system other than for tank washing. Sections of the ship's cargo system may be incorporated in the crude oil washing system, provided that they meet the requirements applicable to crude oil piping.

**3.2.3** Notwithstanding the requirements of 3.2.2, in combination carriers the arrangement of crude oil washing system may allow:

- .1 The removal of the equipment, if necessary, when carrying cargoes other than crude oil, provided that, when reinstated, the system is as originally fitted and tested for oil tightness.
- .2 The use of flexible hose pipes to connect the crude oil washing system to tank washing machines if it is necessary to locate these machines in a cargo tank hatch cover. Such flexible hose pipes must be provided with flanged connections and be manufactured and tested in accordance with the *Rules for the classification of ships, Part 8 - Piping*. The length of these hoses shall be no greater than necessary to connect the tank washing machines to an adjacent point just outside the hatch coaming. These hoses shall be removed to suitably prepared and protected stowage when not in use and be pressure tested by an authority acceptable to the Register at intervals of not more than two and a half years.

**3.2.4** Provision shall be made to prevent overpressure in the tank washing supply piping. Any relief device fitted to prevent overpressure shall discharge into the suction side of the supply pump. Alternative methods to the satisfaction of the Register may be accepted provided an equivalent degree of safety and environmental protection is provided.

One such alternative is that where the system is served only by centrifugal pumps so designed that the pressure derived cannot exceed that for which the piping is designed, a temperature sensing device located in the pump casing is required to stop the pump in the case of overheating.

**3.2.5** Where hydrant valves are fitted for water washing purposes on tank washing lines, all such valves shall comply with 2.1 and provision shall be made for such connections to be blanked off by blank flanges when washing lines may contain crude oil. Alternatively, hydrant valves shall be isolated from the crude oil washing system by spade blanks.

**3.2.6** All connections for pressure gauges or other instrumentation shall be provided with isolating valves adjacent to the lines unless the fitting is of the sealed type.

**3.2.7** No part of the crude oil washing system shall enter the machinery spaces. Where the tank washing system is fitted with a steam heater for use when water washing, the heater must be effectively isolated during crude oil washing by double shut-off valves or by clearly identifiable blanks.

The steam heater referred to shall be located outside the machinery spaces.

**3.2.8** Where a combined crude oil-water washing supply piping is provided the piping shall be so designed that it can be drained so far as is practicable of crude oil, before water washing is commenced, into spaces designated in the Operations and Equipment Manual. These spaces may be the slop tank or other cargo spaces.

**3.2.9** The piping system shall be of such diameter that the greatest number of tank cleaning machines required, as

specified in 3.2.8, can be operated simultaneously at the designed pressure and throughput. The arrangement of the piping shall be such that the required number of tank cleaning machines to each cargo compartment, can be operated simultaneously.

**3.2.10** The piping system shall be tested to 1.5 times the working pressure after it has been installed on the ship.

**3.2.11** The crude oil washing supply piping shall be anchored (firmly attached) to the ship's structure at appropriate locations and means shall be provided to permit freedom of movement elsewhere to accommodate thermal expansion and flexing of the ship. The anchoring shall be such that any hydraulic shock can be absorbed without undue movement of the supply piping.

The anchors should normally be situated at the ends furthest from the entry of the crude oil supply to the supply piping. If tank washing machines are used to anchor the ends of branch pipes, then special arrangements are necessary to anchor these sections when the machines are removed for any reason.

### 3.3 TANK WASHING MACHINES

**3.3.1** The tank washing machines for crude oil washing shall be permanently mounted and shall be of a design acceptable to the *Register*.

**3.3.2** The performance characteristic of a tank washing machine is governed by nozzle diameter, working pressure and the movement pattern and timing. Each tank cleaning machine fitted shall have a characteristic such that the sections of the cargo tank covered by that machine will be effectively cleaned within the time specified in the Operations and Equipment Manual.

**3.3.3** Tank washing machines shall be mounted in each cargo tank and the method of support shall be to the satisfaction of the *Register*. Where the tank washing machines are positioned well below the deck level to cater for protuberances in the tank, consideration may need to be given to additional support for the machines and their supply piping.

**3.3.4** Each machine shall be capable of being isolated by means of stop valves in the supply line. If a deck mounted tank washing machine is removed for any reason, provision shall be made to blank off the oil supply line to the machine for the period the machine is removed. Similarly, provision shall be made to close the tank opening with a plate or equivalent means.

Where more than one submerged machine is connected to the same supply line a single isolating stop valve in the supply line may be acceptable provided the rotation of the submerged machines can be verified in accordance with 3.3.11.1 or 3.3.11.3.

**3.3.5** The drive units for the tank cleaning machines are to be integral with the tank cleaning machine.

**3.3.6** The number and location of the tank washing machines shall be to the satisfaction of the *Register*.

**3.3.7** The location of the machines is dependent upon the characteristics detailed in 3.3.2 and upon the configuration of the internal structure of the tank.

**3.3.8** The number and location of the machines in each cargo tank and oily mixture (slop) tank shall be such that all horizontal and vertical areas are washed by direct impingement or effectively by deflection or splashing of the impinging jet. In assessing an acceptable degree of jet deflection and splashing, particular attention shall be paid to the washing of upward-facing horizontal areas and the following parameters shall be used:

- .1 For horizontal areas of a tank bottom and the upper surfaces of a tank's stringers and other large primary structural members, the total area shielded from direct impingement by deck or bottom transverses, main girders, stringers or similar large primary structural members shall not exceed 10 % of the total horizontal area of tank bottom, the upper surface of stringers, and other large primary structural members.
- .2 For vertical areas of the sides of a tank, the total area of the tank's sides shielded from direct impingement by deck or bottom transverses, main girders, stringers or similar large primary structural members shall not exceed 15% of the total area of the tank's sides.  
In some installations it may be necessary to consider the fitting of more than one type of tank washing machine, in order to effect adequate coverage.

**3.3.9** At the design stage the following minimum procedures shall be used to determine the area of the tank surface covered by direct impingement:

- .1 Using suitable structural plans, lines are set out from the tips of each machine to those parts of the tank within the range of the jets.
- .2 Where the configuration of the tanks is considered by the *Register* to be complicated, a pinpoint of light simulating the tip of the tank washing machine in a scale model of the tank shall be used.
- .3 Shadow diagrams must be on drawings the scale of which must be at least:
  - .1 1:100 for tankers of less than 100,000 tons deadweight,
  - .2 1:200 for tankers of 100,000 tons deadweight and above.
- .4 The drawings must provide at least a plan view, a profile view, and an end elevation for each tank, or for tanks considered to be similar.
- .5 Sufficient detailed drawings of the vessel must be provided to check that all large primary structural members have been included.
- .6 Guidelines for the assessment of shadow diagrams are given in 4.2.9 of Appendix III to IMO Resolution A.446(XI), as amended.

**3.3.10** The design of the deck-mounted tank washing machines shall be such that means are provided, external to the cargo tanks, which, when crude oil washing is in progress,

would indicate the rotation and arc of the movement of the machine. Where the deck-mounted machine is of the non-programmable, dual nozzle type, alternative methods to the satisfaction of the *Register* may be accepted provided an equivalent degree of verification is attained.

**3.3.11** Where submerged machines are required, they should be non-programmable and in order to comply with the requirements of 3.3.8, it must be possible to verify their rotation by one of the following methods:

- .1 By indicators external to the tank.
- .2 By checking the characteristic sound pattern of the machine, in which case the operation of the machine shall be verified towards the end of each wash cycle.

Where two or more submerged machines are installed on the same supply line, valves shall be provided and arranged so that the operation of each machine can be verified independently of the other machines on the same supply line.

- .3 By gas freeing the tank and checking the operation of the machine with water during ballast voyages.  
The method of verification shall be stated in the Operations and Equipment Manual.

**3.3.12** Fixed washing machines shall comply with the following:

- .1 Stresses in piping or deck supports which arise during washing operation or when immersed into liquid shall not exceed allowable stresses.
- .2 Machines shall be made of steel or other material which does not initiate sparking due to friction more than steel.
- .3 Machines shall be earthed through hull.

### 3.4 PUMPS FOR CRUDE OIL WASHING SYSTEM

**3.4.1** The pumps supplying crude oil to the tank cleaning machines shall be either the cargo pumps or pumps specifically provided for the purpose.

**3.4.2** The capacity of the pumps shall be sufficient to provide the necessary throughput at the required pressure for the maximum number of tank cleaning machines required to be operated simultaneously as specified in the Operations and Equipment Manual. In addition to the above requirement, the pumps shall, if an eductor system is fitted for tank stripping, be capable of supplying the eductor driving fluid to meet the requirements of 3.5.2.

**3.4.3** The capacity of the pumps shall be such that the requirements of 3.4.2 can be met with any one pump inoperative. The pumping and piping arrangements shall be such that the crude oil washing system can be effectively operated with any one pump out of use.

**3.4.4** The carriage of more than one grade of cargo shall not prevent crude oil washing of tanks.

**3.4.5** To permit crude oil washing to be effectively carried out where the back pressure presented by the shore terminal is below the pressure required for crude oil washing,

provision shall be made that such an adequate pressure to the washing machines can be maintained in accordance with 3.4.2. This requirement shall be met with any one cargo pump out of action. The minimum supply pressure required for crude oil washing shall be specified in the Operations and Equipment Manual. Should this minimum supply pressure not be obtainable, crude oil washing operations shall not be carried out.

**3.4.6** Pumps shall be in accordance with the *Rules for the classification of ships, Part 8 - Piping* and the *Rules for the classification of ships, Part 9 - Machines*.

### 3.5 STRIPPING SYSTEM

**3.5.1** The design of the system for stripping crude oil from the bottom of every cargo tank shall be to the satisfaction of the *Register*.

**3.5.2** The design and capacity of the tank stripping system shall be such that the bottom of the tank being cleaned is kept free of accumulations of oil and sediment towards completion of the tank washing process.

**3.5.3** The stripping system shall be capable of removing oil at a rate of 1.25 times the total throughput of all the tank cleaning machines to be operated simultaneously when washing the bottom of the cargo tanks or during any stage of the bottom washing as specified in the Operations and Equipment Manual.

**3.5.4** Means such as level gauges, hand dipping and stripping system performance gauges as referred to in 3.5.9 shall be provided for checking that the bottom of every cargo tank is dry after crude oil washing. Suitable arrangements for hand dipping must be provided at the aftermost portion of a cargo tank and in three other suitable locations unless other approved means are fitted for efficiently ascertaining that the bottom of every cargo tank is dry. The cargo tank bottom shall be considered dry if there is no more than a small quantity of oil near the stripping suction with no accumulation of oil elsewhere in the tank. Level indicators system shall be of closed type (water-gas tight).

**3.5.5** Every oil tanker required to be provided with segregated ballast tanks or fitted with a crude oil washing system, shall comply with the following requirements:

- .1 Oil piping is to be so designed and installed that oil retention in the lines is minimised.
- .2 Means shall be provided to drain all cargo pumps and all oil lines at the completion of cargo discharge, where necessary, by connection to a stripping device. The line and pump draining shall be capable of being discharged both to a cargo tank or a slop tank and ashore. For discharge ashore a special small diameter line shall be provided and shall be connected outboard of the ship's manifold valves. The cross-sectional area of this line shall not exceed 10 % of that of a main cargo discharge line.

**3.5.6** In crude oil tankers having individual cargo pumps in each tank, each pump having an individual piping system, dispensation from the required special small diameter

line may be given in cases where the combined amount of oil left in the tank after stripping and the volume of oil in the piping system from the manifold to the tank is less than 0.00085 times the volume of the cargo tank. If a deep well cargo pump system is provided with an evacuating system for retained oil, the above consideration should also apply.

**3.5.7** The means for stripping oil from the cargo tanks shall be by positive displacement pump, self-priming centrifugal pump or eductor, or other methods to the satisfaction of the *Register*. Where a stripping line is connected to a number of tanks, means shall be provided for isolating each tank not being stripped at that particular time.

**3.5.8** The internal structure of the tank shall be such that drainage of oil to the tank suction of the stripping system is adequate to meet the requirements of 3.5.2 and 3.5.4. Care shall be taken that both longitudinal and transverse drainage are satisfactory and shall be verified during the inspection.

**3.5.9** Equipment shall be provided for monitoring the efficiency of the stripping system. All such equipment shall have remote read-out facilities in the cargo control room or in some other safe and convenient place easily accessible to the officer in charge of cargo and crude oil washing operations. Where a stripping pump is provided, the monitoring equipment shall include, as appropriate, a flow indicator, or a stroke counter or a revolution counter, and pressure gauges at the inlet and discharge connections of the pump or equivalent. Where eductors are provided, the monitoring equipment shall include pressure gauges at the driving fluid intake and at the discharge and a pressure/vacuum gauge at the suction intake.

**3.5.10** The trim conditions for crude oil washing given in the Operations and Equipment Manual shall be adhered to.

## 4 IN-WATER SURVEY (IWS)

### 4.1 GENERAL

**4.1.1** The additional class notation **IWS – IN-WATER SURVEY** may be assigned to ships with a hull specially marked and equipped for in-water surveys and complying with below-specified requirements.

Technical documentation to be submitted to the *Register* for the purpose of the first assignment of the subject character of class is listed in the *Rules for the classification of ships, Part 1 – General requirements, Chapter 2 – Surveys during construction and initial survey*.

Requirements for periodical class surveys, for the purpose of maintaining the subject character of class, are included in the *Rules for the classification of ships, Part 1 – General requirements, Chapter 5 – Surveys of ships in service*.

**NOTE:** When performing an in-water examination of the outside of a passenger ship's bottom, statutory requirements as stated in paragraph 5.10 of **IMO Res. A.1207(34) "Survey Guidelines Under the Harmonized System of Survey and Certification (HSSC), 2025"**, as may be amended and **IMO MSC.1/Circ.1348 (Guidelines for the assessment of technical provisions for the performance of an in-water survey in lieu of bottom inspection in dry-dock to permit one dry-dock examination in any five-year period for passenger ships other than ro-ro passenger ships)**, should be appropriately taken into account also.

**NOTE:** When performing inspections of the outside of the ship's bottom of cargo ships with the ship afloat, statutory requirements as stated in paragraph 4.6 of **IMO Res. A.1207(34) "Survey Guidelines Under the Harmonized System of Survey and Certification (HSSC), 2025"**, as may be amended, should be appropriately taken into account also. For ships subject to enhanced survey, the provisions of paragraph 2.2.22 of the applicable part of annex A or B of the "International Code on the Enhanced Programme of Inspections during Surveys of Bulk Carriers and Oil Tankers, 2011 (2011 ESP Code)" should apply.

### 4.2 TECHNICAL REQUIREMENTS

**4.2.1** The underwater part of the hull is to be protected against corrosion, either by an appropriate coating system and/or external cathodic protection.

**4.2.2** The underwater part of the hull is to be provided, where necessary, with permanent markings at selected points on the plating that would enable determining the diver's position on the plating and localization of any damage.

Identification marks and systems are to be supplied on the outer surface of the immersed shell to facilitate the in-water survey by showing clearly the positions of water-tight bulkheads.

Every tank and bulkhead are to be clearly identified on the full immersed shell (side shells and bottom) by:

- at least one marking every five ordinary stiffeners spacing, distributed along the bulkhead length, without exceeding 5 meters between two markings,
- a segmented marking at every angle formed by a bulkhead,
- a cross-shaped marking at every bulkhead intersection,
- the abbreviated name of each tank, to be painted beside one of the boundaries markings.

**4.2.3** Means are to be provided for ascertaining the clearance in the propeller shaft aft bearing (or wear down by poker gauge), as well as the rudder pintle and bush clearances with the ship afloat.

**4.2.4** Liners of rudder stocks and pintles as well as bushes in rudders are to be marked in such a way that the diver will notice any shifting or turning.

**4.2.5** Sea chests must be capable of being cleaned under water, where necessary. Means should be provided to enable the diver to confirm that the sea suction openings are clear.

**4.2.6** For other equipment, such as bow thrusters, or stabilizers, requirements will be specified separately in each particular case.

**4.2.7** Plans and information facilitating the performance of the in-water surveys, as approved by the *Register*, are to be placed onboard and are to indicate the location and/or the general arrangement of:

- all shell openings,
- the stem,
- rudder and fittings,
- the sternpost,
- the propeller, including the means used for identifying each blade,
- anodes, including securing arrangements,
- bilge keels,
- welded seams and butts,
- marking with type, position, size, paint, tank abbreviation table.

The plans are also to include the necessary instructions to facilitate the divers' work, especially for taking clearance measurements.

Moreover, a specific detailed plan showing the systems to be adopted when the ship is floating in order to assess the slack between pintles and gudgeons is to be submitted to the *Register* for approval.

## 5 ASPHALT CARRIERS

### 5.1 GENERAL

**5.1.1** As stated in the *Rules for the classification of ships, Part 1 – general requirements, Chapter 1 – General information, 4*, a **Tanker for oil** intended for the carriage of heated cargo (asphalt or bitumen) having a temperature above 60 [°C] may be assigned with the descriptive class note **Asphalt carrier** when complying with below specified requirements.

Technical documentation to be submitted to the *Register* for the purpose of the first assignment of the subject character of class is listed in the *Rules for the classification of ships, Part 1 – General requirements, Chapter 2 – Surveys during construction and initial survey*.

Requirements for periodical class surveys, for the purpose of maintaining subject descriptive class note, are included in the *Rules for the classification of ships, Part 1 – General requirements, Chapter 5 – Surveys of ships in service*.

**5.1.2** Below stated requirements are related asphalt carriers intended to carry asphalt (or bitumen) as heated cargo in independent tanks.

**5.1.3** In cases of asphalt carriers intended only to carry asphalt (or bitumen) as heated cargo, but in integral cargo tanks and having  $GT \geq 500$ , requirements of Enhanced Survey Programme should to be applied, as stated in the *Rules for the classification of ships, Part 1 – General requirements, Ch. 5 – Surveys of ships in service, 3.1*.

In the case of double-hull asphalt carriers hull survey requirements for double-hull oil tankers should apply (*Rules for the classification of ships, Part 1 – General requirements, Chapter 5 – Surveys of ships in service, Annex B*).

In the case of single-hull asphalt carrier hull survey requirements for single-hull tankers should apply (*Rules for the classification of ships, Part 1 – General requirements, Chapter 5 – Surveys of ships in service, 4.5, 5.4 and 7.7*).

### 5.2 GENERAL REQUIREMENTS

**5.2.1** Generally, asphalt carriers should comply with the requirements in Annex I of MARPOL 1973, as amended with regard to oil fuel tank protection (Reg. 12A), pump-room bottom protection (Reg. 22) and accidental oil outflow performance (Reg. 23).

All new asphalt carriers and existing tankers undergoing conversion to asphalt carriers under supervision of the *Register* are to comply with Annex I of MARPOL 1973 regarding to double hull and double bottom requirements (Reg. 19).

The requirements of Annex I of MARPOL, Regs. 29, 31, and 32 should not apply to oil tankers carrying asphalt or other products subject to the provisions of this Annex, which through their physical properties inhibit effective product/water separation and monitoring, for which the control of discharge under Reg. 34 of Annex I of MARPOL should be effected by the retention of residues on board with the discharge of all contaminated washings to reception facilities.

Asphalt carriers of 30,000 tonnes dwt and above are also to comply with the requirements for segregated ballast tanks (Reg. 18) in Annex I of MARPOL 1973, as amended.

According to MARPOL 1973, Annex I, Reg. 19, as amended, independent cargo tanks are to be so located that the distance from the moulded line of the bottom shell and side shell is to be not less than the limits as required by the aforementioned MARPOL regulation.

**5.2.2** Generally, carriage of asphalt cargoes at temperatures exceeding 300 [°C] is not permitted. Carriage of cargoes exceeding such temperatures will be specially considered.

The above should be considered in conjunction with the requirement that the maximum allowable temperature of the surrounding steel structure should not exceed 80 [°C].

Consequently, in the case of cargoes to be stored at temperatures above 90 [°C], the effects of thermal stresses on the hull and the independent cargo tank due to the elevated temperatures of the asphalt cargo should be considered during the scantling assessment and direct calculations.

**5.2.3** Cargo tanks are to be pre-heated when loading hot cargo in order to minimize the temperature discrepancies, with the loading manual to be developed and available onboard the ship as a guidance for the Master.

Additionally, when the piping lines are heated or cooled, they may put additional loads into the ship structures and therefore, sufficient expansion bends are to be provided to reduce this thermal loading.

**5.2.4** Asphalt carriers are typically considered as tankers with cargo having a flashpoint exceeding 60 [°C] (closed cup test), with the requirements of SOLAS, Regulation II-2 to be complied with.

However, if cargo is to be carried above its flashpoint, the fire safety measures are to comply with the requirements for tankers with cargo having a flashpoint below 60 [°C] in SOLAS, Regulation II-2. The grades of asphalt cargoes to be carried and pertinent flashpoint temperatures are to be included in the loading manual.

**5.2.5** The overproduce which may occur under loading/unloading operations should be considered, if any. In such a case, the diagram of the pressures in loading/unloading conditions is also to be included in the loading manual.

**5.2.6** The supports of independent tanks are to be so designed that the loads from the independent tanks are effectively transmitted to the tank supports, while the independent tanks are allowed to expand in all directions without restraint to reduce thermal stresses in the structures of independent tanks. Generally, the supports of independent tanks are also to be designed to limit the transmission of loads relative to global and local hull deflection from the hull structures to the independent tanks.

**5.2.7** Access to space in the cargo area of asphalt carriers with independent tanks, with an appropriate distance between the surface to be inspected and the ship structure should be provided. For the requirements related to access to space adjacent to the cargo tank refer to the International Code for the Construction and Equipment of Ships Carrying Liquefied Gases in Bulk (IGC Code), as far as applicable.

Asphalt carriers with independent tanks need not to comply with SOLAS Regulation II-1/3-6, which is applicable to oil tankers having integral tanks for the carriage of oil in bulk as contained in the definition of oil in Annex I of MARPOL 1973, as amended.

**5.2.8** In order to allow access for inspections, cofferdams in the cargo area, if fitted, should be provided with sufficient access space (generally not less than 600 mm). Sufficient access space should also be provided for pipe tunnels.

**5.2.9** Additional specific requirements for asphalt carriers:

- .1 Cargo tanks intended for the carriage of asphalt solutions are to be equipped with a heating system capable of preserving the asphalt solutions in their liquid state. Valves are to be fitted on the heating system inlet and outlet.
- .2 Cargo piping and associated fittings outside tanks are to be provided with suitable heating devices.
- .3 Each tank is to be equipped with at least two thermometers in order to ascertain the temperature of the asphalt solution.
- .4 Cargo piping and associated fittings outside tanks are to be suitably insulated, where necessary.
- .5 A fixed deck foam system or equivalent fixed installation should be installed (not required for ships with GT less than 2,000).
- .6 Protection against tank overfilling should be provided.
- .7 Cargo pump rooms are to be provided with a fixed fire-extinguishing system, except where the cargo is carried at a temperature below and not within 15 [°C] of the cargo flash point.
- .8 Spaces located within the cargo area are to be efficiently ventilated. Portable means of ventilation are permitted. Ventilation of the cargo pump room is to be provided.
- .9 Generally, access doors, air inlets and openings to accommodation spaces, service spaces and control stations are not to face the cargo area.
- .10 Fuel tanks located with a common boundary to cargo or tanks for retention of residues are not to be situated within, nor extend partly into, the cargo tank block. Such tanks may, however, be situated aft and/or forward of the cargo tank block. They may be accepted when located as independent tanks on open deck in the cargo area subject to spill and fire safety considerations.  
The arrangement of independent fuel tanks and associated fuel piping systems, including the pumps, may be as for fuel tanks and associated fuel piping systems located in the machinery spaces. For electrical equipment, requirements applicable to hazardous area classification must however be met.
- .11 Tanks containing cargo or cargo residues are to be segregated from accommodation, service, and machinery spaces, tanks containing drinking water, and stores for human consumption by means of a cofferdam or similar space. Double-bottom tanks adjacent to cargo tanks are not to be used as fuel oil tanks. Means are to be provided to keep deck spills away from accommodation and service areas.
- .12 Cargo pump discharge pressure should have a local indication on the pump (and next to the driving machine if located in a separate compartment), or next to the unloading control station.
- .13 Cargo tanks intended for the carriage of asphalt solutions are to be equipped with a heating system capable of preserving the asphalt solutions in their liquid state. Valves are to be fitted on the heating system inlet and outlet.
- .14 Cargo piping and associated fittings outside tanks are to be provided with suitable heating devices.

## 6 CYBER RESILIENCE

### 6.1 GENERAL

**6.1.1** The descriptive notation **Cyber Resilience** may be assigned to ships complying with the requirements stated in 6.2, and systems and equipment under the scope of 6.2 complying with requirements given in 6.3.

**6.1.2** Subject requirements are to be applied to ships as defined below and contracted for construction on or after 1 July 2024.

**NOTE:** For the date of “contract for construction” refer to the *Rules for the classification of ships, Part 1 – General requirements, Chapter 1 – General information, 5.14*, or IACS PR 29 respectively.

### 6.2 CYBER RESILIENCE OF SHIP

#### 6.2.1 Introduction

##### 6.2.1.1 General

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.

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

##### 6.2.1.2 Aim and purpose

The aim of this Head 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 Head targets the ship as a collective entity for cyber resilience and is intended as a base for the complementary application of other *Rules* 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 6.3.

##### 6.2.1.3 Scope of applicability

###### 6.2.1.3.1 Vessels in scope

This Head 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 Head 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.)

###### 6.2.1.3.2 Systems in scope

This Head 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 Head:

- 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 6.3.4 may be accepted by the *Register*, on the condition that requirements in this Head 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
  - any other systems connected to OT systems, either permanently or temporarily (e.g. during maintenance).

The cyber incidents considered in this Head are events resulting from any offensive manoeuvre that targets OT systems onboard ships as defined in 6.2.2.

### 6.2.1.3.3 System Category

System categories are defined in the *Rules for the classification of ships, Part 12 – Electrical equipment*, 2.10 on the basis of the consequences of a system failure to human safety, safety of the vessel and/or threat to the environment.

## 6.2.2 Definitions

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

**Annual survey:** See IACS 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 of 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.

**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 Head, 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 Head 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 Head.

## 6.2.3 Goals and organization of requirements

### 6.2.3.1 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.

### 6.2.3.2 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.

### 6.2.3.3 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.

## 6.2.4 Requirements

This item contains the requirements to be satisfied in order to achieve the primary goal defined in 6.3.1, organized according to the five functional elements identified in 6.3.2.

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 6.2.2 for definitions):

- Shipowner/Company
- Systems integrator
- Supplier
- the Register

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

### 6.2.4.1 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.

#### 6.2.4.1.1 Vessel asset inventory (see IACS Rec. 190)

##### 6.2.4.1.1.1 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 Head 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.

#### 6.2.4.1.1.2 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.

#### 6.2.4.1.1.3 Requirement details

The vessel asset inventory shall include at least the CBSs indicated in 6.2.1.3.2, 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.

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.

#### 6.2.4.1.1.3.1 Hardware

For all hardware devices in the scope of applicability of this Head, the vessel asset inventory shall include at least the information in 6.3.3.1.1.

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

#### 6.2.4.1.1.3.2 Software Rationale

For all software in the scope of applicability of this Head (e.g., application program, operating system, firmware), the vessel asset inventory shall include at least the information in 6.3.3.1.1.

The software of the CBSs in the scope of applicability of this Head 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 6.2.5.3.1.

#### 6.2.4.1.1.4 Demonstration of compliance

##### 6.2.4.1.1.4.1 Design phase

The systems integrator shall submit vessel asset inventory to the *Register* (ref. 6.2.5.1.3).

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

##### 6.2.4.1.1.4.2 Construction phase

The systems integrator shall keep the vessel asset inventory updated.

##### 6.2.4.1.1.4.3 Commissioning phase

The systems integrator shall submit Ship cyber resilience test procedure (ref. 6.2.5.2.1) and demonstrate to the *Register* that:

- Vessel asset inventory is updated and completed at delivery

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

##### 6.2.4.1.1.4.4 Operation phase

For general requirements to surveys in the operation phase, see 6.2.5.3.

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 Head, addressing at least the following requirements in this Head:

- Management of change (6.2.5.3)
- Hardware and software modifications (6.2.4.1.1.3)

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 Head:

- Vulnerabilities and cyber risks (6.2.4.1.1.2 and 6.2.4.1.1.3)
- Security patching (6.2.4.2.6.3.2)

##### First Annual Survey

The shipowner shall present to the *Register* 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 *Register* demonstrate implementation of the Ship cyber security and resilience program by presenting records or other documented evidence as specified for the first annual survey.

##### Renewal (Special) Survey

The shipowner shall demonstrate to the *Register* the activities in 6.2.4.1.1.4.3 as per the Ship cyber resilience test procedure.

#### 6.2.4.2 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.

##### 6.2.4.2.1 Security Zones and Network Segmentation

###### 6.2.4.2.1.1 Requirement

All CBSs in the scope of applicability of this Head 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.)

Only explicitly allowed traffic shall traverse a security zone boundary.

#### 6.2.4.2.1.2 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.

#### 6.2.4.2.1.3 Requirement details

A security zone may contain multiple CBSs and networks, all of which shall comply with applicable security requirements given in 6.2 and 6.3.

The network(s) of a security zone shall be logically or physically segmented from other zones or networks. See also 6.2.4.2.6.3.

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 6.2.1.3.2), these systems should be in a dedicated security zone.

Wireless devices shall be in dedicated security zones. See also 6.2.4.2.5.

Systems, networks or CBSs outside the scope of applicability of this Head are considered untrusted networks and shall be physically segmented from security zones required by 6.2. 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 6.2.4.4.3.

#### 6.2.4.2.1.4 Demonstration of compliance

##### 6.2.4.2.1.4.1 Design phase

The systems integrator shall submit Zones and conduit diagram and the Cyber security design description (see 6.2.5.1.1 and 6.2.5.1.2).

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

- Clear indication of the security zones
- Simplified illustration of each CBS in scope of applicability of this Head, 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 (6.3.3.1.2)
- 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).

##### 6.2.4.2.1.4.2 Construction phase

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

##### 6.2.4.2.1.4.3 Commissioning phase

The systems integrator shall submit Ship cyber resilience test procedure (ref. 6.2.5.2.1) and demonstrate to the *Register* 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.
- 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.

#### 6.2.4.2.1.4.4 Operation phase

For general requirements to surveys in the operation phase, see 6.2.5.3.

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 Head:

- Principle of Least Functionality (6.2.4.2.2.1)
- Explicitly allowed traffic (6.2.4.2.1.1)
- Protection against denial of service (DoS) events (6.2.4.2.2.1)
- Inspection of security audit records (6.2.4.3.1.3)

##### First Annual Survey

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

##### Renewal (Special) Survey

The shipowner shall demonstrate to the *Register* the activities in 6.2.4.2.1.4.3 as per the Ship cyber resilience test procedure.

#### 6.2.4.2.2 Network protection safeguards

##### 6.2.4.2.2.1 Requirement

Security zones shall be protected by firewalls or equivalent means as specified in 6.2.4.2.1.

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 Head 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.

##### 6.2.4.2.2.2 Rational

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.

##### 6.2.4.2.2.3 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.

##### 6.2.4.2.2.4 Demonstration of compliance

###### 6.2.4.2.2.4.1 Design phase

No requirements.

###### 6.2.4.2.2.4.2 Construction phase

No requirements.

###### 6.2.4.2.2.4.3 Commissioning phase

The systems integrator shall submit Ship cyber resilience test procedure (ref. 6.2.5.2.1) and demonstrate the following to the *Register*:

- 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 6.3.5.7 and 6.3.6.3.4.7.

The second and third tests may be omitted if performed during the certification of CBSs as per 6.2.5.2.1.

###### 6.2.4.2.2.4.4 Operation phase

For general requirements to surveys in the operation phase, see 6.2.5.3.

##### Special Survey

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

##### 6.2.4.2.3 Antivirus, antimalware, antispam and other protections from malicious code

###### 6.2.4.2.3.1 Requirement

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

###### 6.2.4.2.3.2 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.

#### 6.2.4.2.3.3 Requirement details

Malware protection shall be implemented on CBSs in the scope of applicability of this Head. 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.

#### 6.2.4.2.3.4 Demonstration of compliance

##### 6.2.4.2.3.4.1 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.
- 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.

##### 6.2.4.2.3.4.2 Construction phase

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

##### 6.2.4.2.3.4.3 Commissioning phase

The systems integrator shall submit Ship cyber resilience test procedure (ref. 6.2.5.2.1) and demonstrate the following to the *Register*:

- 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 6.2.5.2.1.

##### 6.2.4.2.3.4.4 Operation phase

For general requirements to surveys in the operation phase, see 6.2.5.3.

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 Head:

- Maintenance/update (6.2.4.2.3.3)
- Operational procedures, physical safeguards (6.2.4.2.3.3)
- Use of mobile, portable, removable media (6.2.4.2.4.3.4 and 6.2.4.2.7.3)
- Access control (6.2.4.2.4)

#### First Annual Survey

The shipowner shall present to the *Register* 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.

#### Subsequent Annual Surveys

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

#### Renewal (Special) Survey

The shipowner shall demonstrate to the *Register* the activities in 6.2.4.2.3.4.3 as per the Ship cyber resilience test procedure.

#### 6.2.4.2.4 Access control

##### 6.2.4.2.4.1 Requirement

CBSs and networks in the scope of applicability of this Head 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.

##### 6.2.4.2.4.2 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.

#### 6.2.4.2.4.3 Requirement details

Access to CBSs and networks in the scope of applicability of this Head 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.

##### 6.2.4.2.4.3.1 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.

##### 6.2.4.2.4.3.2 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.

##### 6.2.4.2.4.3.3 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).

##### 6.2.4.2.4.3.4 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 6.2.4.2.7.

##### 6.2.4.2.4.3.5 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 on-shore 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 6.3.4.1 of 6.3. 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.

##### 6.2.4.2.4.3.6 Least privilege principle

Any human user allowed to access CBS and networks in the scope of applicability of this Head 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.

#### 6.2.4.2.4.4 Demonstration of compliance

##### 6.2.4.2.4.4.1 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.

##### 6.2.4.2.4.4.2 Construction phase

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

##### 6.2.4.2.4.4.3 Commissioning phase

The systems integrator shall submit Ship cyber resilience test procedure (ref. 6.2.5.2.1) and demonstrate the following to the *Register*:

- 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 6.2.5.2.1)

##### 6.2.4.2.4.4.4 Operation phase

For general requirements to surveys in the operation phase, see 6.2.5.3.

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 Head:

- Physical access control (6.2.4.2.4.3.1)
- Physical access control for visitors (6.2.4.2.4.3.2)
- Physical access control of network access points (6.2.4.2.4.3.3)
- Management of credentials (6.2.4.2.4.3.5)
- Least privilege policy (6.2.4.2.4.3.6)

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 Head:

- Confidential information (6.2.4.1.1.3)

- Information allowed to authorized personnel (6.2.4.2.4.3)
- Information transmitted on the wireless network (6.2.4.2.5.3)

#### First Annual Survey

The shipowner shall present to the *Register* 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 *Register* demonstrate implementation of the Ship cyber security and resilience program by presenting records or other documented evidence as specified for the first annual survey.

### **6.2.4.2.5 Wireless communication**

#### **6.2.4.2.5.1 Requirement**

Wireless communication networks in the scope of this Head 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

#### **6.2.4.2.5.2 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>).

#### **6.2.4.2.5.3 Requirement details**

Cryptographic mechanisms such as encryption algorithms and key lengths in accordance with industry stand-

ards 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 6.2.4.2.1 and protected as per 6.2.4.2.2.

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.

### **6.2.4.2.5.4 Demonstration of compliance**

#### **6.2.4.2.5.4.1 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 Head 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)

#### **6.2.4.2.5.4.2 Construction phase**

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

#### **6.2.4.2.5.4.3 Commissioning phase**

The systems integrator shall submit Ship cyber resilience test procedure (ref. 6.2.5.2.1) and demonstrate the following to the *Register*:

- 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 6.2.5.2.1.

#### **6.2.4.2.5.4.4 Operation phase**

For general requirements to surveys in the operation phase, see 6.2.5.3.

#### Renewal (Special) Survey

Subject to modifications of the wireless networks in the scope of applicability of this Head, the shipowner shall demonstrate to the *Register* the activities in 6.2.4.2.5.4.3 as per the Ship cyber resilience test procedure.

#### 6.2.4.2.6 Remote access control and communication with untrusted networks

##### 6.2.4.2.6.1 Requirement

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

##### 6.2.4.2.6.2 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.

##### 6.2.4.2.6.3 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 Head, 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.

##### 6.2.4.2.6.3.1 Design

CBSs in the scope of applicability of this Head 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.

##### 6.2.4.2.6.3.2 Additional requirements for remote maintenance

When remote access is used for maintenance, the following requirements shall be complied with in addition to those in 6.2.4.2.6.3.1:

- 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 6.3.5.2, 6.3.5.3 and 6.3.5.4.
- 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.

#### 6.2.4.2.6.4 Demonstration of compliance

##### 6.2.4.2.6.4.1 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 Head 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 6.2.4.2.6.3, as applicable.

##### 6.2.4.2.6.4.2 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.

##### 6.2.4.2.6.4.3 Commissioning phase

The systems integrator shall submit Ship cyber resilience test procedure (ref. 6.2.5.2.1) and demonstrate the following to the *Register*:

- Communication with untrusted networks is secured in accordance with 6.3.4.2 and that the communication protocols cannot be negotiated to a less secure version (demonstrate e.g., by use of a network protocol analyzer tool).
- 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 6.3.4.1 item 13).
- Instructions or procedures are provided by the respective product suppliers (see 6.3.3.1.3).

#### 6.2.4.2.6.4.4 Operation phase

For general requirements to surveys in the operation phase, see 6.2.5.3.

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 Head:

- User's manual (6.2.4.2.6.3)
- Roles and permissions (6.2.4.2.6.3)
- Patches and updates (6.2.4.2.6.3.2)
- Confirmation prior to undertaking remote software update (6.2.4.2.6.3.2)
- Interrupt, abort, roll back (6.2.4.2.6.3.2)

#### First Annual Survey

The shipowner shall present to the *Register* 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.

#### Subsequent Annual Surveys

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

#### Renewal (Special) Survey

The shipowner shall demonstrate to the *Register* the activities in 6.2.4.2.6.4.3 as per the Ship cyber resilience test procedure.

### 6.2.4.2.7 Use of Mobile and Portable Devices

#### 6.2.4.2.7.1 Requirement

The use of mobile and portable devices in CBSs in the scope of applicability of this Head shall be limited to only necessary activities and be controlled in accordance with 6.3.4.1 item 10. For any CBS that cannot fully meet these requirements, the interface ports shall be physically blocked.

#### 6.2.4.2.7.2 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.

#### 6.2.4.2.7.3 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.

#### 6.2.4.2.7.4 Demonstration of compliance

##### 6.2.4.2.7.4.1 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 6.3.4.1 item 10, i.e., that shall have protection of interface ports by physical means such as port blockers.

##### 6.2.4.2.7.4.2 Construction phase

The systems integrator shall ensure that use of physical interface ports in the CBSs is controlled in accordance with 6.3.4.1 item 10, and that any use of such devices follows procedures to prevent malware from being introduced in the CBS.

##### 6.2.4.2.7.4.3 Commissioning phase

The systems integrator shall submit Ship cyber resilience test procedure (ref. 6.2.5.2.1) and demonstrate to the *Register* 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
- 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

##### 6.2.4.2.7.4.4 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 Head:

- Policy and procedures (6.2.4.2.4.3.4)
- Physical block of interface ports (6.2.4.2.7.1)
- Use by authorized personnel (6.2.4.2.7.3)

- Connect only authorized devices (6.2.4.2.7.3)
- Consider risk of introducing malware (6.2.4.2.7.3)

First Annual Survey

The shipowner shall present to the *Register* 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 *Register* demonstrate implementation of the Ship cyber security and resilience program by presenting records or other documented evidence as specified for the first annual survey.

Renewal (Special) Survey

The shipowner shall demonstrate to the *Register* the activities in 6.2.4.2.7.4.3 as per the Ship cyber resilience test procedure.

**6.2.4.3 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.

**6.2.4.3.1 Network operation monitoring**

**6.2.4.3.1.1 Requirement**

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

**6.2.4.3.1.2 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.

**6.2.4.3.1.3 Requirement details**

Measures to monitor networks in the scope of applicability of this Head 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 the *Rules for the classification of ships, Part 12 – Electrical equipment*, 2.10.7.2.1.

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

**6.2.4.3.1.4 Demonstration of compliance**

**6.2.4.3.1.4.1 Design phase**

No requirements.

**6.2.4.3.1.4.2 Construction phase**

No requirements.

**6.2.4.3.1.4.3 Commissioning phase**

The systems integrator shall specify in the Ship cyber resilience test procedure and demonstrate to the *Register* 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 6.2.4.4.4.4.3.
- Demonstrate that the CBS will respond in a safe manner to network storm scenarios, considering both unicast and broadcast messages (see also 6.2.4.2.2.4.3)
- 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 6.2.5.2.1.

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

**6.2.4.3.1.4.4 Operation phase**

For general requirements to surveys in the operation phase, see 6.2.5.3.

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 Head:

- Reveal and recognize anomalous activity (6.2.4.3)

- Inspection of security audit records (6.2.4.3.1.3)
- Instructions or procedures to detect incidents (6.2.4.4.1.1)

The above activities may be addressed together with incident response in 6.2.4.4.1.

#### First Annual Survey

The shipowner shall present to the *Register* 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.

#### Subsequent Annual Surveys

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

#### Renewal (Special) Survey

Subject to modifications of the CBSs, the shipowner shall demonstrate to the *Register* the activities in 6.2.4.3.1.4.3 as per the Ship cyber resilience test procedure.

### **6.2.4.3.2 Verification and diagnostic functions of CBS and networks**

#### **6.2.4.3.2.1 Requirement**

CBSs and networks in the scope of applicability of this Head shall be capable to check performance and functionality of security functions required by this Head. 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.

#### **6.2.4.3.2.2 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.

#### **6.2.4.3.2.3 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.

#### **6.2.4.3.2.4 Demonstration of compliance**

##### **6.2.4.3.2.4.1 Design phase**

No requirements.

##### **6.2.4.3.2.4.2 Construction phase**

No requirements.

#### **6.2.4.3.2.4.3 Commissioning phase**

The systems integrator shall submit Ship cyber resilience test procedure (ref. 6.2.5.2.1) and demonstrate to the *Register* 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 6.2.5.2.1.

#### **6.2.4.3.2.4.4 Operation phase**

For general requirements to surveys in the operation phase, see 6.2.5.3.

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 Head:

- Test and maintenance periods (6.2.4.3.2.3)
- Periodic maintenance (6.2.5.3.3)

#### First Annual Survey

The shipowner shall present to the *Register* 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 *Register* demonstrate implementation of the Ship cyber security and resilience program by presenting records or other documented evidence as specified for the first annual survey.

### **6.2.4.4 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.

#### **6.2.4.4.1 Incident response plan**

##### **6.2.4.4.1.1 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 Head.

##### **6.2.4.4.1.2 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.

#### 6.2.4.4.1.3 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.

#### 6.2.4.4.1.4 Demonstration of compliance

##### 6.2.4.4.1.4.1 Design phase

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

- References to information provided by the suppliers (see 6.3.3.1.8) that may be applied by the shipowner to establish plans for incident response.

##### 6.2.4.4.1.4.2 Construction phase

No requirements.

##### 6.2.4.4.1.4.3 Commissioning phase

No requirements.

##### 6.2.4.4.1.4.4 Operation phase

For general requirements to surveys in the operation phase, see 6.2.5.3.

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 Head and shall address at least the following requirements in this Head:

- Description of who, when and how to respond to cyber incidents in accordance with requirements of 6.2.4.4.1
- Procedures or instructions for local/manual control in accordance with requirements in 6.2.4.4.2

- Procedures or instructions for isolation of security zones in accordance with requirements in 6.2.4.4.3
- Description of expected behaviour of the CBSs in the event of cyber incidents in accordance with requirements in 6.2.4.4.4.

##### First Annual Survey

The shipowner shall present to the *Register* 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 *Register* demonstrate implementation of the Ship cyber security and resilience program by presenting records or other documented evidence as specified for the first annual survey.

#### 6.2.4.4.2 Local, independent and/or manual operation

##### 6.2.4.4.2.1 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.

##### 6.2.4.4.2.2 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.

##### 6.2.4.4.2.3 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 6.2.4.2.1 and 6.2.4.2.2 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 Head.

**6.2.4.4.2.4 Demonstration of compliance****6.2.4.4.2.4.1 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 Regulation 31 are protected from cyber incidents in any connected remote or automatic control systems.

**6.2.4.4.2.4.2 Construction phase**

No requirements.

**6.2.4.4.2.4.3 Commissioning phase**

The systems integrator shall submit Ship cyber resilience test procedure (ref. 6.2.5.2.1) and demonstrate to the *Register* that the required local controls in the scope of applicability of this Head 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 6.2.5.2.1.

**6.2.4.4.2.4.4 Operation phase**

For general requirements to surveys in the operation phase, see 6.2.5.3.

Renewal (Special Survey)

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

**6.2.4.4.3 Network isolation****6.2.4.4.3.1 Requirement**

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

**6.2.4.4.3.2 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.

**6.2.4.4.3.3 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.

**6.2.4.4.3.4 Demonstration of compliance****6.2.4.4.3.4.1 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.

**6.2.4.4.3.4.2 Construction phase**

No requirements.

**6.2.4.4.3.4.3 Commissioning phase**

The systems integrator shall submit Ship cyber resilience test procedure (ref. 6.2.5.2.1) and demonstrate to the *Register* 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 6.2.5.2.1.

**6.2.4.4.3.4.4 Operation phase**

For general requirements to surveys in the operation phase, see 6.2.5.3.

Renewal (Special Survey)

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

**6.2.4.4.4 Fallback to a minimal risk condition****6.2.4.4.4.1 Requirement**

In the event of a cyber incident impairing the ability of a CBS or network in the scope of applicability of this Head 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.

**6.2.4.4.4.2 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.

**6.2.4.4.4.3 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.

#### 6.2.4.4.4.4 Demonstration of compliance

##### 6.2.4.4.4.4.1 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 Head.

##### 6.2.4.4.4.4.2 Construction phase

No requirements.

##### 6.2.4.4.4.4.3 Commissioning phase

The systems integrator shall submit Ship cyber resilience test procedure (ref. 6.2.5.2.1) and demonstrate to the *Register* that CBSs in the scope of applicability of this Head respond to cyber incidents in a safe manner (as per 6.2.4.4.4.4.1), 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 6.2.4.3.1.4.3.

The above tests may be omitted if performed during the certification of CBSs as per 6.2.5.2.1.

##### 6.2.4.4.4.4.4 Operation phase

For general requirements to surveys in the operation phase, see 6.2.5.3.

##### Renewal (Special) Survey

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

#### 6.2.4.5 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.

##### 6.2.4.5.1 Recovery plan

###### 6.2.4.5.1.1 Requirement

A recovery plan shall be made by the shipowner to support restoring CBSs under the scope of applicability of this Head 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.

###### 6.2.4.5.1.2 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.

##### 6.2.4.5.1.3 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.

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.

**6.2.4.5.1.4 Demonstration of compliance****6.2.4.5.1.4.1 Design phase**

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

- references to information provided by the suppliers (see 6.3.3.1.8) that may be applied by the shipowner to establish plans to recover from cyber incidents.

**6.2.4.5.1.4.2 Construction phase**

No requirements.

**6.2.4.5.1.4.3 Commissioning phase**

The systems integrator shall submit Ship cyber resilience test procedure (ref. 6.2.5.2.1) and demonstrate to the *Register* the effectiveness of the procedures and instructions provided by the suppliers to respond to cyber incidents as specified in 6.2.4.5.2 and 6.2.4.5.3.

The above tests may be omitted if performed during the certification of CBSs as per 6.2.5.2.1.

**6.2.4.5.1.4.4 Operation phase**

For general requirements to surveys in the operation phase, see 6.2.5.3.

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 Head and shall address at least the following requirements in this Head:

- Description of who, when and how to restore and recover from cyber incidents in accordance with requirements in 6.2.4.5.1
- 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 6.2.4.5.2.
- Reference to user manuals or procedures for backup, shutdown, reset, restore and restart of the CBSs in accordance with requirements in 6.2.4.5.2 and 6.2.4.5.3.

First Annual Survey

The shipowner shall present to the *Register* 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 *Register* demonstrate implementation of the Ship cyber security and resilience program by presenting records or other documented evidence as specified for the first annual survey.

**6.2.4.5.2 Backup and restore capability****6.2.4.5.2.1 Requirement**

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

**6.2.4.5.2.2 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.

**6.2.4.5.2.3 Requirement details****6.2.4.5.2.3.1 Restore capability**

CBSs in the scope of applicability of this Head 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.

**6.2.4.5.2.3.2 Backup**

CBSs and networks in the scope of applicability of this Head 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.

**6.2.4.5.2.4 Demonstration of compliance****6.2.4.5.2.4.1 Design phase**

No requirements.

**6.2.4.5.2.4.2 Construction phase**

No requirements.

**6.2.4.5.2.4.3 Commissioning phase**

The systems integrator shall submit Ship cyber resilience test procedure (ref. 6.2.5.2.1) and demonstrate to the *Register* the procedures and instructions for backup and restore provided by the suppliers for CBSs in the scope of applicability of this Head.

The above tests may be omitted if performed during the certification of CBSs as per 6.2.5.2.1.

#### 6.2.4.5.2.4.4 Operation phase

For general requirements to surveys in the operation phase, see 6.2.5.3.

##### Special survey

Subject to modifications of the CBSs, the shipowner shall demonstrate to the *Register* the activities in 6.2.4.5.2.4.3 as per the Ship cyber resilience test procedure.

#### 6.2.4.5.3 Controlled shutdown, reset, roll-back and restart

##### 6.2.4.5.3.1 Requirement

CBS and networks in the scope of applicability of this Head 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.

##### 6.2.4.5.3.2 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 and 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.

##### 6.2.4.5.3.3 Requirement details

CBS and networks in the scope of applicability of this Head 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.

#### 6.2.4.5.3.4 Demonstration of compliance

##### 6.2.4.5.3.4.1 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 Head.

##### 6.2.4.5.3.4.2 Construction phase

No requirements.

##### 6.2.4.5.3.4.3 Commissioning phase

The systems integrator shall submit Ship cyber resilience test procedure (ref. 6.2.5.2.1) and demonstrate to the *Register* that manuals or procedures are established for shutdown, reset and restore of the CBSs in the scope of applicability of this Head. These manuals/procedures shall be provided to the shipowner.

The above tests may be omitted if performed during the certification of CBSs as per 6.2.5.2.1.

##### 6.2.4.5.3.4.4 Operation phase

For general requirements to surveys in the operation phase, see 6.2.5.3.

##### Renewal (Special) Survey

Subject to modifications of the CBSs, the shipowner shall demonstrate to the *Register* the activities in 6.2.4.5.3.4.3 as per the Ship cyber resilience test procedure.

#### 6.2.5 Demonstration of compliance

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

Documentation to be submitted by suppliers to the *Register* is specified in 6.3. The approved versions of this

documentation shall also be provided by the suppliers to the systems integrator as specified in 6.3.6.2.

Documents to be provided by the systems integrator are listed in 6.2.5.1 and 6.2.5.2.

Documents to be provided by the shipowner are listed in 6.2.5.3.

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

- Documentation of the CBSs provided by the suppliers (see 6.3.6.2)
- Documentation produced by the systems integrator (see 6.2.5.1 and 6.2.5.2)

#### 6.2.5.1 During design and construction phases

The supplier shall demonstrate compliance to the *Register* by following the certification process specified in 6.3.6.

The systems integrator shall demonstrate compliance by submitting documents in the following subsections to the *Register* 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 the *Rules for the classification of ships, Part 12 – Electrical equipment, 2.10*.

##### 6.2.5.1.1 Zones and conduit diagram

The content of this document is specified in 6.2.4.2.1.4.1.

##### 6.2.5.1.2 Cyber security design description (CSDD)

The content of this document is specified in subsections “Design phase” for each requirement in 6.2.4.

##### 6.2.5.1.3 Vessel asset inventory

The content of this document is specified in section 4.1.1.

##### 6.2.5.1.4 Risk assessment for the exclusion of CBSs

The content of this document is specified in 6.2.6.

##### 6.2.5.1.5 Description of compensating countermeasures

If any CBS in the scope of applicability of this Head has been approved with compensating countermeasures in lieu of a requirement in 6.3, this document shall specify the respective CBS, the lacking security capability, as well as provide a detailed description of the compensating countermeasures. See also 6.3.3.1.3 requiring that the supplier describes such compensating countermeasures in the system documentation.

#### 6.2.5.2 Upon ship commissioning

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

1. Submit updated design documentation to the *Register* (as-built versions of the documents in 6.2.5.1)
2. Submit Ship cyber resilience test procedure to the *Register* describing how to demonstrate compliance with this Head by testing and/or analytic evaluation.

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

#### 6.2.5.2.1 Ship cyber resilience test procedure

The content of this document is specified for the Commissioning phase in each subsection “Demonstration of compliance” in 6.2.4.

For each CBS, the required inherent security capabilities and configuration thereof are verified and tested in the certification process of each CBS (see 6.3). 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 6.3. Nevertheless, all tests shall be included in the Ship cyber resilience test procedure and the decision to omit tests will be taken by the *Register*. 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 6.2.5.1.2.

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

Before submitting the Ship cyber resilience test procedure to the *Register*, 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 *Register* may request execution of additional tests.

#### 6.2.5.3 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 Head.

Modifications to the CBSs in scope of applicability of this Head shall be carried out in accordance with the management of change (MoC) requirements in 6.3. 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 *Register*.

#### 6.2.5.3.1 First annual survey

In due time before the first annual survey of the ship, the shipowner shall submit to the *Register* 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 Head.

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 Head.

After the *Register* 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 of the 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.

#### 6.2.5.3.2 Subsequent annual surveys

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

#### 6.2.5.3.3 Renewal (Special) survey

Upon renewal of the ship's classification certificate, the shipowner shall carry out testing witnessed by the *Register* 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 *Register* based on modifications to the CBSs as specified in subsections "Operation phase" in 6.2.4.

### 6.2.6 Risk assessment for exclusion of CBS from the application of requirements

#### 6.2.6.1 Requirement

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

#### 6.2.6.2 Rationale

Exclusion of a CBS falling under the scope of applicability of this Head from the application of relevant requirements needs to be duly justified and documented. Such exclusion can be accepted by the *Register* 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.

#### 6.2.6.3 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 *Register* 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;

- 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).

#### 6.2.6.4 Acceptance criteria

Exclusion of a CBS falling under the scope of applicability of this Head from the application of relevant requirements can be accepted by the *Register* 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 *Register*. The *Register* 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 Head:

- 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 Head (see 6.2.1.3)

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;

## 6.3 CYBER RESILIENCE OF ON-BOARD SYSTEMS AND EQUIPMENT

### 6.3.1 General

#### 6.3.1.1 Introduction

Technological evolution of vessels, ports, container terminals, etc. and increased reliance upon Operational Technology (OT) and Information Technology (IT) has created an increased possibility of cyber-attacks to affect business, personnel data, human safety, the safety of the ship, and also possibly threaten the marine environment. Safeguarding shipping from current and emerging threats must involve a range

of controls that are continually evolving which would require incorporating security features in the equipment and systems at design and manufacturing stage. It is therefore necessary to establish a common set of minimum requirements to deliver systems and equipment that can be described as cyber resilient.

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

#### 6.3.1.2 Limitations

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

- UR E10 for environmental performance for the system hardware
- the *Rules for the classification of ships, Part 12 – Electrical equipment*, 2.10 for safety of equipment for the functionality of the software

#### 6.3.1.3 Scope of applicability

The requirements specified in this Head are applicable to computer based systems specified in 6.2 for the following types of vessels:

Mandatory requirements for

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

Non-mandatory guidance to:

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

For navigation and radiocommunication systems, the application of IEC 61162-460 or other equivalent standards in lieu of the required security capabilities in 6.3.4 may be accepted by the *Register*, on the condition that requirements in 6.2 are complied with.

#### 6.3.1.3.1 Information and Communication Technology (ICT)

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

- the *Rules for the classification of ships, Part 12 – Electrical equipment*, 2.10

- Requirements given in 6.2
- IACS Recommendation No. 166

#### 6.3.1.4 Definitions & Abbreviations

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

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

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

**Computer Based System (CBS):** A programmable electronic device, or interoperable set of programmable electronic devices, organized to achieve one or more specified purposes such as collection, processing, maintenance, use, sharing, dissemination, or disposition of information. CBS on-board include IT and OT systems. A CBS may be a combination of subsystems connected via network. On-board CBS may be connected directly or via public means of communications (e.g. Internet) to ashore CBSs, other vessels' CBS and/or other facilities.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

**System Categories (I, II, III):** System categories based on their effects on system functionality, which are defined in the *Rules for the classification of ships, Part 12 – Electrical equipment*, 2.10.

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

**Untrusted network:** Any network outside the scope of applicability of this Head.

## 6.3.2 Security Philosophy

### 6.3.2.1 Systems and Equipment

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

**6.3.2.1.2** Equipment may be one of the following:

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

### 6.3.2.2 Cyber Resilience

The cyber resilience requirements in 6.3.4 will be applicable for all systems in scope of UR E26 as applicable. Additional requirements related to interface with untrusted networks will only apply for systems where such connectivity is designed.

### 6.3.2.3 Essential Systems Availability

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

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

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

### 6.3.2.4 Compensating Countermeasures

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

Compensating countermeasure(s) shall meet the intent and rigor of the original stated requirement considering the referenced standards as well as the differences between each requirement and the related items in the standards, and follow the principles specified in 6.3.3.1.3.

## 6.3.3 Documentation

### 6.3.3.1 CBS Documentation

The following documents shall be submitted to the *Register* for review and approval in accordance with the requirements in this Head. See also 6.3.6.2.

#### 6.3.3.1.1 CBS asset inventory (see IACS Rec. 190)

The CBS asset inventory shall include the information below.

List of hardware components (e.g., host devices, embedded devices, network devices):

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

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

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

#### 6.3.3.1.2 Topology diagrams

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

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

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

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

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

### 6.3.3.1.3 Description of security capabilities

This document shall describe how the CBS with its hardware and software components meets the required security capabilities in 6.3.4.1.

Any network interfaces to other CBSs in the scope of applicability of 6.2 shall be described. The description shall include destination CBS, data flows, and communication protocols. If the System integrator has allocated the destination CBS to another security zone, components providing protection of the security zone boundary (see 6.2.4.2.2.1) shall be described in detail if delivered as part of the CBS.

Any network interfaces to other systems or networks outside the scope of applicability of 6.2 (untrusted networks) shall be described. The description shall specify compliance with the additional security capabilities in 6.3.4.2, and include relevant procedures or instructions for the crew. Components providing protection of the security zone boundary (see 6.2.4.2.2.1) shall be described in detail if delivered as part of the CBS.

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

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

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

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

### 6.3.3.1.4 Test procedure of security capabilities

This document shall describe how to demonstrate by testing that the system complies with the requirements in 6.3.4.1 and 6.3.4.2, including any compensating countermeasures. Demonstration of compliance by analytic evaluation may be specially considered. The procedure shall include a separate chapter for each applicable requirement and describe:

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

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

### 6.3.3.1.5 Security configuration guidelines

This document shall describe recommended configuration settings of the security capabilities and specify default values. The objective is to ensure the security capabilities are implemented in accordance with 6.2 and any specifications by the System integrator (e.g. user accounts, authorisation, password policies, safe state of machinery, firewall rules, etc.)

The document shall serve as basis for verification of item no. 29 in 6.3.4.1.

### 6.3.3.1.6 Secure development lifecycle documents

This documentation shall be submitted to the *Register* upon request and shall describe the supplier's processes and controls in accordance with requirements for secure development lifecycle in 6.3.5. Software updates and patching shall be described. The document shall prepare the *Register* for survey as per 6.3.6.3.4.

### 6.3.3.1.7 Plans for maintenance and verification of the CBS

This document shall be submitted to the *Register* upon request and shall include procedures for security-related maintenance and testing of the system. The document shall include instructions for how the user can verify correct operation of the system's security functions as required by item no.19 in 6.3.4.1.

### 6.3.3.1.8 Information supporting the owner's incident response and recovery plan

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

- Local independent control (see 6.2.4.4.2)
- Network isolation (see 6.2.4.4.3)
- Forensics by use of audit records (see 6.3.4.1 item no.13)
- Deterministic output (see 6.2.4.4.4 and 6.3.4.1 item no. 20)
- Backup (see 6.3.4.1 item no. 26)
- Restore (see 6.3.4.1 item no. 27)
- Controlled shutdown, reset, roll-back and restart (see 6.2.4.5.3)

### 6.3.3.1.9 Management of change plan

This document shall be submitted to the *Register* upon request. It is expected that this procedure is not specific for cyber security and is also required by the *Rules for the classification of ships, Part 12 – Electrical equipment*, 2.10.

### 6.3.3.1.10 Test reports

CBSs with Type approval certificate covering the security capabilities of this Head may be exempted from survey by the *Register*. However, test reports signed by the supplier shall be submitted to the *Register*, demonstrating that the supplier has completed design, construction, testing, configuration, and hardening as would otherwise be verified by the *Register* in survey (6.3.6.3).

## 6.3.4 System Requirements

This Head specifies the required security capabilities for CBSs in the scope specified in 6.3.1.3.

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

### 6.3.4.1 Required security capabilities

The following security capabilities are required for all CBSs in the scope specified in 6.3.1.3.

Table 6.3.4.1

Item No.	Objective	Requirements
Protect against casual or coincidental access by unauthenticated entities		
1	Human user identification and authentication	The CBS shall identify and authenticate all human users who can access the system directly or through interfaces (IEC 62443-3-3/SR 1.1)
2	Account management	The CBS shall provide the capability to support the management of all accounts by authorized users, including adding, activating, modifying, disabling and removing account (IEC 62443-3-3/SR 1.3)
3	Identifier management	The CBS shall provide the capability to support the management of identifiers by user, group and role. (IEC 62443-3-3/SR 1.4)
4	Authenticator management	The CBS shall provide the capability to: <ul style="list-style-type: none"> <li>- Initialize authenticator content</li> <li>- Change all default authenticators upon control system installation</li> <li>- Change/refresh all authenticators</li> <li>- Protect all authenticators from unauthorized disclosure and modification when stored and transmitted.</li> </ul> (IEC 62443-3-3/SR 1.5)
5	Wireless access management	The CBS shall provide the capability to identify and authenticate all users (humans, software processes or devices) engaged in wireless communication (IEC 62443-3-3/SR 1.6)
6	Strength of password-based authentication	The CBS shall provide the capability to enforce configurable password strength based on minimum length and variety of character types. (IEC 62443-3-3/SR 1.7)
7	Authenticator feedback	The CBS shall obscure feedback during the authentication process. (IEC 62443-3-3/SR 1.10)
Protect against casual or coincidental misuse		
8	Authorization enforcement	On all interfaces, human users shall be assigned authorizations in accordance with the principles of segregation of duties and least privilege. (IEC 62443-3-3/SR 2.1)
9	Wireless use control	The CBS shall provide the capability to authorize, monitor and enforce usage restrictions for wireless connectivity to the system according to commonly accepted security industry practices (IEC 62443-3-3/SR 2.2)
10	Use control for portable and mobile devices	When the CBS supports use of portable and mobile devices, the system shall include the capability to <ol style="list-style-type: none"> <li>a) Limit the use of portable and mobile devices only to those permitted by design</li> <li>b) Restrict code and data transfer to/from portable and mobile devices</li> </ol> Note: Port limits / blockers (and silicone) could be accepted for a specific system (IEC 62443-3-3/SR 2.3)
11	Mobile code	The CBS shall control the use of mobile code such as java scripts, ActiveX and PDF. (IEC 62443-3-3/SR 2.4)
12	Session lock	The CBS shall be able to prevent further access after a configurable time of inactivity or following activation of manual session lock. (IEC 62443-3-3/SR 2.5)
13	Auditable events	The CBS shall generate audit records relevant to security for at least the following events: access control, operating system events, backup and restore events, configuration changes, loss of communication. (IEC 62443-3-3/SR 2.8)
14	Audit storage capacity	The CBS shall provide the capability to allocate audit record storage capacity according to commonly recognized recommendations for log management. Auditing mechanisms shall be implemented to reduce the likelihood of such capacity being exceeded. (IEC 62443-3-3/SR 2.9)

Item No.	Objective	Requirements
15	Response to audit processing failures	The CBS shall provide the capability to prevent loss of essential services and functions in the event of an audit processing failure. (IEC 62443-3-3/SR 2.10)
16	Timestamps	The CBS shall timestamp audit records. (IEC 62443-3-3/SR 2.11)
Protect the integrity of the CBS against casual or coincidental manipulation		
17	Communication integrity	The CBS shall protect the integrity of transmitted information. Note: Cryptographic mechanisms shall be employed for wireless networks. (IEC 62443-3-3/SR 3.1)
18	Malicious code protection	The CBS shall provide capability to implement suitable protection measures to prevent, detect and mitigate the effects due to malicious code or unauthorized software. It shall have the feature for updating the protection mechanisms (IEC 62443-3-3/SR 3.2)
19	Security functionality verification	The CBS shall provide the capability to support verification of the intended operation of security functions and report when anomalies occur during maintenance (IEC 62443-3-3/SR 3.3)
20	Deterministic output	The CBS shall provide the capability to set outputs to a predetermined state if normal operation cannot be maintained as a result of an attack. The predetermined state could be: <ul style="list-style-type: none"> <li>- Unpowered state,</li> <li>- Last-known value, or</li> <li>- Fixed value</li> </ul> (IEC 62443-3-3/SR 3.6)
Prevent the unauthorized disclosure of information via eavesdropping or casual exposure		
21	Information confidentiality	The CBS shall provide the capability to protect the confidentiality of information for which explicit read authorization is supported, whether at rest or in transit. Note: For wireless network, cryptographic mechanisms shall be employed to protect confidentiality of all information in transit. (IEC 62443-3-3/SR 4.1)
22	Use of cryptography	If cryptography is used, the CBS shall use cryptographic algorithms, key sizes and mechanisms according to commonly accepted security industry practices and recommendations. (IEC 62443-3-3/SR 4.3)
Monitor the operation of the CBS and respond to incidents		
23	Audit log accessibility	The CBS shall provide the capability for accessing audit logs on read only basis by authorized humans and/or tools. (IEC 62443-3-3/SR 6.1)
Ensure that the control system operates reliably under normal production conditions		
24	Denial of service protection	The CBS shall provide the minimum capability to maintain essential functions during DoS events. Note: It is acceptable that the CBS may operate in a degraded mode upon DoS events, but it shall not fail in a manner which may cause hazardous situations. Overload-based DoS events should be considered, i.e. where the networks capacity is attempted flooded, and where the resources of a computer is attempted consumed. (IEC 62443-3-3/SR 7.1)
25	Resource management	The CBS shall provide the capability to limit the use of resources by security functions to prevent resource exhaustion. (IEC 62443-3-3/SR 7.2)
26	System backup	The identity and location of critical files and the ability to conduct backups of user-level and system-level information (including system state information) shall be supported by the CBS without affecting normal operations (IEC 62443-3-3/SR 7.3)

Item No.	Objective	Requirements
27	System recovery and re-constitution	The CBS shall provide the capability to be recovered and reconstituted to a known secure state after a disruption or failure. (IEC 62443-3-3/SR 7.4)
28	Alternative power source	The CBS shall provide the capability to switch to and from an alternative power source without affecting the existing security state or a documented degraded mode. (IEC 62443-3-3/SR 7.5)
29	Network and security configuration settings	The CBS shall provide the capability to be configured according to recommended network and security configurations as described in guidelines provided by the supplier. The CBS shall provide an interface to the currently deployed network and security configuration settings. (IEC 62443-3-3/SR 7.6)
30	Least Functionality	The installation, the availability and the access rights of the following shall be limited to the strict needs of the functions provided by the CBS: - operating systems software components, processes and services - network services, ports, protocols, routes and hosts accesses and any software (IEC 62443-3-3/SR 7.7)

#### 6.3.4.2 Additional security capabilities

The following additional security capabilities are required for CBSs with network communication to untrusted networks (i.e. interface to any networks outside the scope of 6.2).

CBSs with communication traversing the boundaries of security zones shall also meet requirements for network segmentation and zone boundary protection in 6.2.4.2.1 and 6.2.4.2.2.

Table 6.3.4.2

Item No.	Objective	Requirements
31	Multifactor authentication for human users	Multifactor authentication is required for human users when accessing the CBS from or via an untrusted network. (IEC 62443-3-3/SR 1.1, RE 2)
32	Software process and device identification and authentication	The CBS shall identify and authenticate software processes and devices (IEC 62443-3-3/SR 1.2)
33	Unsuccessful login attempts	The CBS shall enforce a limit of consecutive invalid login attempts from untrusted networks during a specified time period. (IEC 62443-3-3/SR 1.11)
34	System use notification	The CBS shall provide the capability to display a system use notification message before authenticating. The system use notification message shall be configurable by authorized personnel. (IEC 62443-3-3/SR 1.12)
35	Access via Untrusted Networks	Any access to the CBS from or via untrusted networks shall be monitored and controlled. (IEC 62443-3-3/SR 1.13)
36	Explicit access request approval	The CBS shall deny access from or via untrusted networks unless explicitly approved by authorized personnel on board. (IEC 62443-3-3/SR 1.13, RE1)
37	Remote session termination	The CBS shall provide the capability to terminate a remote session either automatically after a configurable time period of inactivity or manually by the user who initiated the session. (IEC 62443-3-3/SR 2.6)
38	Cryptographic integrity protection	The CBS shall employ cryptographic mechanisms to recognize changes to information during communication with or via untrusted networks. (IEC 62443-3-3/SR 3.1, RE1)
39	Input validation	The CBS shall validate the syntax, length and content of any input data via untrusted networks that is used as process control input or input that directly impacts the action of the CBS. (IEC 62443-3-3/SR 3.5)
40	Session integrity	The CBS shall protect the integrity of sessions. Invalid session IDs shall be rejected. (IEC 62443-3-3/SR 3.8)
41	Invalidation of session IDs after session termination	The system shall invalidate session IDs upon user logout or other session termination (including browser sessions). (IEC 62443-3-3/SR 3.8, RE1)

### 6.3.5 Secure Development Lifecycle Requirements

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

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

A document shall be produced that records how the security aspects have been addressed in above phases and shall at minimum integrate controlled processes as set out in below 6.3.5.1 to 6.3.5.7. The said document is required to be submitted to class for review and approval.

**6.3.5.1** (IEC 62443-4-1/SM-8) The manufacturer shall have procedural and technical controls in place to protect private keys used for code signing, if applicable, from unauthorized access or modification.

**6.3.5.2** (IEC 62443-4-1/SUM-2) A process shall be employed to ensure that documentation about product security updates is made available to users (which could be through

establishing a cyber security point of contact or periodic publication which can be accessed by the user) that includes but is not limited to:

- a) The product version number(s) to which the security patch applies;
- b) Instructions on how to apply approved patches manually and via an automated process;
- c) Description of any impacts that applying the patch to the product can have, including reboot;
- d) Instructions on how to verify that an approved patch has been applied; and
- e) Risks of not applying the patch and mitigations that can be used for patches that are not approved or deployed by the asset owner.

**6.3.5.3** (IEC 62443-4-1/SUM-3) A process shall be employed to ensure that documentation about dependent component or operating system security updates is available to users that includes but is not limited to:

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

**6.3.5.4** (IEC 62443-4-1/SUM-4) A process shall be employed to ensure that security updates for all supported products and product versions are made available to product users in a manner that facilitates verification that the security patch is authentic.

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

**6.3.5.5** (IEC 62443-4-1/SG-1) A process shall exist to create product documentation that describes the security defence in depth strategy for the product to support installation, operation and maintenance that includes:

- a) Security capabilities implemented by the product and their role in the defence in depth strategy;
- b) Threats addressed by the defence in depth strategy; and
- c) Product user mitigation strategies for known security risks associated with the product, including risks associated with legacy code.

**6.3.5.6** (IEC 62443-4-1/SG-2) A process shall be employed to create product user documentation that describes the security defence in depth measures expected to be provided by the external environment in which the product is to be used.

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

- a) Integration of the product, including third-party components, with its product security context
- b) Integration of the product's application programming interfaces/protocols with user applications;

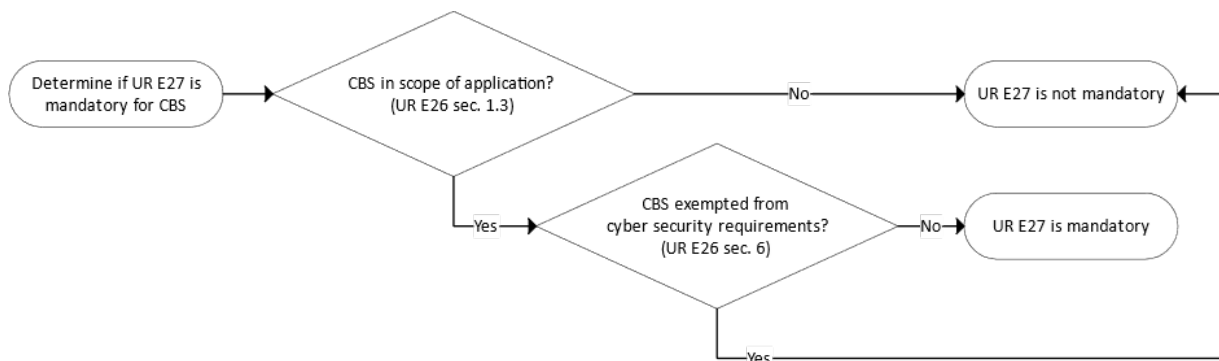
- c) Applying and maintaining the product's defence in depth strategy
- d) Configuration and use of security options/capabilities in support of local security policies, and for each security option/capability:
  - i. its contribution to the product's defence in depth strategy
  - ii. descriptions of configurable and default values that include how each affects security along with any potential impact each has on work practices; and
  - iii. setting/changing/deleting its value;
- e) Instructions and recommendations for the use of all security-related tools and utilities that support administration, monitoring, incident handling and evaluation of the security of the product;
- f) Instructions and recommendations for periodic security maintenance activities;
- g) Instructions for reporting security incidents for the product to the supplier;
- h) Description of the security best practices for maintenance and administration of the product.

## 6.3.6 Demonstration of compliance

### 6.3.6.1 Introduction

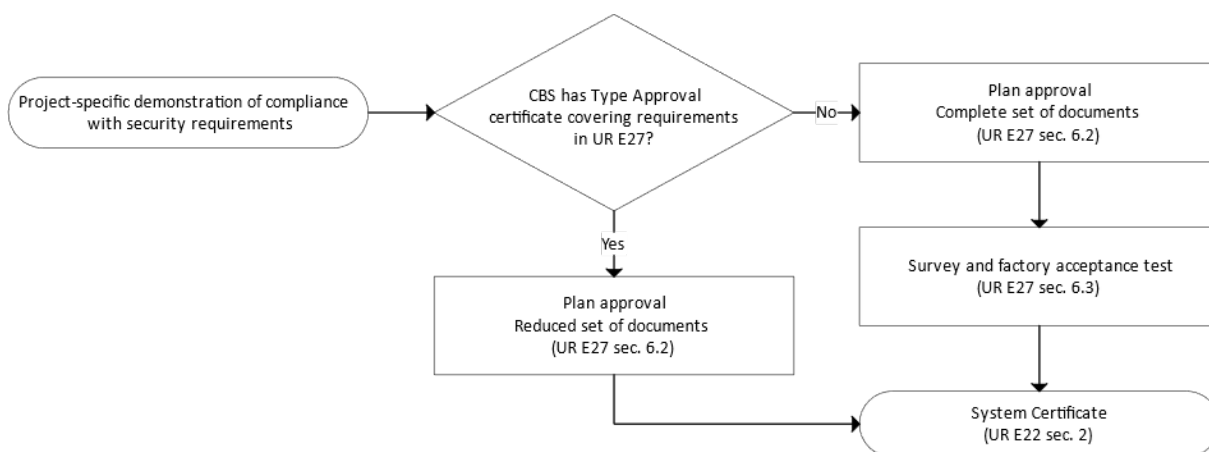
Suppliers shall in cooperation with the System integrator determine if this Head is mandatory for the CBS, see Figure 6.3.6.1-1.

Figure 6.3.6.1-1



Compliance with security requirements shall be demonstrated as indicated in Figure 6.3.6.1-2. This classification process is ship-specific and shall result in a System certificate.

Figure 6.3.6.1-2



Type approval is voluntary and applies for CBSs that are standard and routinely manufactured. See the *Rules for the classification of ships, Part 12 – Electrical equipment, 2.10* for definition of System certification and Type approval.

The process in Figure 6.3.6.1-1 and Figure 6.3.6.1-2 applies also if other equivalent standards are applied for navigation and radiocommunication equipment (see 6.3.1.3). In such case:

- the process in Figure 6.3.6.1-1 illustrates if the equivalent standard is mandatory (in lieu of requirements of this Head)
- the process in Figure 6.3.6.1-2 illustrates that the certification process is lessened if the CBS has been type approved in accordance with the equivalent standard.

### 6.3.6.2 Plan approval

Plan approval is assessment of documents of a CBS intended for a specific vessel. The documents in 6.3.3 are required to be submitted by the supplier. The documents shall enable the *Register* to verify compliance with requirements in this Head.

If the CBS holds a valid Type approval certificate covering the requirements of this Head, subject to approval by the *Register*, the supplier may submit a reduced set of vessel-specific documents to the *Register*.

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

### 6.3.6.3 Survey and factory acceptance test

Survey and factory acceptance testing (FAT) is a vessel-specific verification activity required for CBSs that do

not hold a valid Type approval certificate covering the requirements of this Head.

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

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

The following subsections specify the survey and FAT activities.

#### **6.3.6.3.1 General survey items**

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

It shall also be demonstrated that the system to be delivered is correctly represented by the approved documentation. This shall be done by inspecting the system and comparing the components and arrangement/architecture with the asset inventory (6.3.3.1.1) and the topology diagrams (6.3.3.1.2).

#### **6.3.6.3.2 Test of security capabilities**

The supplier shall test the required security capabilities on the system to be delivered. The tests shall be carried out in accordance with the approved test procedure in 6.3.3.1.4 and be witnessed/accepted by the *Register* surveyor.

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

#### **6.3.6.3.3 Correct configuration of security capabilities**

The supplier shall test/demonstrate for the class surveyor that security settings in the system's components have been configured in accordance with the configuration guidelines in 6.3.3.1.5. This demonstration may be carried out in conjunction with testing of the security capabilities.

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

#### **6.3.6.3.4 Secure development lifecycle**

The supplier shall, in accordance with documentation in 6.3.3.1.6, demonstrate compliance with requirements for secure development lifecycle in 6.3.5.

#### **6.3.6.3.4.1 Controls for private keys (IEC 62443-4-1/SM-8)**

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

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

The policies and procedures shall address roles, responsibilities and work processes. The technical controls shall include e.g. physical access restrictions and cryptograph-

ic hardware (e.g. Hardware security module) for storage of the private key.

#### **6.3.6.3.4.2 Security update documentation (IEC 62443-4-1/SUM-2)**

The supplier shall present management system documentation substantiating that a process is established in the organization to ensure security updates are informed to the users. The information to the users shall include the items listed in 6.3.5.2.

#### **6.3.6.3.4.3 Dependent component security update documentation (IEC 62443-4-1/SUM-3)**

The supplier shall present management system documentation, as required by 6.3.5.3, substantiating that a process is established in the organization to ensure users are informed whether the system is compatible with updated versions of acquired software in the system (new versions/patches of operating system or firmware). The information shall address how to manage risks related to not applying the updated acquired software.

#### **6.3.6.3.4.4 Security update delivery (IEC 62443-4-1/SUM-4)**

The supplier shall present management system documentation, as required by 6.3.5.4, substantiating that a process is established in the organization ensuring that system security updates are made available to users, and describing how the user may verify the authenticity of the updated software.

#### **6.3.6.3.4.5 Product defence in depth (IEC 62443-4-1/SG-1)**

The supplier shall present management system documentation, as required by 6.3.5.5, substantiating that a process is established in the organization to document a strategy for defence-in-depth measures to mitigate security threats to software in the CBS during installation, maintenance and operation.

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

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

The supplier shall present management system documentation, as required by 6.3.5.6, substantiating that a process is established in the organization to document defence-in-depth measures expected to be provided by the external environment, such as physical arrangement, policies and procedures.

#### **6.3.6.3.4.7 Security hardening guidelines (IEC 62443-4-1/SG-3)**

The supplier shall present management system documentation, as required by 6.3.5.7, substantiating that a process is established in the organization to ensure that hardening guidelines are produced for the system.

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

## 6.4 TECHNICAL DOCUMENTATION

Technical documentation required to be submitted to the Register for the purpose of the assignment of subject descriptive class note are listed in IACS UR E26 - Appendix II and IACS UR E27 - Appendix II.

## 6.5 PERIODICAL CLASS SURVEYS

6.5.1 Specific requirements for periodical class surveys for the purpose of the maintenance of subject descriptive class note are listed in Table 6.5.1

Table 6.5.1 - Requirements for periodical class surveys

Head 6.2	Systems integrator			Shipowner			
	Design	Construction	Commissioning	Operation	First Annual Survey	Annual Survey	Renewal (Special Survey)
Approved supplier documentation [6.2.5]		Maintain	Maintain	Maintain			
Zones and conduit diagram [6.2.5.1.1]	Submit	Maintain	Maintain	Maintain			
Cyber security design description [6.2.5.1.2]	Submit	Maintain	Maintain	Maintain			
Vessel asset inventory [6.2.5.1.3]	Submit	Maintain	Maintain	Maintain			
Risk assessment for the exclusion of CBSs [6.2.5.1.4] <sup>NOTE 1</sup>	Submit	Maintain	Maintain	Maintain			
Description of compensating countermeasures [6.2.5.1.5] <sup>NOTE 1</sup>	Submit	Maintain	Maintain	Maintain			
Ship cyber resilience test procedure [6.2.5.2.1]		Submit	Demonstrate	Maintain			Demonstrate
Ship cyber security and resilience program [6.2.5.3.1] - Management of change (MoC) [6.2.4.1.1.4.4] - Management of software updates [6.2.4.1.1.4.4] - Management of firewalls [6.2.4.2.1.4.4] - Management of malware protection [6.2.4.2.3.4.4] - Management of access control [6.2.4.2.4.4.4] - Management of confidential information [6.2.4.2.4.4.4] - Management of remote access [6.2.4.2.6.4.4] - Management of mobile and portable devices [6.2.4.2.7.4.4] - Detection of security anomalies [6.2.4.3.1.4.4] - Verification of security functions [6.2.4.3.2.4.4] - Incident response plans [6.2.4.4.1.4.4] - Recovery plans [6.2.4.5.1.4.4]				Maintain	Submit	Demonstrate	
NOTE 1: If applicable							
LEGEND:							
<b>Submit:</b> The stakeholder shall submit the document to the <i>Register</i> for verification and approval of compliance with requirements in this Head.							
<b>Maintain:</b> The stakeholder shall submit the document to the <i>Register</i> for verification and approval of compliance with requirements in this Head							
<b>Demonstrate:</b> The stakeholder shall demonstrate compliance to the <i>Register</i> in accordance with the approved document.							

## 7 SHIPS CARRYING INDUSTRIAL PERSONNEL

### 7.1 GENERAL

**7.1.1** Descriptive class note **Carriage of Industrial Personnel** may be assigned to a main ship type notation when the ship complies with IMO MSC.527(106), "International Code of Safety for Ships Carrying Industrial Personnel (IP Code)" carrying more than twelve (12) industrial personnel, and when Industrial Personnel Safety Certificate has been issued.

**7.1.2** For the purpose of this Section the following definitions should apply:

- .1 Industrial personnel means all persons transported or accommodated on board for the purpose of offshore industrial activities performed on board other ships and/or offshore facilities.
- .2 Carriage means transportation, accommodation, or both.
- .3 Offshore industrial activities mean the construction, maintenance, decommissioning, operation, or servicing of offshore facilities related, but not limited, to exploration and exploitation of resources by the renewable or hydrocarbon energy sectors, aquaculture, ocean mining or similar activities.
- .4 Personnel transfer means the full sequence of the operation of transferring personnel and their equipment at sea to or from a ship to which IP Code applies and from or to another ship or an offshore facility.

**7.1.3** Regarding requirements for the harmonization of the Industrial Personnel Safety Certificate with SOLAS Safety Certificates, refer to:

- .1 IACS UI SC 303 (*Harmonisation of Industrial Personnel Safety Certificates with SOLAS Safety Certificates*); and
- .2 IMO MSC.1/Circ.1680 (*Unified interpretations of SOLAS Regulation XV/5.1 and paragraph 3.5 of part 1 of the International Code of Safety for Ships Carrying Industrial Personnel (IP Code) on the Harmonization of the Industrial Personnel Safety Certificate with SOLAS Safety Certificates*).

### 7.2 APPLICATION

**7.2.1** Descriptive class note **Carriage of Industrial Personnel** applies to either new, or existing cargo ships or high-speed cargo crafts, of  $GT \geq 500$ , engaged in international voyages and that carry an aggregate number of industrial personnel, special personnel and passengers exceeding 12 persons, and when complying with the IP Code.

## 7.3 REQUIREMENTS FOR THE ASSIGNMENT

### 7.3.1 General

The requirements for the assignment of the subject descriptive class note consists of:

- .1 General requirements contained in the *Rules for the classification of ships, Part 1 – General requirements*.
- .2 Specific requirements related to the assigned main ship type notation as contained in the relevant parts of the *Rules for the classification of ships*.
- .3 Goals and functional requirements stated in the Part II of the IP Code.
- .4 Relevant safety objectives of SOLAS, or the basic safety principles of the HSC Code, as appropriate.

### 7.3.2 Additional regulations for cargo ships

**7.3.2.1** Subdivision and stability. In order to meet the functional requirements from paragraph II/3.2.1 of the IP Code, the following applies:

- .1 Where the ship is certified to carry more than 240 persons on board, it shall meet the requirements of SOLAS Regulation II-1/5 as though the ship is a passenger ship, and the industrial personnel are counted as passengers. However, SOLAS Regulation II-1/5.5 is not applicable.
- .2 Subdivision and damage stability shall be in accordance with SOLAS Ch. II-1, where the ship is considered a passenger ship, and industrial personnel are counted as passengers, with the value  $R$  as follows:
  - .1 where the ship is certified to carry more than 240 persons, the value  $R$  is assigned as  $R$ ;
  - .2 where the ship is certified to carry not more than 60 persons, the value  $R$  is assigned as  $0.8R$ ; or
  - .3 for more than 60 persons, but not more than 240 persons, the value  $R$  shall be determined by linear interpolation between the values given in subparagraphs .1 and .2 above.

$$R = 1 - \frac{5,000}{L_s + 2.5N + 15,225}$$

Where:

$$N = N_1 + 2N_2$$

$N_1$  = number of persons for whom lifeboats are provided

$N_2$  = number of persons (including officers and crew) the ship is permitted to carry in excess of  $N_1$

- .3 Where the conditions of service are such that compliance with paragraph 7.3.2.1.2 above on the basis of  $N=N_1+2N_2$  is impracticable and where the Administration considers that a suitably reduced degree of hazard exists, a lesser value of  $N$  may be taken but in no case less than  $N=N_1+N_2$ .
- .4 For ships to which paragraph 7.3.2.1.2.1 above applies, the requirements of SOLAS Regulations II-1/8 and II-1/8-1 and of SOLAS Ch. II-1, Parts B-2, B-3 and B-4 shall be applied as though the ship is a passenger ship and the industrial personnel are passengers. However, SOLAS Regulations II-1/14 and II-1/18 are not applicable.
- .5 For ships to which paragraphs 7.3.2.1.2.2 and 7.3.2.1.2.3 above apply, except as provided in paragraph 2.1.6 below, the provisions of SOLAS Ch. II-1, Parts B-2, B-3 and B-4 shall apply as though the ship is a cargo ship and the industrial personnel are crew. However, the requirements of SOLAS Regulations II-1/8 and II-1/8-1 need not be applied and SOLAS Regulations II-1/14 and II-1/18 are not applicable.
- .6 All ships certified in accordance with IP Code shall comply with SOLAS Regulations II-1/9, II-1/13, II-1/19, II-1/20 and II-1/21 as though the ship is a passenger ship.

Applicable provisions of the *Rules for the classification of ships, Part 4 - Stability* and provisions of the *Rules for the classification of ships, Part 5 - Subdivision* shall be taken into account also.

**7.3.2.2 Machinery installations.** In order to meet the functional requirements from paragraph II/4.2.1 of the IP Code, the ship shall comply with SOLAS Regulation II-1/35-1 as though the ship is a passenger ship.

In order to meet the functional requirement set out in paragraph II/4.2.2 of the IP Code, where the ship is certified to carry more than 240 persons on board, it shall comply with the requirements of SOLAS Regulation II-1/29 as though the ship is a passenger ship.

Applicable provisions of the *Rules for the classification of ships, Part 8 - Machinery installation* shall be taken into account also.

**7.3.2.3 Electrical installations.** In order to meet the functional requirements set out in paragraph II/5.2.1 of the IP Code, the following applies:

- .1 for installations in ships of more than 50 m in length carrying not more than 60 persons on board, the requirements in SOLAS Regulation II-1/42.2.6.1 shall apply in addition to the requirements in SOLAS Regulation II-1/43; and
- .2 for installations in ships carrying more than 60 persons on board, SOLAS Regulation II-1/42 shall apply.

In order to meet the functional requirement set out in paragraph II/5.2.2 of the IP Code for installations on ships carrying more than 60 persons on board, SOLAS Regulation II-1/45.12 shall apply.

Applicable provisions of the *Rules for the classification of ships, Part 12 - Electrical equipment* shall be taken into account also.

**7.3.2.4 Periodically unattended machinery spaces.** In order to meet the functional requirements set out in paragraph II/6.2 of the IP Code, ships carrying more than 240 persons on board shall be considered as passenger ships in relation to SOLAS Ch. II-1, Part E.

Applicable provisions of the *Rules for the classification of ships, Part 13 - Automation* shall be taken into account also.

**7.3.2.5 Fire safety.** In order to meet the functional requirement set out in paragraph II/7.2 and 4.2.3 of the IP Code, the following applies:

- .1 where the ship is certified to carry more than 240 persons on board, the requirements of SOLAS Ch. II-2 for passenger ships carrying more than 36 passengers shall apply, and
- .2 where the ship is certified to carry more than 60, but not more than 240 persons on board, the requirements of SOLAS Ch. II-2 for passenger ships carrying not more than 36 passengers apply, except that SOLAS Regulations II-2/21 and 22 need not to apply.

Applicable provisions of the *Rules for the classification of ships, Part 17 - Fire protection* shall be taken into account also.

**7.3.2.6 Dangerous goods.** In order to meet the functional requirements from paragraph II/9.2 of the IP Code, and when carrying dangerous goods in packaged form, the ship should comply with regulation IV/8.2 of the IP Code.

In order to meet the functional requirements from paragraph II/9.2 of the IP Code, and when carrying dangerous goods in solid form in bulk, the ship should comply with regulation IV/8.3 of the IP Code.

In order to meet the functional requirements from paragraph II/9.2 of the IP Code, and when carrying dangerous liquid chemicals, liquefied gases and oil, the ship should comply with regulation IV/8.4 of the IP Code.

### 7.3.4 Additional regulations for high-speed cargo craft

**7.3.4.1** Applicable provisions of the *Rules for the classification of ships, Part 28 - High-speed craft* shall be taken into account also.

**7.3.4.2 Subdivision and stability.** In order to meet the functional requirements set out in paragraph II/3.2 of the IP Code, the following applies:

- .1 Chapter 2, Part B, except 2.13.2 and 2.14, of the HSC Code shall apply in lieu of Chapter 2, Part C of the HSC Code.
- .2 When applying the provisions of Chapter 2 of the HSC Code, the expression "passenger" shall be read as "persons on board other than crew". In addition, the mass of each such person shall be assumed to be 90 kg instead of 75 kg.

**7.3.4.3** Machinery installations. In order to meet the functional requirements set out in paragraph II/4.2 of the IP Code, provisions in Chapter 10, Part B of the HSC Code shall apply as applicable to category A passenger craft in lieu of Chapter 10, Part C of the HSC Code.

**7.3.4.4** Electrical installations. In order to meet the functional requirements set out in paragraph II/5.2 of the IP Code, paragraph 12.7.10 of the HSC Code shall apply.

**7.3.4.5** Dangerous goods. Industrial personnel may only bring dangerous goods on board for the purpose of their role off the craft and with the prior consent of the master of the craft. These dangerous goods shall be considered as cargo and shall be transported in accordance with Chapter 7, Part D of the HSC Code.

In order to meet the functional requirements set out in paragraph II/9.2 of the IP Code:

- .1 for the purpose of carrying industrial personnel, the areas and spaces on craft where industrial personnel are not permitted to enter shall be clearly marked,
- .2 the arrangement for personnel transfer shall be located outside the cargo area,
- .3 the access to the arrangements for personnel transfer shall, as far as practicable, be located outside the cargo area, and
- .4 embarkation or personnel transfer and loading or unloading of cargo shall not take place simultaneously.

## 7.4 TECHNICAL DOCUMENTATION

**7.4.1** Technical documentation to be submitted to the *Register* for the purpose of the assignment of subject descriptive class note to a cargo ship, includes the documentation needed to confirm compliance with the functional requirements stated in 7.3.3.

**7.4.2** Technical documentation to be submitted to the *Register* for the purpose of the assignment of subject descriptive class note to a high-speed cargo craft needed to confirm compliance with the functional requirements is stated in 7.3.4.

## 7.5 PERIODICAL CLASS SURVEYS

**7.5.1** There are no specific requirements for periodical class surveys for the purpose of the maintenance of subject descriptive class note, and as long as the vessel is in possession of valid Industrial Personnel Safety Certificate.

**7.5.2** In addition to the requirements stated in 7.5.1, requirements for periodical class surveys related to the maintenance of the main ship type notation are to be complied with.

## 8 TRANSHIPPING UNITS

### 8.1 GENERAL

**8.1.1** Descriptive class note **Transshipping unit** may be assigned to the main ship type class notation in cases when a **Bulk Carrier** or **Floating crane** is specifically arranged and equipped (e.g. with cranes, loaders or conveyors) for the transfer of bulk cargo (such as coal or ore) from the delivering unit and to the receiving unit, located at specially designated navigation area.

**8.1.2** Self-propelled transshipping units may carry out only limited transfer voyages within their designated navigation area. Designated navigation area in which transshipping unit operates is to be entered in the Certificate of class. Voyages in ballast condition (e.g. to reach a dry-docking facility) are only to be considered by the *Register* on a case-by-case basis.

Description of such designated navigation area in which the unit is allowed to operate as transshipping unit is to be entered in the Certificate of class (e.g. "Navigation within 12 nautical miles from the shore operating as transshipping unit").

**8.1.3** The descriptive class note **Transshipping unit** is no longer applicable if the validity of the main ship type class notation is terminated.

**8.1.4** The application of the descriptive class note **Transshipping unit** for transshipping floating terminals (units specially intended to tranship the cargo between more than one delivering and receiving units simultaneously, with these units normally having cargo storage capability) is subjected to special consideration of the *Register*.

### 8.2 APPLICATION

**8.2.1** The descriptive class note **Transshipping unit** applies either to new, or to existing **Bulk carriers** or **Floating cranes** of  $GT \geq 500$ , which are positioned, moored or anchored at the offshore location, or which are berthed alongside the terminal, and when to be used for the transfer of bulk cargo from the delivering unit to the receiving unit.

### 8.3 REQUIREMENTS FOR THE ASSIGNMENT

**8.3.1** The requirements for the assignment of the subject descriptive class note consists of:

- .1 General requirements contained in the *Rules for the classification of ships, Part 1 – General requirements*.
- .2 Specific requirements related to the assigned main ship type notation **Bulk Carrier** or **Floating Crane**, as contained in the relevant parts of the *Rules for the classification of ships*.

In addition to the above, relevant safety objectives of the SOLAS, MARPOL, and ILLC 66 as well as the

basic safety principles of the ILO Conventions must be observed.

### 8.4 TECHNICAL DOCUMENTATION

**8.4.1** Technical documentation to be submitted to the *Register* for the purpose of the assignment of subject descriptive class note in the case of newbuilding consists of:

- .1 Technical documentation for the purpose of the assignment of the relevant main ship type notation (Bulk Carrier or Floating Crane).
- .2 In the case of existing ships to be converted to Transshipping unit, an addendum to existing stability file to include stability conditions covering cargo loading / discharging / transferring with the use of cranes, loaders, or conveyors.
- .3 Technical documentation related to cargo handling gear intended for cargo transfer and as listed in Head 1.4 of the *Rules for technical supervisions of sea-going ships Part 19, Cargo handling gear and lifting appliances.*, as applicable.
- .4 Other documentation deemed necessary by the *Register*.

### 8.5 PERIODICAL CLASS SURVEYS

In addition to surveys related to the maintenance of the main ship type class notation, including ESP survey requirements when applicable, the survey of the following items is to be performed.

#### 8.5.1 Annual survey

**8.5.1.1** The survey on the weather deck is to include:

- .1 Verification that no modification of the cargo handling system(s) layout has been made. Particular attention is to be paid to cargo handling arrangements passing in close proximity to accommodation and/or control stations.
- .2 Verification that, when expected and fitted, special arrangements to avoid unintentional release of lifted cargo are maintained and unmodified.
- .3 General examination, as far as applicable, of cargo handling system(s) with particular attention to the connection of their foundations to the hull structure.
- .4 General examination of the ship-to-unit mooring arrangements, including winches, cables, fairleads and mooring cleats, bumpers, fenders, and relevant connection to the hull structures.
- .5 For Transshipping units which are intended to be moored alongside in between two other ships (e.g. a barge being discharged and a bulk carrier being loaded), examination of the means of access and verification that they are available in all operational conditions.

- .6 Verification that instruction to the Master in a way of an approved stability file covering cargo loading / discharging / transferring operations is available on board.
- .7 Verification of the mooring and anchoring arrangements.

**8.5.1.2** The survey of cargo handling gear is to include:

- .1 Verification of the condition of cargo handling (transfer) system according to the *Rules for technical supervisions of sea-going ships Part 19, Cargo handling gear and lifting appliances*, and in addition the verification of the following, as applicable:
  - a) belt conveyors,
  - b) spiral conveyors,
  - c) screw conveyors,
  - d) pneumatic conveyors,
  - e) chain conveyors (buckets, pockets, etc.),
  - f) wire conveyors,
  - g) cable conveyors (wagons, buckets, pockets, etc.),
  - h) chain elevators (buckets, pockets, etc.),
  - i) cable elevators (buckets, pockets, etc.),
  - j) loading and discharging boom(s) and combinations of these.

**8.5.1.3** Additionally, the survey of the cargo handling gear is to include, as far as applicable:

- .1 An examination of the instruction/installation manual to verify the layout of the complete system(s) and confirm correspondence to the actual system(s) fitted on board.
- .2 Verification that maintenance of the system(s) has been carried out according to the Manufacturer's instructions and schedules.
- .3 A general examination of components of the system in order to verify their satisfactory condition of maintenance.
- .4 Verification and test of the cargo handling system alarm and safety devices.
- .5 A running test of the system in order verify the satisfactory working and operation conditions.

## 8.5.2 Renewal survey

**8.5.2.1** The survey of the hull items is to include:

- .1 Requirements applicable for the Annual survey according to 8.5.1.1.
- .2 Examination of cargo handling system(s) with particular attention to the structures pertaining to the system(s), such as pillars, columns, girders, support trusses connection of their foundations to the hull structure. The examination may be supported by thickness measurements as deemed necessary by the Surveyor of the *Register*.
- .3 Examination of hull structures underneath the foundations of the cargo handling system(s) with particular attention to the areas

where stress concentration or increased corrosion are likely to develop.

- .4 A general examination of components of the system to verify their satisfactory condition of maintenance.
- .5 Examination of the ship-to-unit mooring arrangements, including winches, cables, fairleads and mooring cleats, bumpers, fenders and relevant connection to the hull structures, with disassembly as deemed necessary to verify the condition of the equipment and control and safety devices.
- .6 Examination of hull structures underneath the foundations of the ship-to-unit mooring arrangements with particular attention to the areas where stress concentration or increased corrosion are likely to develop.

**8.5.2.2** The survey of cargo handling (transfer) system is to include:

- .1 Examination of components of the system(s) in order to verify their satisfactory condition of maintenance. The inspections may be supplemented by dismantling of the system components as deemed necessary by the Surveyor of the *Register*.
- .2 Examination and working test of the hydraulic oil system, as applicable, pertaining to the cargo handling system(s).
- .3 Examination and test of all electrical systems related to the cargo handling system(s). Examination is to be supplemented by insulation tests of all electrical equipment.
- .4 For ship's cranes and lifting machinery and gear intended for loading, unloading and transfer of cargo falling under provisions of the *Rules for technical supervisions of sea-going ships Part 19, Cargo handling gear and lifting appliances*, overload test of the cargo is to be carried according to ILO requirements.
- .5 Overload test of the cargo handling system(s) not falling under provisions of the *Rules for technical supervisions of sea-going ships Part 19, Cargo handling gear and lifting appliances*, is to be performed with test loads as expected by the System(s) Manufacturer(s). In the absence of data, the test loads should be at least 1.1 times the Safety Working Load (SWL) of the system. If a Cargo Handling System is equipped with a gearing system(s) it is necessary to verify, during the test, that each gear tooth is tested under testing load(s).
- .6 After testing, fixed structures and associated gear are to be disassembled and examined as deemed necessary by the Surveyor of the *Register*. The tests and inspections are not to reveal deformations or unacceptable defects.

## 9 MOBILE STORAGE UNITS

### 9.1 GENERAL

**9.1.1** Descriptive class note **Mobile storage unit** may be assigned to the main ship type class notation **Floating storage** when an existing oil tanker is converted in moored unit at a fixed offshore location intended for the storage and discharge of liquid hydrocarbons and which makes no change to its operational and safety characteristics.

**9.1.2** Self-propelled vessels with the assigned descriptive class note **Mobile storage unit** may carry out only limited transfer voyages within their designated navigation area for loading/unloading operations or safety reasons. Such voyages are to be always pre-approved with the *Register*.

Description of such fixed offshore location where the unit is allowed to operate is to be entered in the Certificate of class (e.g. "Navigation within 12 nautical miles from the shore operating as mobile storage unit").

**9.1.3** Conditions for voyages in ballast condition (e.g. to reach a dry-docking facility or transferring to different intended operation sites) are only to be considered by the *Register* on a case-by-case basis.

For that purpose, additional character of class denoting navigation area should be assigned, but only for transferring of the unit in ballast condition (e.g. *1 (unrestricted navigation)* with additional description: "Transfer – the vessel is allowed to transfer from one location to another by means of her own propulsion or in towing conditions in unrestricted navigation".)

**9.1.4** In the case of vessels with the assigned descriptive class note **Mobile storage unit**, and for which the *Register* has issued a corresponding authorization, it may be permitted to carry out the voyage outside their assigned navigation area and to carry liquid hydrocarbons only in towing condition.

**9.1.5** The descriptive class note **Mobile storage unit** is no longer applicable if the validity of the main ship type class notation is terminated.

**9.1.6** If the descriptive class note **Mobile storage unit** is assigned to the main ship type class notation **Floating storage** when an existing oil tanker is converted in moored unit at a fixed offshore location, the requirements of the Enhanced Survey Programme regarding the scope of survey are to be applicable.

### 9.2 APPLICATION

**9.2.1** The descriptive class note **Mobile storage unit** applies to **Floating storage** units as stated in 91.1.

### 9.3 REQUIREMENTS FOR THE ASSIGNMENT

**9.3.1** The requirements for the assignment of the subject descriptive class note consists of:

- .1 General requirements contained in the *Rules for the classification of ships, Part 1 – General requirements*.
- .2 Specific requirements related to oil tankers, as contained in the relevant parts of the *Rules for the classification of ships*.

In addition to the above, relevant safety objectives of the SOLAS, MARPOL, and ILLC 66 as well as the basic safety principles of the ILO Conventions must be observed.

### 9.4 TECHNICAL DOCUMENTATION

**9.4.1** Technical documentation to be submitted to the *Register* in the case of an existing oil tanker to be converted in **Mobile storage unit** under supervision of the *Register* consists of:

- .1 Pumping arrangement at the forward and after ends and drainage of cofferdams and pump rooms.
- .2 Diagram of the oil cargo tank venting system with:
  - a) indication of the outlet position,
  - b) details of the pressure/vacuum valves and flame arrestors,
  - c) details of the draining arrangements, if any.
- .3 Diagram of the oil cargo tank level gauging system with overflow safety arrangements.
- .4 Diagram of the oil cargo tank heating system.
- .5 Oil cargo tank cleaning system.
- .6 Gas freeing system of cargo tanks.
- .7 Diagram of bilge system in cargo area.
- .8 Diagram of ballast system in cargo area.
- .9 Diagram of air, sounding and scuppers in cargo area.
- .10 Plan of hazardous areas.
- .11 Document giving details of types of cables and safety characteristics of the equipment installed in hazardous areas.
- .12 Diagrams of tank level indicator systems, high level alarm systems and overflow control systems where requested.
- .13 Fixed deck foam systems.
- .14 Fixed fire extinguishing systems in cargo pump rooms.
- .15 Arrangement of fixed inert gas systems.
- .16 Other documentation deemed necessary by the *Register*.

### 9.5 PERIODICAL CLASS SURVEYS

**9.5.1** Periodical class surveys (Annual, Intermediate and Renewal), as applicable for oil tankers, are to be performed.

**9.5.2** Periodical class surveys as applicable for **Floating storage** units, are to be performed.

**9.5.3** In addition to the above, at each Annual, Intermediate and Renewal class survey, the survey is to include:

- .1 Enhanced Survey Programme items applicable for oil tankers and as specified in the *Rules for the classification of ships, Part 1 – General requirements, Chapter 5 – Surveys of ships in service.*
- .2 Verification of the mooring and anchoring arrangements.
- .3 Verification of statutory related items (SOLAS, MARPOL, ILLC 66) as applicable for oil tankers.