Requirements concerning

ELECTRICAL AND ELECTRONIC INSTALLATIONS

CONTENTS

E17	Generators and generator systems, having the ship's propulsion machinery as their prime mover, not forming part of the ship's main source of electrical power	Rev.1 Feb 2021
E18	Recording of the type, location and maintenance cycle of batteries	Rev.1 Dec 2014
E19	Ambient temperatures for electrical equipment installed in environmentally controlled spaces	Rev.1 Sept 2005
E20	Installation of electrical and electronic equipment in engine rooms protected by fixed water-based local application fire-fighting systems (FWBLAFFS)	Rev.1 June 2009
E21	Requirements for uninterruptible power system (UPS) units as alternative and/or transitional power	Corr.1 June 2022
E22	Computer-based systems	Rev.3 June 2023
E23	Selection of low voltage circuit breakers on the basis of their short circuit capacity and co-ordination in service	Deleted Mar 2011
E24	Harmonic Distortion for Ship Electrical Distribution System including Harmonic Filters	Rev.1 Dec 2018
E25	Failure detection and response of all types of steering control systems	Rev.2 Mar 2022
E26	Cyber resilience of ships	New Apr 2022
E27	Cyber resilience of on-board systems and equipment	New Apr 2022

E1 (1975) Governing characteristics of generator prime movers

see revised M 3.2

◀◀

E2 Deleted (December 1996)

◀◀

E3 Deleted (December 1996)

◀◀

E4 Earthing of non-current-carrying parts

(1978)

Deleted in June 2000.

E5 Voltage and frequency variations

(1979) (Rev.1 Sept. 2005)

1. All electrical appliances supplied from the main or emergency systems are to be so designed and manufactured that they are capable of operating satisfactorily under the normally occurring variations in voltage and frequency.

2. Unless otherwise stated in the national or international standards, all equipment should operate satisfactorily with the variations from its rated value shown in the Tables 1 to 3 on the following conditions.

(a) For alternative current components, voltage and frequency variations shown in the Table 1 are to be assumed.

(b) For direct current components supplied by d.c. generators or converted by rectifiers, voltage variations shown in the Table 2 are to be assumed.

(c) For direct current components supplied by electrical batteries, voltage variations shown in the Table 3 are to be assumed.

3. Any special system, e.g. electronic circuits, whose function cannot operate satisfactorily within the limits shown in the Table should not be supplied directly from the system but by alternative means, e.g. through stabilized supply.

Table 1: Voltage and frequency variations for a.c. distribution systems

Quantity in Operation	Variations	
	Permanent	Transient
Frequency	±5%	±10% (5 sec)
Voltage	+6%, -10%	±20% (1.5 sec)

Table 2: Voltage variations for d.c distribution systems

Parameters	Variations
Voltage tolerance (continuous)	±10%
Voltage cyclic variation deviation	5%
Voltage ripple (a.c. r.m.s. over steady d.c. voltage)	10%

Table 3: Voltage variations for battery systems

Systems	Variations
Components connected to the battery during charging (see Note)	+30%, -25%
Components not connected to the battery during charging	+20%, -25%
Note: Different voltage variations as determined by the charging/discharging characteristics, including ripple voltage from the charging device, may be considered.	

END

E6 Deleted

End of Document

E7 Cables

(1975) (Rev.1 1990) (Rev.2 June 2000) (Rev.3 May 2006) (Rev.4 Apr 2016) (Rev.5 Feb 2021)

1. Cables are to be of a type approved by the Classification Society.

2. Cables manufactured in accordance with the relevant recommendations of IEC 60092-350:2020, 60092-352:2005, 60092-353:2016, 60092-354:2020, 60092-360:2014, 60092-370:2019 and 60092-376:2017 will be accepted by the Classification Society provided that they are tested to its satisfaction.

3. Cables manufactured and tested to standards other than those specified in 2 will be accepted provided they are in accordance with an acceptable and relevant international or national standard and are of an equivalent or higher safety level than those listed in paragraph 2. However, cables such as flexible cable, fibre-optic cable, etc. used for special purposes may be accepted provided they are manufactured and tested in accordance with the relevant standards accepted by the Classification Society.

Note:

1. Rev.4 of this UR is to be uniformly implemented by IACS Societies from 1 July 2017.

2. Rev.5 of this UR is to be uniformly implemented by IACS Societies for cables:

   i) when an application for certification of cables is dated on or after 1 July 2022; or

   ii) which are installed in new ships contracted for construction on or after 1 July 2022.

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

4. The “date of application for certification of cables” is the date of whatever document the Classification Society requires/accepts as an application or request for certification of cables.

End of Document

E8 Starting arrangements of internal combustion engines

(1977)
(Rev.1 1996)
(Corr. Aug 2000)

Deleted in Dec 2003

(E8 has been merged with UR M49 to form a new UR M61 (Dec 2003))

E9 Earthing and bonding of cargo tanks/ process plant/piping systems for the control of static electricity

E9 (1988) Rev.1 Oct 2012)

E9.1 The hazard of an incentive discharge due to the build-up of static electricity resulting from the flow of liquids/gases/vapours can be avoided if the resistance between the cargo tanks/process plant/piping systems and the hull of the ship is not greater than 10^6 ohm.

E9.2 This value of resistance will be readily achieved without the use of bonding straps where cargo tanks/process plant/piping systems are directly or via their supports, either welded or bolted to the hull of the ship.

E9.3 Bonding straps are required for cargo tanks/process plant/piping systems which are not permanently connected to the hull of the ship, e.g.

a) independent cargo tanks;

b) cargo tanks/piping systems which are electrically separated from the hull of the ship;

c) pipe connections arranged for the removal of spool pieces.

d) wafer-style valves with non-conductive (e.g PTFE) gaskets or seals.

E9.4 Where bonding straps are required, they should be:

a) clearly visible so that any shortcomings can be clearly detected;

b) designed and sited so that they are protected against mechanical damage and that they are not affected by high resistivity contamination e.g. corrosive products or paint;

c) easy to install and replace.

E9.5 Checks should be made on the resistance to the hull of the ship during construction of the ship and at subsequent major surveys, supplemented by visual inspection during annual surveys.

Note:

1. Revision 1 of this UR is to be implemented for ships contracted for construction on or after 1 January 2014.

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

End of Document

E10 Test Specification for Type Approval

(1991) (Rev.1 1993) (Rev.2 1997) (Rev. 2.1 July 1999) (Rev.3 May 2001) (Corr.1 July 2003) (Rev.4 May 2004) (Rev.5 Dec 2006) (Rev.6 Oct 2014) (Rev.7 Oct 2018) (Rev.8 Feb 2021) (Corr.1 Jan 2022) (Rev.9 Aug 2023)

E10.1 General

This Test Specification is applicable, but not confined, to electrical, electronic and programmable equipment intended for control, monitoring, alarm and protection systems for use in ships.

E10.2 Testing

These tests are to demonstrate the ability of the equipment to function as intended under the specified testing conditions.

The extent of the testing (i.e. the selection and sequence of carrying out tests and number of pieces to be tested) is to be determined upon examination and evaluation of the equipment or component subject to testing giving due regard to its intended usage.

Equipment is to be tested in its normal position if otherwise not specified in the test specification.

Note:

1. Rev.5 of this UR is to be uniformly implemented by IACS Societies from 1 January 2008.

2. Rev.6 of this UR is to be uniformly implemented by IACS Societies from 1 January 2016.

3. Rev.7 of this UR is to be uniformly implemented by IACS Societies for equipment for which the date of application for type approval certification is dated on or after 1 January 2020.

4. Equipment intended to be installed on ships contracted for construction on or after 1 January 2022 is to comply with Rev.7 of this UR.

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

6. The “date of application for type approval” is the date of documents accepted by the Classification Society as request for type approval certification of a new equipment type or of an equipment type that has undergone substantive modifications in respect of the one previously type approved, or for renewal of an expired type approval certificate.

7. Rev.8 of this UR is to be uniformly implemented by IACS Societies for equipment for which the date of application for type approval certification is dated on or after 1 July 2022.

8. Rev.9 of this UR is to be uniformly implemented by IACS Societies for equipment for which the date of application for type approval certification is dated on or after 1 July 2024.

E10 (cont)

Relevant tests are as listed in the Table.

Note:

a) * These test requirements are harmonised with IEC 60092-504:2016 “Electrical Installations in Ships - Part 504: Special features - Control and Instrumentation” and IEC 60533:2015 “Electrical and electronic installations in ships – electromagnetic compatibility”. Electrical and electronic equipment on board ships, required neither by classification rules nor by International Conventions, liable to cause electromagnetic disturbance shall be of type which fulfil the test requirements of test specification items 19 and 20.

b) As used in this document, and in contrast to a complete performance test, a functional test is a simplified test sufficient to verify that the equipment under test (EUT) has not suffered any deterioration caused by the individual environmental tests.

Type testing condition for equipment covered by E10.1

NO.	TEST	PROCEDURE ACC. TO:*	TEST PARAMETERS	OTHER INFORMATION
	***** indicates the testing procedure which is normally to be applied. However, equivalent testing procedure may be accepted by the individual Society provided that the Unified Requirements stated in the other columns are fulfilled. Later versions (including revisions) of the international standards specified in this UR are acceptable for use, provided the Scociety determines them to be equivalent to the technical specifications of this UR.			
1.	Visual inspection	-	-	- conformance to drawings, design data
2.	Performance test	Manufacturer performance test programme based upon specification and relevant Rule requirements. When the EUT is required to comply with an international performance standard, e.g. protection relays, verification of requirements in the standard are to be part of the performance testing required in this initial test and subsequent performance tests after environmental testing where required in the UR.	- standard atmosphere conditions - temperature: 25°C ± 10°C - relative humidity: 60% ± 30% - air pressure: 96 KPa ± 10KPa	- confirmation that operation is in accordance with the requirements specified for particular system or equipment; - checking of self-monitoring features; - checking of specified protection against an access to the memory; - checking against effect of unerroneous use of control elements in the case of computer systems.

E10
(cont)

<table>
<tr><th>NO.</th><th>TEST</th><th>PROCEDURE ACC. TO:*</th><th>TEST PARAMETERS</th><th>OTHER INFORMATION</th></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>3.</td><td>External power supply failure</td><td>-</td><td>- 3 interruptions during 5 minutes;
- switching-off time 30 s each case</td><td rowspan="2">- The time of 5 minutes may be exceeded if the equipment under test needs a longer time for start-up, e.g. booting sequence
- For equipment which requires booting, one additional power supply interruption during booting to be performed
Verification of:
- equipment behaviour upon loss and restoration of supply;
- possible corruption of programme or data held in programmable electronic systems, where applicable.</td></tr>
<tr><td>4.</td><td>Power supply variations
a) electric

b) pneumatic and hydraulic</td><td>-</td><td>AC SUPPLY
<table><tr><th>Combination</th><th>Voltage variation permanent %</th><th>Frequency variation permanent %</th></tr><tr><td>1
2
3
4</td><td>+6
+6
-10
-10</td><td>+5
-5
-5
+5</td></tr><tr><td></td><td>voltage transient 1,5 s %</td><td>frequency transient 5 s %</td></tr><tr><td>5
6</td><td>+20
-20</td><td>+10
-10</td></tr></table>DC SUPPLY
<table><tr><td>Voltage tolerance continuous</td><td>±10%</td></tr><tr><td>Voltage cyclic variation</td><td>5%</td></tr><tr><td>Voltage ripple</td><td>10%</td></tr></table>Electric battery supply:
- +30% to –25% for equipment connected to charging battery or as determined by the charging/discharging characteristics, including ripple voltage from the charging device;
- +20% to –25% for equipment not connected to the battery during charging.

Pressure: ±20%
Duration: 15 minutes</td></tr>
</table>

E10
(cont)

NO.	TEST	PROCEDURE ACC. TO:*	TEST PARAMETERS	OTHER INFORMATION
5.	Dry heat (see note 1)	IEC 60068-2-2:2007 Test Bb for non-heat dissipating equipment	Temperature: 55° ± 2°C Duration: 16 hours or Temperature: 70°C ± 2°C Duration: 16 hours	- equipment operating during conditioning and testing; - functional test (b) during the last hour at the test temperature. - for equipment specified for increased temperature the dry heat test is to be conducted at the agreed test temperature and duration.
		IEC 60068-2-2:2007 Test Be for heat dissipating equipment	Temperature: 55° ± 2°C Duration: 16 hours or Temperature: 70°C ± 2°C Duration: 16 hours	- equipment operating during conditioning and testing with cooling system on if provided; - functional test (b) during the last hour at the test temperature. - for equipment specified for increased temperature the dry heat test is to be conducted at the agreed test temperature and duration.
6.	Damp heat	IEC 60068-2-30:2005 test D_b	Temperature: 55°C Humidity: 95% Duration: 2 cycles 2 x (12 +12 hours)	- measurement of insulation resistance before test; - the test shall start with 25°C ± 3°C and at least 95% humidity; - equipment operating during the complete first cycle and switched off during second cycle except for functional test; - functional test during the first 2 hours of the first cycle at the test temperature and during the last 2 hours of the second cycle at the test temperature; Duration of the second cycle can be extended due to more convenient handling of the functional test. - recovery at standard atmosphere conditions; - insulation resistance measurements and performance test.
7.	Vibration	IEC 60068-2-6:2007 Test F_c	2 $^{+3}$ Hz to 13.2 Hz – amplitude ±1mm	- duration in case of no resonance condition 90

E10
(cont)

NO.	TEST	PROCEDURE ACC. TO:*	TEST PARAMETERS	OTHER INFORMATION
			$^{-0}$ 13.2 Hz to 100 Hz – acceleration ± 0.7 g. For severe vibration conditions such as, e.g. on diesel engines, air compressors, etc.: 2.0 Hz to 25 Hz – amplitude ±1.6 mm 25.0 Hz to 100 Hz – acceleration ± 4.0 g. Note: More severe conditions may exist for example on exhaust manifolds or fuel oil injection systems of diesel engines. For equipment specified for increased vibration levels the vibration test is to be conducted at the agreed vibration level, frequency range and duration. Values may be required to be in these cases 40 Hz to 2000 Hz - acceleration ± 10.0g at 600°C, duration 90 min.*	minutes at 30 Hz; - duration at each resonance frequency at which Q≥ 2 is recorded - 90 minutes; - during the vibration test, functional tests are to be carried out; - tests to be carried out in three mutually perpendicular planes; - it is recommended as guidance that Q does not exceed 5. - where sweep test is to be carried out instead of the discrete frequency test and a number of resonant frequencies is detected close to each other, duration of the test is to be 120 min. Sweep over a restricted frequency range between 0.8 and 1.2 times the critical frequencies can be used where appropriate. Note: Critical frequency is a frequency at which the equipment being tested may exhibit: - malfunction and/or performance deterioration - mechanical resonances and/or other response effects occur, e.g. chatter
8.	Inclination	IEC 60092-504:2016	Static 22.5° Dynamic 22.5°	a) inclined to the vertical at an angle of at least 22.5° b) inclined to at least 22.5° on the other side of the vertical and in the same plane as in (a), c) inclined to the vertical at an angle of at least 22.5° in plane at right angles to that used in (a), d) inclined to at least 22.5° on the other side of the vertical and in the same plane as in (c). Note: The period of testing in each position should be sufficient to fully evaluate the behaviour of the equipment. Using the directions defined in a) to d) above, the equipment is to be rolled to an angle of 22.5° each side of the vertical with a period of 10 seconds.

E10
(cont)

<table>
<tr><th>NO.</th><th>TEST</th><th>PROCEDURE ACC. TO:*</th><th>TEST PARAMETERS</th><th>OTHER INFORMATION</th></tr>
<tr><td></td><td></td><td></td><td></td><td>The test in each direction is to be carried out for not less than 15 minutes.
On ships for the carriage of liquified gases and chemicals, the emergency power supply is to remain operational with the ship flooded up to a maximum final athwart ship inclination of 30°.

Note: These inclination tests are normally not required for equipment with no moving parts.</td></tr>
<tr><td>9.</td><td>Insulation resistance</td><td colspan="2"><table>
<tr><td rowspan="2">Rated supply voltage Un (V)</td><td rowspan="2">Test voltage (D.C. voltage) (V)</td><td colspan="2">Min. insulation resistance</td></tr>
<tr><td>before test
M ohms</td><td>after test
M ohms</td></tr>
<tr><td>Un ≤ 65</td><td>2 x Un
min. 24V</td><td>10</td><td>1,0</td></tr>
<tr><td>Un > 65</td><td>500</td><td>100</td><td>10</td></tr>
</table></td><td>- For high voltage equipment, reference is made to
UR E11.
- insulation resistance test is to be carried out before and after: damp heat test, cold test, salt mist test and high voltage test;
- between all phases and earth; and where appropriate, between the phases.
Note: Certain components e.g. for EMC protection may be required to be disconnected for this test.</td></tr>
<tr><td>10.</td><td>High voltage</td><td colspan="2"><table>
<tr><td>Rated voltage
Un (V)</td><td>Test voltage (A.C. voltage 50 or 60Hz)
(V)</td></tr>
<tr><td>Up to 65</td><td>2 x Un + 500</td></tr>
<tr><td>66 to 250</td><td>1500</td></tr>
<tr><td>251 to 500</td><td>2000</td></tr>
<tr><td>501 to 690</td><td>2500</td></tr>
</table></td><td>- For high voltage equipment, reference is made to
UR E11.
- separate circuits are to be tested against each other and all circuits connected with each other tested against earth;
- printed circuits with electronic components may be removed during the test;
- period of application of the test voltage: 1 minute</td></tr>
<tr><td>11.</td><td>Cold</td><td>IEC 60068-2-1:2007</td><td>Temperature: +5°C ± 3°C
Duration: 2 hours
or
Temperature: –25°C ± 3°C
Duration: 2 hours
(see note 2)</td><td>- initial measurement of insulation resistance;
- equipment not operating during conditioning and
testing except for functional test;
- functional test during the last hour at the test temperature;
- insulation resistance measurement and the</td></tr>
</table>

E10
(cont)

NO.	TEST	PROCEDURE ACC. TO:*	TEST PARAMETERS	OTHER INFORMATION
				functional test after recovery
12.	Salt mist	IEC 60068-2-52:2017 Test Kb	Four spraying periods with a storage of 7 days after each.	- initial measurement of insulation resistance and initial functional test; - equipment not operating during conditioning; - functional test on the 7th day of each storage period; - insulation resistance measurement and performance test 4 to 6h after recovery. (see Note 3) - on completion of exposure, the equipment shall be examined to verify that deterioration or corrosion (if any) is superficial in nature.
13.	Electrostatic discharge	IEC 61000-4-2:2008	Contact discharge: 6kV Air discharge: 2kV, 4kV, 8kV Interval between single discharges: 1 sec. No. of pulses: 10 per polarity According to test level 3.	- to simulate electrostatic discharge as may occur when persons touch the appliance; - the test is to be confined to the points and surfaces that can normally be reached by the operator; - Performance Criterion B (See Note 4).
14.	Electromagnetic field	IEC 61000-4-3:2020 or IEC 61000-4-3:2006+AMD1:2007+AMD2:2010	Frequency range: 80 MHz to 6 GHz Modulation**: 80% AM at 1000Hz Field strength: 10V/m Frequency sweep rate: ≤1.5 x 10^{-3} decades/s (or 1%/3 sec) According to test level 3.	- to simulate electromagnetic fields radiated by different transmitters; - the test is to be confined to the appliances exposed to direct radiation by transmitters at their place of installation. - Performance criterion A (See Note 5) **If for tests of equipment an input signal with a modulation frequency of 1000 Hz is necessary a modulation frequency of 400 Hz may be chosen. - If an equipment is intended to receive radio signals for the purpose of radio communication (e.g. wifi router, remote radio controller), then the immunity limits at its communication frequency do not apply, subject to the

E10 (cont)

NO.	TEST	PROCEDURE ACC. TO:*	TEST PARAMETERS	OTHER INFORMATION
				provisions “Specific requirements for wireless data links” in UR E22.
15.	Conducted low Frequency		AC: Frequency range: rated frequency to 200th harmonic; Test voltage (rms): 10% of supply to 15th harmonic reducing to 1% at 100th harmonic and maintain this level to the 200th harmonic, min 3 V r.m.s, max 2 W. DC: Frequency range: 50 Hz - 10 kHz; Test voltage (rms): 10% of supply max. 2 W	- to stimulate distortions in the power supply system generated for instance, by electronic consumers and coupled in as harmonics; - performance criterion A (see Note 5). - See figure - “Test set-up” - for keeping max. 2W, the voltage of the test signal may be lower.
16.	Conducted Radio Frequency	IEC 61000-4-6:2013	AC, DC, I/O ports and signal/control lines: Frequency range: 150 kHz - 80 MHz Amplitude: 3 V rms (See Note 6) Modulation ***: 80% AM at 1000 Hz Frequency sweep range: ≤ 1.5 x 10^{-3} decades/s (or 1%/3sec.) According to test level 2.	- Equipment design and the choice of materials is to stimulate electromagnetic fields coupled as high frequency into the test specimen via the connecting lines. - performance criterion A (see Note 5). *** If for tests of equipment an input signal with a modulation frequency of 1000 Hz is necessary a modulation frequency of 400 Hz may be chosen.
17.	Electrical Fast Transients / Burst	IEC 61000-4-4:2012	Single pulse rise time: 5 ns (between 10% and 90% value) Single pulse width: 50 ns (50% value) Amplitude (peak): 2kV line on power supply port/earth; 1kV on I/O data control and communication ports (coupling clamp) Pulse period: 300 ms; Burst duration: 15 ms;	- arcs generated when actuating electrical contacts; - interface effect occurring on the power supply, as well as at the external wiring of the test specimen; - performance criterion B (see Note 4).

E10
(cont)

<table>
<tr><th>NO.</th><th>TEST</th><th>PROCEDURE ACC. TO:*</th><th>TEST PARAMETERS</th><th>OTHER INFORMATION</th></tr>
<tr><td></td><td></td><td></td><td>Duration/polarity: 5 min
According to test level 3.</td><td></td></tr>
<tr><td>18.</td><td>Surge</td><td>IEC 61000-4-5:2017</td><td>Test applicable to AC and DC power ports
Open-circuit voltage:
Pulse rise time: 1.2 µs (front time)
Pulse width: 50 µs (time to half value)
Amplitude (peak): 1kV line/earth;
0.5kV line/line
Short-circuit current:
Pulse rise time: 8 µs (front time)
Pulse width: 20 µs (time to half value)
Repetition rate: ≥ 1 pulse/min
No of pulses: 5 per polarity
Application: continuous
According to test level 2.</td><td>- interference generated for instance, by switching
“ON” or “OFF” high power inductive consumers;
- test procedure in accordance with figure 10 of the standard for equipment where power and signal lines are identical;
- performance criterion B (see Note 4).</td></tr>
<tr><td>19.</td><td>Radiated Emission</td><td>CISPR 16-2-3:2016
IEC 60945:2002 for 156-165 MHz</td><td>Limits below 1000 MHz

For equipment installed in the bridge and deck zone.

<table><tr><th>Frequency range:</th><th>Quasi peak limits:</th></tr><tr><td>0.15 - 0.3 MHz</td><td>80 - 52 dBµV/m</td></tr><tr><td>0.3 - 30 MHz</td><td>52 - 34 dBµV/m</td></tr><tr><td>30 - 1000 MHz</td><td>54 dBµV/m</td></tr><tr><td>except for:</td><td></td></tr><tr><td>156 -165 MHz</td><td>24 dBµV/m</td></tr></table>
For equipment installed in the general power distribution zone.

<table><tr><th>Frequency range:</th><th>Quasi peak limits:</th></tr><tr><td>0.15 - 30 MHz</td><td>80 - 50 dBµV/m</td></tr><tr><td>30 - 100 MHz</td><td>60 - 54 dBµV/m</td></tr><tr><td>100 - 1000 MHz</td><td>54 dBµV/m</td></tr><tr><td>except for:</td><td></td></tr></table></td><td>- procedure in accordance with the standard but distance 3 m between equipment and antenna
- for the frequency band 156 MHz to 165 MHz the measurement shall be repeated with a receiver bandwidth of 9 kHz (as per IEC 60945:2002).
- alternatively the radiation limit at a distance of 3 m from the enclosure port over the frequency 156 MHz to 165 MHz shall be 30 dB micro-V/m Peak (as per IEC 60945:2002).</td></tr>
</table>

E10
(cont)

NO.	TEST	PROCEDURE ACC. TO:*	TEST PARAMETERS	OTHER INFORMATION
			156 -165 MHz | 24 dBµV/m Limits above 1000 MHz Frequency range: 1000 - 6000 MHz | Average limit: 54 dBµV/m	- procedure in accordance with the standard (distance 3 m between equipment and antenna) -Equipment intended to transmit radio signals for the purpose of radio communication (e.g. wifi router, remote radio controller) may be exempted from limit, within its communication frequency range, subject to the provisions " Specific requirements for wireless data links" in UR E22.
20.	Conducted Emission	CISPR 16-2-1:2017	Test applicable to AC and DC power ports For equipment installed in the bridge and deck zone. Frequency range: 10 - 150 kHz | Limits: 96 - 50 dBµV 150 - 350 kHz | 60 - 50 dBµV 350 kHz - 30 MHz | 50 dBµV For equipment installed in the general power distribution zone. Frequency range: 10 - 150 kHz | Limits: 120 - 69 dBµV 150 - 500 kHz | 79 dBµV 0.5 - 30 MHz | 73 dBµV	
21.	Flame retardant	IEC 60092-101:2018 or	Flame application: 5 times 15 s each. Interval between each application: 15s or 1 time 30s. Test criteria based upon application.	- the burnt out or damaged part of the specimen by not more than 60 mm long. - no flame, no incandescence or - in the event of a flame or incandescence being present, it shall extinguish itself within 30 s of the removal of the needle flame

E10
(cont)

NO.	TEST	PROCEDURE ACC. TO:*	TEST PARAMETERS	OTHER INFORMATION
		IEC 60695-11-5:2016	The test is performed with the EUT or housing of the EUT applying needle-flame test method.	without full combustion of the test specimen. - any dripping material shall extinguish itself in such a way as not to ignite a wrapping tissue. The drip height is 200 mm ± 5 mm.

E10
(cont)

Notes:

1. Dry heat at 70 °C is to be carried out to automation, control and instrumentation equipment subject to high degree of heat, for example mounted in consoles, housings, etc. together with other heat dissipating power equipment.

2. For equipment installed in non-weather protected locations or cold locations test is to be carried out at –25°C.

3. Salt mist test is to be carried out for equipment installed in weather exposed areas.

4. Performance Criterion B: (For transient phenomena): The EUT shall continue to operate as intended after the tests. No degradation of performance or loss of function is allowed as defined in the technical specification published by the manufacturer. During the test, degradation or loss of function or performance which is self recoverable is however allowed but no change of actual operating state or stored data is allowed.

5. Performance Criterion A: (For continuous phenomena): The Equipment Under Test shall continue to operate as intended during and after the test. No degradation of performance or loss of function is allowed as defined in relevant equipment standard and the technical specification published by the manufacturer.

6. For equipment installed on the bridge and deck zone, the test levels shall be increased to 10V rms for spot frequencies in accordance with IEC 60945:2002 at 2, 3, 4, 6.2, 8.2, 12.6, 16.5, 18.8, 22, 25 MHz.

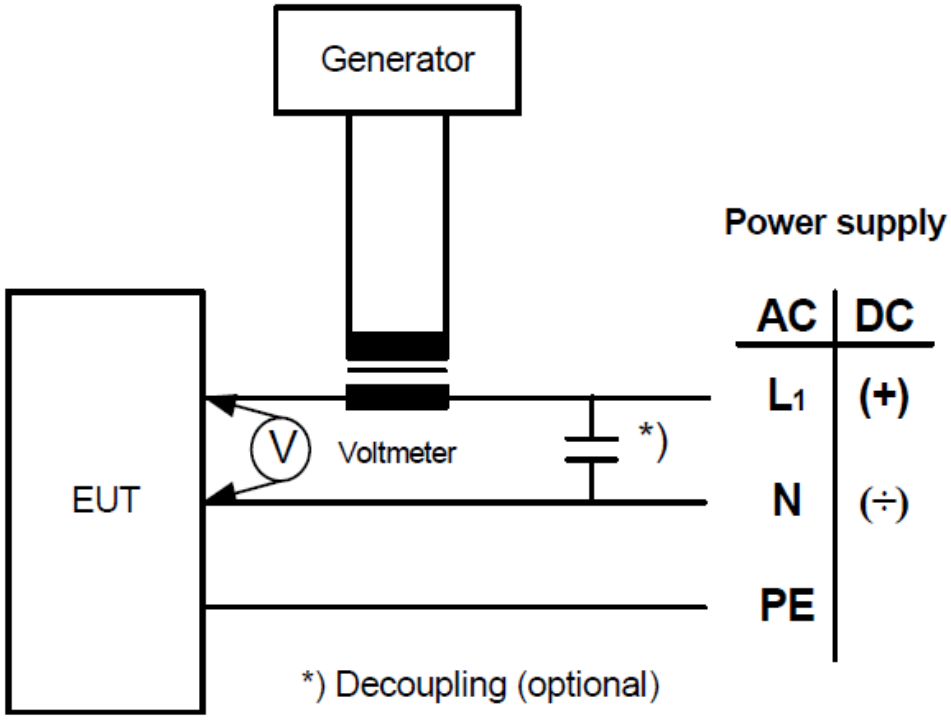


Figure - Test Set-up – Conducted Low Frequency Test

End of Document

E11 Unified requirements for systems with voltages above 1 kV up to 15 kV

(1991) (Rev.1 May 2001) (Rev.2 July 2003) (Rev.3 Feb 2015) (Corr.1 June 2018) (Rev.4 Feb 2021)

1. General

1.1 Field of application

The following requirements apply to a.c. three-phase systems with nominal voltage exceeding 1kV, the nominal voltage is the voltage between phases.

If not otherwise stated herein, construction and installation applicable to low voltage equipment generally apply to high voltage equipment.

1.2 Nominal system voltage

The nominal system voltage is not to exceed 15 kV.

Note: Where necessary for special application, higher voltages may be accepted by the Society.

1.3 High-voltage, low-voltage segregation

Equipment with voltage above about 1 kV is not to be installed in the same enclosure as low voltage equipment, unless segregation or other suitable measures are taken to ensure that access to low voltage equipment is obtained without danger.

2. System Design

2.1 Distribution

2.1.1 Network configuration for continuity of ship services

It is to be possible to split the main switchboard into at least two independent sections, by means of at least one circuit breaker or other suitable disconnecting devices, each supplied by at least one generator. If two separate switchboards are provided and interconnected with cables, a circuit breaker is to be provided at each end of the cable.

Services which are duplicated are to be divided between the sections.

Note:

1. Rev.3 of this UR is to be uniformly implemented by IACS Societies from 1 July 2016.

2. Rev.4 of this UR is to be uniformly implemented by IACS Societies for high voltage systems which are installed in new ships contracted for construction on or after 1 July 2022.

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

E11
(cont)

2.1.2 Earthed neutral systems

In case of earth fault, the current is not to be greater than full load current of the largest generator on the switchboard or relevant switchboard section and not less than three times the minimum current required to operate any device against earth fault.

It is to be assured that at least one source neutral to ground connection is available whenever the system is in the energised mode. Electrical equipment in directly earthed neutral or other neutral earthed systems is to withstand the current due to a single phase fault against earth for the time necessary to trip the protection device.

2.1.3 Neutral disconnection

Means of disconnection are to be fitted in the neutral earthing connection of each generator so that the generator may be disconnected for maintenance and for insulation resistance measurement.

2.1.4 Hull connection of earthing impedance

All earthing impedances are to be connected to the hull. The connection to the hull is to be so arranged that any circulating currents in the earth connections do not interfere with radio, radar, communication and control equipment circuits.

2.1.5 Divided systems

In the systems with neutral earthed, connection of the neutral to the hull is to be provided for each section.

2.2 Degrees of protection

2.2.1 General

Each part of the electrical installation is to be provided with a degree of protection appropriate to the location, as a minimum the requirements of IEC 60092-201:2019.

2.2.2 Rotating machines

The degree of protection of enclosures of rotating electrical machines is to be at least IP 23. The degree of protection of terminals is to be at least IP44.

For motors installed in spaces accessible to unqualified personnel, a degree of protection against approaching or contact with live or moving parts of at least IP4X is required.

2.2.3 Transformers

The degree of protection of enclosures of transformers is to be at least IP23.

For transformers installed in spaces accessible to unqualified personnel a degree of protection of at least IP4X is required.

For transformers not contained in enclosures, see para 7.1.

E11
(cont)

2.2.4 Switchgear, controlgear assemblies and converters

The degree of protection of metal enclosed switchgear, controlgear assemblies and static convertors is to be at least IP32. For switchgear, control gear assemblies and static converters installed in spaces accessible to unqualified personnel, a degree of protection of at least IP4X is required.

2.3 Insulation

2.3.1 Air clearance

In general, for Non Type Tested equipment phase-to-phase air clearances and phase-to-earth air clearances between non-insulated parts are to be not less than those specified in Table 2.3.1.

Table 2.3.1

Nominal Voltage (kV)	Minimum air clearance (mm)
3(3.3)	55
6 (6.6)	90
10 (11)	120
15	160

Intermediate values may be accepted for nominal voltages provided that the next higher air clearance is observed.

In the case of smaller distances, appropriate voltage impulse test must be applied.

2.3.2 Creepage distances

Creepage distances between live parts and between live parts and earthed metal parts are to be in accordance with IEC 60092-503:2007 for the nominal voltage of the system, the nature of the insulation material and the transient overvoltage developed by switch and fault conditions.

2.4 Protection

2.4.1 Faults on the generator side of circuit breaker

Protective devices are to be provided against phase-to-phase faults in the cables connecting the generators to the main switchboard and against interwinding faults within the generators. The protective devices are to trip the generator circuit breaker and to automatically de-excite the generator.

In distribution systems with a neutral earthed, phase to earth faults are also to be treated as above.

2.4.2 Faults to earth

Any earth fault in the system is to be indicated by means of a visual and audible alarm. In low impedance or direct earthed systems provision is to be made to automatic disconnect the faulty circuits. In high impedance earthed systems, where outgoing feeders will not be

E11 (cont)

isolated in case of an earth fault, the insulation of the equipment is to be designed for the phase to phase voltage.

Note: Earthing factor is defined as the ratio between the phase to earth voltage of the health phase and the phase to phase voltage. This factor may vary between $(1/\sqrt{3})$ and 1.

A system is defined effectively earthed (low impedance) when this factor is lower than 0.8. A system is defined non-effectively earthed (high impedance) when this factor is higher than 0.8.

2.4.3 Power transformers

Power transformers are to be provided with overload and short circuit protection. When transformers are connected in parallel, tripping of the protective devices at the primary side has to automatically trip the switch connected at the secondary side.

2.4.4 Voltage transformers for control and instrumentation

Voltage transformers are to be provided with overload and short circuit protection on the secondary side.

2.4.5 Fuses

Fuses are not to be used for overload protection.

2.4.6 Low voltage systems

Lower voltage systems supplied through transformers from high voltage systems are to be protected against overvoltages. This may be achieved by:

i) direct earthing of the lower voltage system.
ii) appropriate neutral voltage limiters.
iii) earthed screen between the primary and secondary windings of transformers.

3. Rotating machinery

3.1 Stator windings of generators

Generator stator windings are to have all phase ends brought out for the installation of the differential protection.

3.2 Temperature detectors

Rotating machinery is to be provided with temperature detectors in their stator windings to actuate a visual and audible alarm in a normally attended position whenever the temperature exceeds the permissible limit.

If embedded temperature detectors are used, means are to be provided to protect the circuit against overvoltage.

3.3 Tests

In addition to the tests normally required for rotating machinery, a high frequency high

E11 (cont)

voltage test in accordance with IEC 60034-15:2009 is to be carried out on the individual coils in order to demonstrate a satisfactory withstand level of the inter-turn insulation to steep fronted switching surges.

4. Power Transformers

4.1 General

Dry type transformers have to comply with IEC 60076-11:2018. Liquid cooled transformers have to comply with the applicable Parts of the IEC 60076 Series. Oil immersed transformers are to be provided with the following alarms and protections:

- liquid level (Low) - alarm
- liquid temperature (High) - alarm
- liquid level (Low) - trip or load reduction
- liquid temperature (High) - trip or load reduction
- gas pressure relay (High) - trip

5. Cables

5.1 General

Cables are to be constructed in accordance with the IEC 60092-353:2016 and 60092-354:2020 or other equivalent Standard.

6. Switchgear and controlgear assemblies

6.1 General

Switchgear and controlgear assemblies are to be constructed according to the IEC 62271-200:2011 and the following additional requirements.

6.2 Construction

6.2.1 Mechanical construction

Switchgear is to be of metal – enclosed type in accordance with IEC 62271-200:2011 or of the insulation – enclosed type in accordance with the IEC 62271-201:2014.

6.2.2 Locking facilities

Withdrawable circuit breakers and switches are to be provided with mechanical locking facilities in both service and disconnected positions. For maintenance purposes, key locking of withdrawable circuit breakers and switches and fixed disconnectors is to be possible.

Withdrawable circuit breakers are to be located in the service position so that there is no relative motion between fixed and moving portions.

6.2.3 Shutters

The fixed contacts of withdrawable circuit breakers and switches are to be so arranged that in the withdrawable position the live contacts are automatically covered.
Shutters are to be clearly marked for incoming and outgoing circuits. This may be achieved with the use of colours or labels.

E11
(cont)

6.2.4 Earthing and short-circuiting

For maintenance purposes an adequate number of earthing and short-circuiting devices is to be provided to enable circuits to be worked upon with safety.

6.2.5 Internal arc Classification (IAC)

Switchgear and controlgear assemblies shall be internal arc classified (IAC).

Where switchgear and controlgear are accessible by authorized personnel only Accessibility Type A is sufficient (IEC 62271-200:2011; Annex AA; AA 2.2). Accessibility Type B is required if accessible by non-authorised personnel.

Installation and location of the switchgear and controlgear shall correspond with its internal arc classification and classified sides (F, L and R).

6.3 Auxiliary systems

6.3.1 Source and capacity of supply

If electrical energy and/or physical energy is required for the operation of circuit breakers and switches, a stored supply of such energy is to be provided for at least two operations of all the components.

However, the tripping due to overload or short-circuit, and under-voltage is to be independent of any stored electrical energy sources. This does not preclude shunt tripping provided that alarms are activated upon lack of continuity in the release circuits and power supply failures.

6.3.2 Number of external supply sources

When external source of supply is necessary for auxiliary circuits, at least two external sources of supply are to be provided and so arranged that a failure or loss of one source will not cause the loss of more than one generator set and/or set of essential services.
Where necessary one source of supply is to be from the emergency source of electrical power for the start up from dead ship condition.

6.4 High voltage test

A power-frequency voltage test is to be carried out on any switchgear and controlgear assemblies. The test procedure and voltages are to be according to the IEC 62271-200:2011 section 7/ routine test.

E11
(cont)

7. Installation

7.1 Electrical equipment

Where equipment is not contained in an enclosure but a room forms the enclosure of the equipment, the access doors are to be so interlocked that they cannot be opened until the supply is isolated and the equipment earthed down.

At the entrance of the spaces where high-voltage electrical equipment is installed, a suitable marking is to be placed which indicates danger of high-voltage. As regard the high-voltage electrical equipment installed out-side a.m. spaces, the similar marking is to be provided. An adequate, unobstructed working space is to be left in the vicinity of high voltage equipment for preventing potential severe injuries to personnel performing maintenance activities. In addition, the clearance between the switchboard and the ceiling/deckhead above is to meet the requirements of the Internal Arc Classification according to IEC 62271-200:2011 (see 6.2.5).

7.2 Cables

7.2.1 Runs of cables

In accommodation spaces, high voltage cables are to be run in enclosed cable transit systems.

7.2.2 Segregation

High voltage cables are to be segregated from cables operating at different voltage ratings each other; in particular, they are not to be run in the same cable bunch, nor in the same ducts or pipes, or, in the same box.
Where high voltage cables of different voltage ratings are installed on the same cable tray, the air clearance between cables is not to be less than the minimum air clearance for the higher voltage side in 2.3.1. However, high voltage cables are not to be installed on the same cable tray for the cables operating at the nominal system voltage of 1 kV and less.

7.2.3 Installation arrangements

High voltage cables, in general, are to be installed on cable trays when they are provided with a continuous metallic sheath or armour which is effectively bonded to earth; otherwise they are to be installed for their entire length in metallic castings effectively bonded to earth.

7.2.4 Terminations

Terminations in all conductors of high voltage cables are to be, as far as practicable, effectively covered with suitable insulating material. In terminal boxes, if conductors are not insulated, phases are to be separated from earth and from each other by substantial barriers of suitable insulating materials.
High voltage cables of the radial field type, i.e. having a conductive layer to control the electric field within the insulation, are to have terminations which provide electric stress control.

Terminations are to be of a type compatible with the insulation and jacket material of the cable and are to be provided with means to ground all metallic shielding components (i.e. tapes, wires etc).

E11 (cont)

7.2.5 Marking

High voltage cables are to be readily identifiable by suitable marking.

7.2.6 Test after installation

Before a new high voltage cable installation, or an addition to an existing installation, is put into service a voltage withstand test is to be satisfactorily carried out on each completed cable and its accessories.

The test is to be carried out after an insulation resistance test.

For cables with rated voltage (U_0/U) above 1.8/3 kV (U_m=3.6 kV) an a.c. voltage withstand test may be carried out upon advice from high voltage cable manufacturer. One of the following test methods to be used:

a) test for 5 min with the phase-to-phase voltage of the system applied between the conductor and the metallic screen/sheath.

b) test for 24 h with the normal operating voltage of the system.

Alternatively, a d.c. test voltage equal to 4 Uo may be applied for 15 minutes.

For cables with rated voltage (U_0/U) up to 1.8/3 kV (U_m=3.6 kV) a d.c. voltage equal to 4 Uo shall be applied for 15 minutes.

After completion of the test, the conductors are to be connected to earth for a sufficient period in order to remove any trapped electric charge.

An insulation resistance test is then repeated.

End of Document

E12 Electrical Equipment allowed in paint stores and in the enclosed spaces leading to paint stores

(1994) (Corr.1 1997) (Rev.1 May 2001) (Rev.2 Dec 2020)

1. General

Electrical equipment is to be installed in paint stores and in ventilation ducts serving such spaces only when it is essential for operational services.

Certified safe type equipment of the following type is acceptable;

a. intrinsically safe Exi

b. flameproof Exd

c. pressurised Exp

d. increased safety Exe

e. special protection Exs

Cables (through-runs or terminating cables) of armoured type or installed in metallic conduits are to be used.

2. Minimum Requirements

The minimum requirements for the certified safe type equipment are as follows:

- explosion group II B

- temperature class T3

Footnote:
The paint stores and inlet and exhaust ventilation ducts under Clause 1 are classified as Zone-1 and areas on open deck under Clause 4 as Zone 2, as defined in IEC 60092-502:1999.

A watertight door may be considered as being gastight.

Note:

1. Rev.2 of this Unified Requirement is to be uniformly implemented by IACS Societies on ships contracted for construction on and after 1 January 2022.

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

E12
(Cont)

3. Special requirements

3.1 Switches, protective devices, motor control gear of electrical equipment installed in a paint store are to interrupt all poles or phases and preferably are to be located in non-hazardous space.

3.2 In the areas on open deck within 1m of inlet and exhaust ventilation openings or within 3 m of exhaust mechanical ventilation outlets, the following electrical equipment may be installed:

- electrical equipment with the type of protection as permitted in paint stores;
- equipment of protection class Exn;
- appliances which do not generate arcs in service and whose surface does not reach unacceptably high temperature;
- appliances with simplified pressurised enclosures or vapour-proof enclosures (minimum class of protection IP55) whose surface does not reach unacceptably high temperature; or
- cables as specified in clause 1.

3.3 The enclosed spaces giving access to the paint store may be considered as nonhazardous, provided that:

- the door to the paint store is a gastight door with self-closing devices without holding back arrangements,
- the paint store is provided with an acceptable, independent, natural ventilation system ventilated from a safe area, and
- warning notices are fitted adjacent to the paint store entrance stating that the store contains flammable liquids.

End of Document

E13 Test requirements for Rotating Machines

(1996) (Rev.1 May 2001) (Corr.1 May 2004) (Rev.2 Aug 2015) (Corr.1 June 2018) (Rev.3 Dec 2020) (Corr.1 May 2022)

1. General

All machines are to be tested by the manufacturer.

Manufacturer's test records are to be provided for machines for essential services, for other machines they are to be available upon request.

All tests are to be carried out according to IEC 60092-301:1980/AMD2:1995.

All machines of 100kW and over, intended for essential services, are to be surveyed by the Society during test and, if appropriate, during manufacturing.

Note: An alternative survey scheme may be agreed by the Society with the manufacturer whereby attendance of the Surveyor will not be required as required above.

Note:

1. Rev.2 of this UR is to be uniformly implemented by IACS Societies for rotating machines:

   i) when an application for certification of a rotating machine is dated on or after 1 January 2017; or

   ii) which are installed in new ships for which the date of contract for construction is on or after 1 January 2017.

2. Rev.3 of this UR is to be uniformly implemented by IACS Societies for rotating machines:

   i) when an application for certification of a rotating machine is dated on or after 1 January 2022; or

   ii) which are installed in new ships for which the date of contract for construction is on or after 1 January 2022.

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

E13
(cont)

2. Shaft Material

Shaft material for electric propulsion motors and for main engine driven generators where the shaft is part of the propulsion shafting is to be certified by the Society.

Shaft material for other machines is to be in accordance with recognised international or national standard.

3. Tests

Type tests are to be carried out on a prototype machine or on the first of a batch of machines, and routine tests carried out on subsequent machines in accordance with Table 1.

Note: Test requirements may differ for shaft generators, special purpose machines and machines of novel construction.

E13
(cont)

Table 1

No.	Tests	A.C. Generators		Motors	
		Type test[1]	Routine test[2]	Type test[1]	Routine test[2]
1.	Examination of the technical documentation, as appropriate and visual inspection	x	x	x	x
2.	Insulation resistance measurement	x	x	x	x
3.	Winding resistance measurement	x	x	x	x
4.	Verification of the voltage regulation system	x	x[3]		
5.	Rated load test and temperature rise measurements	x		x	
6.	Overload/overcurrent test	x	x[4]	x	x[4]
7.	Verification of steady short circuit conditions[5]	x			
8.	Overspeed test	x	x	x[6]	x[6]
9.	Dielectric strength test	x	x	x	x
10.	No-load test	x	x	x	x
11.	Verification of degree of protection	x		x	
12.	Verification of bearings	x	x	x	x

[1] Type tests on prototype machine or tests on at least the first batch of machines.

[2] The report of machines routine tested is to contain the manufacturer's serial number of the machine which has been type tested and the test result.

[3] Only functional test of voltage regulator system.

[4] Only applicable for machine of essential services rated above 100kW.

[5] Verification of steady short circuit condition applies to synchronous generators only.

[6] Not applicable for squirrel cage motors.

E13
(cont)

4. Description of the test

4.1 Examination of the technical documentation, as appropriate and visual inspection

4.1.1 Examination of the technical documentation

Technical documentation of machines rated at 100kW and over is to be available for examination by the Surveyor.

4.1.2 Visual inspection

A visual examination is to be made of the machine to ensure, as far as is practicable, that it complies with technical documentation.

4.2 Insulation resistance measurement

Immediately after the high voltage tests the insulation resistances are to be measured using a direct current insulation tester between:

a) all current carrying parts connected together and earth,

b) all current carrying parts of different polarity or phase, where both ends of each polarity or phase are individually accessible.

The minimum values of test voltages and corresponding insulation resistances are given in Table 2. The insulation resistance is to be measured close to the operating temperature, or an appropriate method of calculation is to be used.

Table 2

Related Voltage Un (V)	Minimum Test Voltage (V)	Test Minimum Insulation Resistance (MΩ)
Un ≤ 250	2 x Un	1
250 < Un ≤ 1000	500	1
1000 < Un ≤ 7200	1000	(Un / 1000) + 1
7200 < Un ≤ 15000	5000	(Un / 1000) + 1

4.3 Winding resistance measurement

The resistances of the machine windings are to be measured and recorded using an appropriate bridge method or voltage and current method.

4.4 Verification of the voltage regulation system

The alternating current generator, together with its voltage regulation system shall, at all loads from no-load running to full load, be able to keep rated voltage at the rated power factor under steady conditions within ± 2.5%. These limits may be increased to ± 3.5% for emergency sets.

When the generator is driven at rated speed, giving its rated voltage, and is subjected to a sudden change of symmetrical load within the limits of specified current and power factor, the voltage is not to fall below 85% nor exceed 120% of the rated voltage.

E13 (cont)

The voltage of the generator is then to be restored to within plus or minus 3% of the rated voltage for the main generator sets in not more than 1.5 s. For emergency sets, these values may be increased to plus or minus 4% in not more than 5 s, respectively.

In the absence of precise information concerning the maximum values of the sudden loads, the following conditions may be assumed: 60% of the rated current with a power factor of between 0.4 lagging and zero to be suddenly switched on with the generator running at no load, and then switched off after steady - state conditions have been reached. Subject to Classification Society's approval, such voltage regulation during transient conditions may be calculated values based on the previous type test records, and need not to be tested during factory testing of a generator.

4.5 Rated load test and temperature rise measurements

The temperature rises are to be measured at the rated output, voltage, frequency and the duty for which the machine is rated and marked in accordance with the testing methods specified in IEC 60034-1:2017, or by means of a combination of other tests.

The limits of temperature rise are those specified in the relevant table of IEC 60034-1:2017 adjusted as necessary for the ambient reference temperatures specified in UR M40.

4.6 Overload/overcurrent tests

Overload test is to be carried out as a type test for generators as a proof of overload capability of generators and excitation system, for motors as a proof of momentary excess torque as required in IEC 60034-1:2017. The overload test can be replaced at routine test by the overcurrent test. The over current test shall be the proof of current capability of windings, wires, connections etc. of each machine. The overcurrent test can be done at reduced speed (motors) or at short circuit (generators).

4.7 Verification of steady short-circuit conditions

It is to be verified that under steady-state short-circuit conditions, the generator with its voltage regulating system is capable of maintaining, without sustaining any damage, a current of at least three times the rated current for a duration of at least 2 s or, where precise data is available, for a duration of any time delay which will be fitted in the tripping device for discrimination purposes.

In order to provide sufficient information to the party responsible for determining the discrimination settings in the distribution system where the generator is going to be used, the generator manufacturer shall provide documentation showing the transient behaviour of the short circuit current upon a sudden short-circuit occurring when excited, and running at nominal speed. The influence of the automatic voltage regulator shall be taken into account, and the setting parameters for the voltage regulator shall be noted together with the decrement curve. Such a decrement curve shall be available when the setting of the distribution system's short-circuit protection is calculated. The decrement curve need not be based on physical testing. The manufacturer's simulation model for the generator and the voltage regulator may be used where this has been validated through the previous type test on the same model.

E13 (cont)

4.8 Overspeed test

Machines are to withstand the overspeed test as specified in to IEC 60034-1:2017. This test is not applicable for squirrel cage motors.

4.9 Dielectric strength test

Machines are to withstand a dielectric test as specified in IEC 60034-1:2017.

For high voltage machine an impulse test is to be carried out on the coils according to UR E11.

4.10 No load test

Machines are to be operated at no load and rated speed whilst being supplied at rated voltage and frequency as a motor or if a generator it is to be driven by a suitable means and excited to give rated terminal voltage.

During the running test, the vibration of the machine and operation of the bearing lubrication system, if appropriate, are to be checked.

4.11 Verification of degree of protection

As specified in IEC 60034-5:2000+AMD1:2006.

4.12 Verification of bearings

Upon completion of the above tests, machines which have sleeve bearings are to be opened upon request for examination by the Classification Society Surveyor, to establish that the shaft is correctly seated in the bearing shells.

End of Document

E15 Electrical Services Required to be Operable Under Fire Conditions and Fire Resistant Cables

(Nov 1999) (Rev.1 May 2004) (Rev.2 Feb 2006) (Rev.3 Dec 2014) (Rev.4 Dec 2020)

1 Electrical services required to be operable under fire conditions are as follows:

- Control and power systems to power-operated fire doors and status indication for all fire doors
- Control and power systems to power-operated watertight doors and their status indication
- Emergency fire pump
- Emergency lighting
- Fire and general alarms
- Fire detection systems
- Fire-extinguishing systems and fire-extinguishing media release alarms
- Low location lighting
- Public address systems
- Remote emergency stop/shutdown arrangements for systems which may support the propagation of fire and/or explosion

2 Where cables for services specified in 1 including their power supplies pass through high fire risk areas, and in addition for passenger ships, main vertical fire zones, other than those which they serve, they are to be so arranged that a fire in any of these areas or zones does not affect the operation of the service in any other area or zone. This may be achieved by either of the following measures:

a) Cables being of a fire resistant type complying with IEC 60331-1:2018 for cables of greater than 20 mm overall diameter, otherwise IEC 60331-21:1999+AMD1:2009 or IEC 60331-2:2018 for cables with an overall diameter not exceeding 20 mm, are installed and run continuous to keep the fire integrity within the high fire risk area, see Figure 1.

Notes:

1. Rev.3 of this UR is to be uniformly implemented by IACS Societies from 1 January 2016.

2. Rev.4 of this Unified Requirement is to be uniformly implemented by IACS Societies on ships contracted for construction on and after 1 January 2022.

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

E15
(cont'd)

b) At least two-loops/radial distributions run as widely apart as is practicable and so arranged that in the event of damage by fire at least one of the loops/radial distributions remains operational.

c) Systems that are self monitoring, fail safe or duplicated with cable runs as widely separated as is practicable may be exempted.

3 The electrical cables to the emergency fire pump are not to pass through the machinery spaces containing the main fire pumps and their source(s) of power and prime mover(s). They are to be of a fire resistant type, in accordance with 2 (a), where they pass through other high fire risk areas.

Notes:

a) For the purpose of E15 application, the definition for "high fire risk areas" is the following:

(i) Machinery spaces as defined by Regulation 3.30 of SOLAS Chapter II-2, as amended by IMO resolutions up to MSC.421(98) (hereinafter the same), except spaces having little or no fire risk as defined by paragraphs (10) of Regulation 9.2.2.3.2.2 of SOLAS Chapter II-2. (Including the interpretations for tables 9.3, 9.4, 9.5, 9.6, 9.7 and 9.8 given in MSC/Circ.1120 as amended by MSC.1/Circ.1436 and MSC.1/Circ.1510)

(ii) Spaces containing fuel treatment equipment and other highly flammable substances

(iii) Galley and Pantries containing cooking appliances

(iv) Laundry containing drying equipment

(v) Spaces as defined by paragraphs (8), (12), and (14) of Regulation 9.2.2.3.2.2 of SOLAS Chapter II-2 for ships carrying more than 36 passengers

b) Fire resistant type cables should be easily distinguishable.

c) For special cables, requirements in the following standards may be used:

IEC 60331-23:1999: Procedures and requirements – Electric data cables
IEC 60331-25:1999: Procedures and requirements – Optical fibre cables

E15
(cont'd)

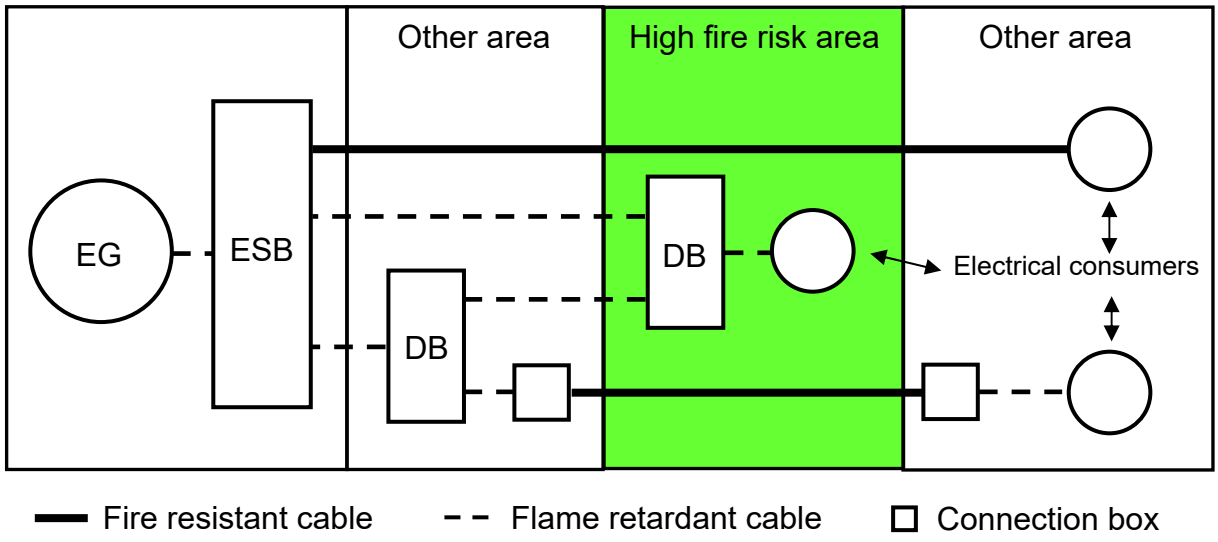


Figure 1

End of Document

E16 Cable trays/protective casings made of plastics materials

(June 2002)

1. General requirement

Cable trays/protective casings made of plastics materials are to be type tested [1].

Note: "Plastics" means both thermoplastic and thermosetting plastic materials with or without reinforcement, such as PVC and fibre reinforced plastics - FRP. "Protective casing" means a closed cover in the form of a pipe or other closed ducts of non-circular shape.

2. Installation Requirements

2.1. Cable trays/protective casings made of plastics materials are to be supplemented by metallic fixing and straps such that in the event of a fire they, and the cables affixed, are prevented from falling and causing an injury to personnel and/or an obstruction to any escape route.

Note: When plastics cable trays/protective casings are used on open deck, they are additionally to be protected against UV light.

2.2. The load on the cable trays/protective casings is to be within the Safe Working Load (SWL). The support spacing is not to be greater than the Manufacturer's recommendation nor in excess of spacing at the SWL test. In general the spacing is not to exceed 2 meters.

Note: The selection and spacing of cable tray/protective casing supports are to take into account:
- cable trays/protective casings' dimensions;
- mechanical and physical properties of their material;
- mass of cable trays/protective casings;
- loads due weight of cables, external forces, thrust forces and vibrations;
- maximum accelerations to which the system may be subjected;
- combination of loads .

2.3. The sum of the cables' total cross-sectional area, based on the cables' external diameter, is not to exceed 40% of the protective casing's internal cross-sectional area. This does not apply to a single cable in a protective casing.

Note:

1) Cable trays/protective casings made of plastic materials are to be type tested in accordance with the Type Approval Procedure applied by the Society. For guidance on testing, refer to REC 73.

E17
(June 2002)
(Rev.1
Feb 2021)

Generators and generator systems, having the ship's propulsion machinery as their prime mover, not forming part of the ship's main source of electrical power

Generators and generator systems, having the ship's propulsion machinery as their prime mover but not forming part of the ship's main source of electrical power[1] may be used whilst the ship is at sea to supply electrical services required for normal operational and habitable conditions provided that:

1. there are sufficient and adequately rated additional generators fitted, which constitute the main source of electrical power required by SOLAS, meeting the requirements of IEC 60092-201:2019 paragraph 8.1.1.

2. arrangements are fitted to automatically start one or more of the generators, constituting the main source of electrical power required by SOLAS, in compliance with paragraph 2.2 of SC 157 and also upon the frequency variations exceeding ± 10% of the limits specified below.

3. within the declared operating range of the generators and/or generator systems the specified limits for the voltage variations in IEC 60092-301:1980/AMD2:1995 and the frequency variations in UR E5 can be met.

4. the short circuit current of the generator and/or generator system is sufficient to trip the generator/generator system circuit-breaker taking into account the selectivity of the protective devices for the distribution system.

5. where considered appropriate, load shedding arrangements are fitted to meet the requirements of paragraph 2.3 of SC 157.

6. on ships having remote control of the ship's propulsion machinery from the navigating bridge means are provided, or procedures be in place, so as to ensure that supplies to essential services are maintained during manoeuvring conditions in order to avoid a blackout situation[2].

Footnotes:

1. Such generator systems are those whose operation does not meet the requirements of IEC 60092-201:2019, paragraph 8.1.1.

2. A 'blackout situation' means that the main and auxiliary machinery installations, including the main power supply, are out of operation but the services for bringing them into operation (e.g. compressed air, starting current from batteries etc.) are available.

Note:

1. Rev.1 of this UR is to be uniformly implemented by IACS Societies on ships for which the date of contract for construction is on or after 1 July 2022.

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

End of Document

E18 Recording of the Type, Location and Maintenance Cycle of Batteries

(July 2003) (Rev.1 Dec 2014)

1. Where batteries are fitted for use for essential (UI SC134) and emergency services a schedule of such batteries is to be compiled and maintained. The schedule, which is to be reviewed by the Society during plan approval or the newbuilding survey, is to include at least the following information regarding the battery(ies):

- Type and manufacturer's type designation.
- Voltage and ampere-hour rating.
- Location.
- Equipment and/or system(s) served.
- Maintenance/replacement cycle dates.
- Date(s) of last maintenance and/or replacement.
- For replacement batteries in storage, the date of manufacture and shelf life.[1]

2. Procedures are to be put in place to ensure that where batteries are replaced that they are of an equivalent performance type.

3. Where vented[2] type batteries replace valve-regulated sealed[3] types, it is to be ensured that there is adequate ventilation[4] and that the Society's requirements relevant to the location and installation of vented types batteries are complied with.

4. Details of the schedule and of the procedures are to be included in the ship's safety management system and be integrated into the ship's operational maintenance routine as appropriate[5] to be verified by the Society's surveyor.

Note:

1. Rev.1 of this UR is to be uniformly implemented by IACS Societies from 1 January 2016.

E18
(cont)

1 Shelf life is the duration of storage under specified conditions at the end of which a battery retains the ability to give a specified performance.

2 A vented battery is one in which the cells have a cover provided with an opening through which products of electrolysis and evaporation are allowed to escape freely from the cells to atmosphere.

3 A valve-regulated battery is one in which cells are closed but have an arrangement (valve) which allows the escape of gas if the internal pressure exceeds a predetermined value.

4 The ventilation arrangements for installation of vented type batteries which have charging power higher than 2kW are to be such that the quantity of air expelled is at least equal to:

$Q = 110In$

where

n = number of cells in series

I = maximum current delivered by the charging equipment during gas formation, but not less than 25 per cent of the maximum obtainable charging current in amperes

Q = quantity of air expelled in litres/hr.

The ventilation rate for compartments containing valve-regulated batteries may be reduced to 25 per cent of that given above.

5 See section 10 of the IMO ISM Code.

End of Document

E19 Ambient Temperatures for Electrical Equipment installed in environmentally controlled spaces

(July 2003) (Rev.1 Sept. 2005)

1. Where electrical equipment is installed within environmentally controlled spaces the ambient temperature for which the equipment is to be suitable may be reduced from 45°C and maintained at a value not less than 35°C provided:

- the equipment is not for use for emergency services.
- temperature control is achieved by at least two cooling units so arranged that in the event of loss of one cooling unit, for any reason, the remaining unit(s) is capable of satisfactorily maintaining the design temperature.
- the equipment is able to be initially set to work safety within a 45°C ambient temperature until such a time that the lesser ambient temperature may be achieved; the cooling equipment is to be rated for a 45°C ambient temperature.
- audible and visual alarms are provided, at a continually manned control station, to indicate any malfunction of the cooling units.

2. In accepting a lesser ambient temperature than 45°C, it is to be ensured that electrical cables for their entire length are adequately rated for the maximum ambient temperature to which they are exposed along their length.

3. The equipment used for cooling and maintaining the lesser ambient temperature is to be classified as a secondary essential service, in accordance with UI SC 134 and to be subject to survey in accordance with the requirements of the relevant Society.

END

E20 Installation of electrical and electronic equipment in engine rooms protected by fixed water-based local application fire-fighting systems (FWBLAFFS)

(May 2004) (Rev.1 June 2009)

Definitions:

Protected space:

- Is a machinery space where a FWBLAFFS is installed.

Protected areas:

- Areas within a protected space which is required to be protected by FWBLAFFS.

Adjacent areas:

- Areas, other than protected areas, exposed to direct spray.
- Areas, other than those defined above, where water may extend.

See also Fig. 1

Electrical and electronic equipment enclosures located within areas protected by FWBLAFFS and those within adjacent areas exposed to direct spray are to have a degree of protection not less than IP44, except where evidence of suitability is submitted to and approved by the Society.

The electrical and electronic equipment within adjacent areas not exposed to direct spray may have a lower degree of protection provided evidence of suitability for use in these areas is submitted taking into account the design and equipment layout, e.g. position of inlet ventilation openings, cooling airflow for the equipment is to be assured.

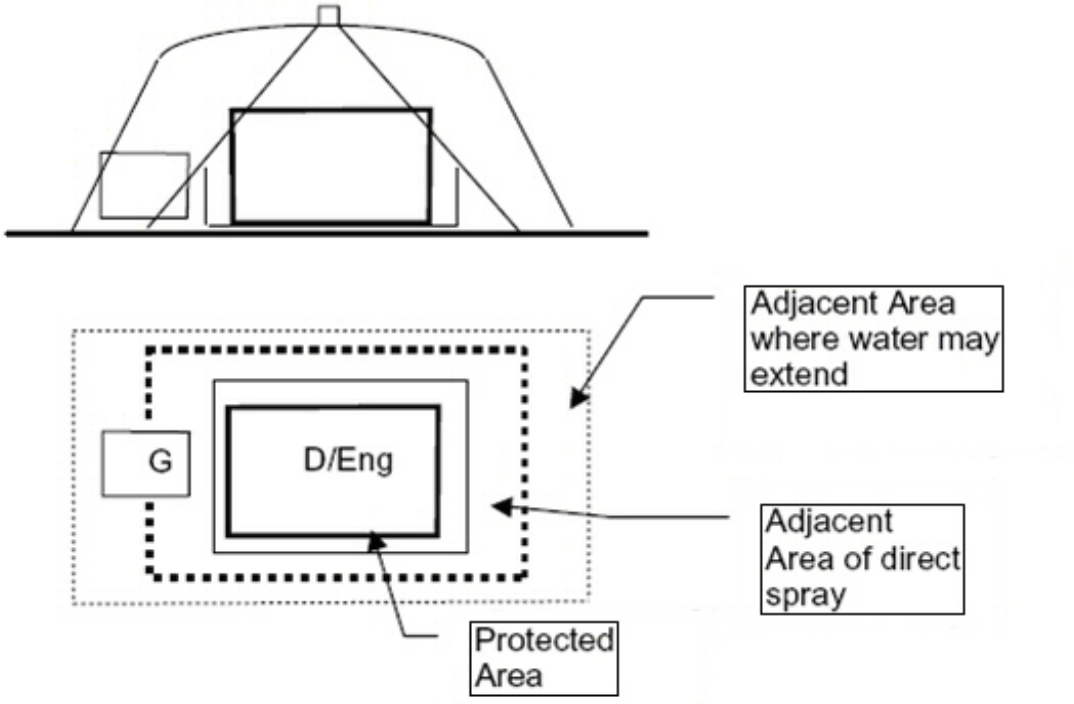
Note

1. Additional precautions may be required to be taken in respect of:

    a. tracking as the result of water entering the equipment
    b. potential damage as the result of residual salts from sea water systems
    c. high voltage installations
    d. personnel protection against electric shock

E20
(cont)

Fig. 1



End of Document

E21 Requirements for uninterruptible power system (UPS) units as alternative and/or transitional power

(Sep 2005)
(Rev.1
Feb 2021)
(Corr.1
June 2022)

Scope:

These requirements to UPS units, as defined in IEC 62040-3:2011, apply when providing an alternative power supply or transitional power supply to services as defined in SOLAS II-1/42 and SOLAS II-1/43.

A UPS unit complying with these requirements may provide an alternative power supply as an accumulator battery in terms of being an independent power supply for services defined in SOLAS II-1/42.2.3 or SOLAS II-1/43.2.4.

Definitions:

Uninterruptible Power System (UPS) - combination of converters, switches and energy storage means, for example batteries, constituting a power system for maintaining continuity of load power in case of input power failure [IEC 62040-3:2011]

Off-line UPS unit - a UPS unit where under normal operation the output load is powered from the bypass line (raw mains) and only transferred to the inverter if the bypass supply fails or goes outside preset limits. This transition will invariably result in a brief (typically 2 to 10 ms) break in the load supply.

Line interactive UPS unit - an off-line UPS unit where the bypass line switch to stored energy power when the input power goes outside the preset voltage and frequency limits.

On-line UPS unit - a UPS unit where under normal operation the output load is powered from the inverter, and will therefore continue to operate without break in the event of the supply input failing or going outside preset limits.

Notes:

1. Rev.1 of this UR is to be uniformly implemented by IACS Societies:

   i) when an application for certification of UPS is dated on or after 1 July 2022; or

   ii) which are installed in new ships contracted for construction on or after 1 July 2022.

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

3. The “date of application for certification of UPS” is the date of whatever document the Classification Society requires/accepts as an application or request for certification of UPS.

E21
(cont)

1. Design and construction

1.1 UPS units are to be constructed in accordance with IEC 62040-1:2017, IEC 62040-2:2016, IEC 62040-3:2011, IEC 62040-4:2013 and/or IEC 62040-5-3:2016, as applicable, or an acceptable and relevant national or international standard.

1.2 The operation of the UPS is not to depend upon external services.

1.3 The type of UPS unit employed, whether off-line, line interactive or on-line, is to be appropriate to the power supply requirements of the connected load equipment.

1.4 An external bypass is to be provided.

1.5 The UPS unit is to be monitored and audible and visual alarm is to be given in a normally attended location for

- power supply failure (voltage and frequency) to the connected load,

- earth fault,

- operation of battery protective device,

- when the battery is being discharged, and

- when the bypass is in operation for on-line UPS units.

2. Location

2.1 The UPS unit is to be suitably located for use in an emergency.

2.2 UPS units utilising valve regulated sealed batteries may be located in compartments with normal electrical equipment, provided the ventilation arrangements are in accordance with the requirements of IEC 62040-1:2017, IEC 62040-2:2016, IEC 62040-3:2011, IEC 62040-4:2013 and/or IEC 62040-5-3:2016, as applicable, or an acceptable and relevant national or international standard.

3. Performance

3.1 The output power is to be maintained for the duration required for the connected equipment as stated in SOLAS II-1/42 or SOLAS II-1/43.

3.2 No additional circuits are to be connected to the UPS unit without verification that the UPS unit has adequate capacity. The UPS battery capacity is, at all times, to be capable of supplying the designated loads for the time specified in the regulations.

3.3 On restoration of the input power, the rating of the charge unit shall be sufficient to recharge the batteries while maintaining the output supply to the load equipment.

E21
(cont)

4. Testing and survey

4.1 UPS units of 50 kVA and over are to be surveyed by the Society during manufacturing and testing.

4.2 Appropriate testing is to be carried out to demonstrate that the UPS unit is suitable for its intended environment. This is expected to include as a minimum the following tests:

- Functionality, including operation of alarms;

- Temperature rise;

- Ventilation rate;

- Battery capacity.

4.3 Where the supply is to be maintained without a break following a power input failure, this is to be verified after installation by practical test.

End of Document

E22 Computer-based systems

(Dec 2006) (Corr.1 Oct 2007) (Rev.1 Sept 2010) (Rev.2 June 2016) (Rev.3 June 2023)

1 Introduction

1.1 Scope

These requirements apply to design, construction, commissioning and maintenance of computer-based systems where they depend on software for the proper achievement of their functions.
These requirements apply to systems which provide control, alarm, monitoring, safety, or internal vessel communication functions that are subject to classification requirements.

1.2 Exclusion

Computer-based systems that are covered by statutory regulations are excluded from the requirements of this UR.

Guidance:
Examples of such systems are navigation systems and radio communication system required by SOLAS chapter V and IV, and vessel loading instrument/stability computer.

For loading instrument/stability computer, IACS recommendation no.48 may be considered.

Note:

1. This UR is to be applied only to such systems on new ships contracted for construction on and after 1 January 2008 by IACS Societies.
2. Rev.1 of this UR is to be applied only to such systems on new ships contracted for construction on and after 1 January 2012 by IACS Societies.
3. Rev.2 of this UR is to be applied only to such systems on new ships contracted for construction on and after 1 July 2017 by IACS Societies.
4. Rev.3 of this UR is to be applied to such systems on new ships contracted for construction on and after 1 July 2024 by IACS Societies and may be used for other ships as non-mandatory guidance.
5. The “contracted for construction” date means the date on which the contract to build the vessel is signed between the prospective owner and the shipbuilder. For further details regarding the date of “contract for construction”, refer to IACS Procedural Requirement (PR) No. 29.

E22 (cont)

1.3 References

1.3.1 Normative standards

For the purposes of this UR, the following standards are normative:

- IACS UR E10 Test specification for type approval
- IACS UR E26 Cyber resilience of ships
- IACS UR E27 Cyber resilience of on-board systems and equipment

1.3.2 Informative standards

For the purposes of this UR, the following standards are listed for information and may be used for the development of hardware/software of computer-based systems:

- IEC 61508:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems
- ISO/IEC 12207:2017 Systems and software engineering – Software life cycle processes
- ISO 9001:2015 Quality Management Systems – Requirements
- ISO/IEC 90003:2018 Software engineering - Guidelines for the application of ISO 9001:2015 to computer software
- IEC 60092-504:2016 Electrical installations in ships - Part 504: Special features - Control and instrumentation
- ISO/IEC 25000:2014 Systems and software engineering - Systems and software Quality Requirements and Evaluation (SQuaRE) - Guide to SQuaRE
- ISO/IEC 25041:2012 Systems and software engineering - Systems and software Quality Requirements and Evaluation (SQuaRE) - Evaluation guide for developers, acquirers and independent evaluators
- IEC 61511:2016 Functional safety - Safety instrumented systems for the process industry sector
- ISO/IEC 15288:2015 Systems and software engineering - System life cycle process
- ISO 90007:2017 Quality management – Guidelines for configuration management
- ISO 24060:2021 Ships and marine technology - Ship software logging system for operational technology

Other industry standards may also be considered.

1.4 Structure

The general certification requirements for computer-based systems and the relation to type approval is described in paragraph 2. The requirements and extent of verification of a

E22 (cont)

computer-based system depends on its categorization into one of three categories. The categories are described in paragraph 3.

The requirements of this UR cover the lifecycle of computer-based system from design through operations. The requirements are split into groups representing the different phases of the life cycle and the roles responsible for fulfilling the requirements.
The activities related to the development and delivery of a computer-based system is described in paragraph 4, while the activities related to the maintenance in the operational phase are described in paragraph 5.

Management of changes to software and systems is given special attention in this UR, and the main aspects of a management of change process are described in paragraph 6.

Most requirements in this UR are related to the way of working, and thus focus on activities to be performed, but it also contains some technical requirements. The technical requirements on computer-based systems have been gathered in paragraph 7.

Each activity contains a requirement part which describes the minimum requirements on the role in question, and a part which describes the Class Society's verification of the activity in question.

1.5 Definition of abbreviations and terminology

1.5.1 Abbreviations

Table 1 Abbreviations

Abbreviation:	**Expansion:**
Cat I	Category one systems as defined in paragraph 3.1
Cat II	Category two systems as defined in paragraph 3.1
Cat III	Category three systems as defined in paragraph 3.1
COTS	Commercial off-the-shelf
FAT	Factory acceptance test
FMEA	Failure mode and effect analysis
IT	Information technology
OT	Operational technology
PMS	Planned maintenance system
SAT	System acceptance test
SOST	System of systems test
SSLS	Ship software logging system
UR	Unified requirement

E22
(cont)

1.5.2 Terminology

Table 2 Terminology

Term:	Definition:
Black-box description	A description of a system's functionality and behaviour and performance as observed from outside the system in question
Black-box test methods	Verification of the functionality, performance, and robustness of a system, sub-system or component by only manipulating the inputs and observing the outputs. This does not require any knowledge of the system's inner workings and focuses only on the observable behaviour of the system/component under test in order to achieve the desired level of verification.
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.
Failure mode description	A document describing the effects due to failures in the system, not failures in the equipment supported by the system. The following aspects shall be covered: - list of failures which are subject to assessment, with - description of the system response to each of the above failures - comments to the consequence of each of these failures
Owner	The organization or person which orders the vessel in the construction phase or the organization which owns or manages the vessel in service. In the context of this UR this is a defined role with specific responsibilities.
Parameterization	To configure and tune system and software functionality by changing parameters. It does not usually require-computer programming and is normally done by the system supplier or a service provider, not the operator or end-user.
Programmable device	Physical component where software is installed
Robustness	The ability to respond to abnormal inputs and conditions
Service supplier	A person or company, not employed by an IACS Member, who at the request of an equipment manufacturer, shipyard, vessel's owner or other client acts in connection with inspection work and provides services for a ship or a mobile offshore unit such as measurements, tests or maintenance of safety systems and equipment, the results of which are used by surveyors in making decisions affecting classification or statutory certification and services
Simulation test	Monitoring, control, or safety system testing where the equipment under control is partly or fully replaced with simulation tools, or where parts of the communication network and lines are replaced with simulation tools.

E22
(cont)

Term:	Definition:
Society Certificate	Compliance document issued by a Class Society stating: - conformity with applicable rules and requirements. - that the tests and inspections have been carried out on: - the finished certified component itself; or - on samples taken from earlier stages in the production of the component, when applicable. - that the inspection and tests were performed in the presence of the Surveyor or in accordance with special agreements, i.e. Alternative Certification Scheme (ACS)
Software component	A standalone piece of code that provides specific and closely coupled functionality.
Software master files	The computer-files that constitutes the original source of the software. For custom made software this may be readable source- code files, and for COTS software it may be different forms of binary files.
Software-structure	Overview of how the different software components interact and is commonly referred to as the Software Architecture, or Software Hierarchy
Sub-system	Identifiable part of a system, which may perform a specific function or set of functions.
Supplier	A generic term used for any organisation or person that is a contracted or a subcontracted provider of services, system components, or software.
System	A combination of components, equipment and logic which has a defined purpose, functionality, and performance. In the context of this UR, a specific system is delivered by one system supplier.
System of systems	A system which is made up of several systems In the context of this UR, the system of systems encompasses all monitoring, control and safety systems delivered from the Shipyard as a part of a vessel
System supplier	An organisation or person that is contracted or a subcontracted provider of system components or software under the coordination of the Systems integrator. In the context of this UR this is a defined role with specific responsibilities.
Systems integrator	Single organization or a person coordinating interaction between suppliers of systems and sub-systems on all stages of life cycle of computer-based systems in order to integrate them into a verified vessel-wide system of systems and to provide proper operation and maintenance of the computer-based systems. In the context of this UR this is a defined role with specific responsibilities. During the design and delivery phase the Shipyard is the default Systems integrator, during operations phase the Owner is the default.
Type approval Certificate	Compliance document issued by a Class Society by which the Society declares that a product design meets a minimum set of technical requirements
Vessel	Ship or offshore unit where the computer-based system is to be installed.

E22
(cont)

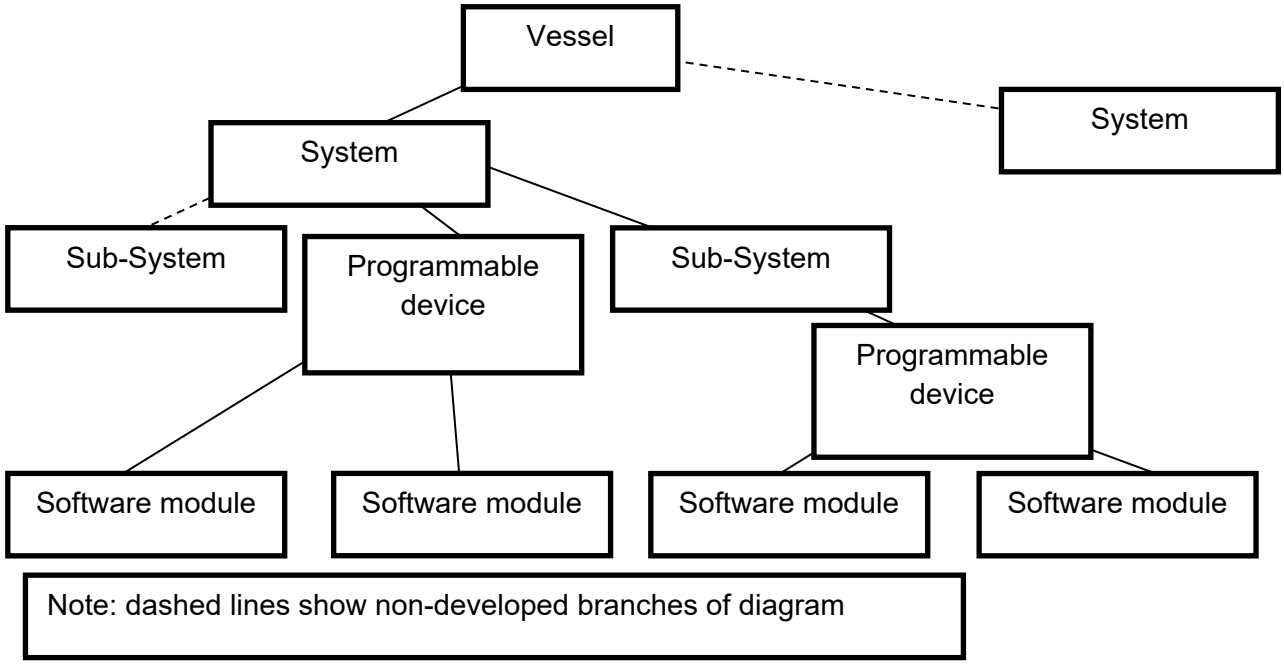


Figure 1 - Illustrative System Hierarchy

E22
(cont)

2 Approval of system and components

2.1 System certification

Computer-based systems that are necessary to accomplish vessel-functions of category II or category III (as defined in paragraph 3.1 below) shall be delivered with a vessel-specific Society certificate. The objective of the vessel-specific system certification is to confirm that design and manufacturing of the system has been completed and that the system complies with applicable rules of the classification Society.

Vessel-specific system certification consist of two main verification activities:

1) Assessment of vessel-specific documentation
(see paragraph 4.2 and paragraph 6)

2) Survey and testing of the system to be delivered to the vessel (see paragraph 4.2.7)

The classification Society may accept Alternative Certification Scheme (ACS) provided that the requirements are met, and that the system is provided with a vessel-specific certificate.

2.2 Type approval of computer-based systems
Computer-based systems that are routinely manufactured and include standardized software functions may be type approved in accordance with specified rules of the classification Society. Hardware shall be documented according to the requirement in paragraph 4.2.4.

The type approval consist of two main verification activities:

1) Assessment of type-specific documentation

2) Survey and testing of the standardized functions

Type approval will normally not yield exemption from vessel-specific system certification since vessel-specific functions, parameter configurations and installation elements demand vessel-specific verification.

3 System categories

3.1 System category definitions

The categorization of a system in the context of this UR is based on the potential severity of the consequences if the system serving the function fails. Table 3 provides the definitions of the categories.

Table 3 System categories

Category:	Failure effects:	Typical System functionality:
I	Those systems, failure of which will not lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment.	- Monitoring, informational and administrative functions

E22
(cont)

II	Those systems, failure of which could eventually lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment.	- Vessel alarm, monitoring and control functions which are necessary to maintain the vessel in its normal operational and habitable conditions
III	Those systems, failure of which could immediately lead to dangerous or catastrophic situations for human safety, safety of the vessel and/or threat to the environment.	- Control functions for maintaining the vessel's propulsion and steering - Vessel safety functions

3.2 Class Societies' scope

Category I systems are normally not subject to verification by the Class society, as failure of these systems shall not lead to dangerous situations. However, information pertinent to category I systems shall be required upon request to determine the correct category or ensure that they do not influence the operation of systems in category II and category III.

3.3 System category examples

The category of a system shall always be evaluated in the context of the specific vessel in question; thus, the categorization of a system may vary from one vessel to the next. This means that the examples of categories below are given as guidance only. For determining the categorization of systems for a specific vessel, see paragraph 4.3.3.

Examples of category I systems:
Fuel monitoring system, maintenance support system, diagnostics and troubleshooting system, closed circuit television, cabin security, entertainment system, fish detection system.

Examples of category II systems:
Fuel oil treatment system, alarm monitoring and safety systems for propulsion and auxiliary machinery, Inert gas system, control, monitoring and safety system for cargo containment system.

Examples of category III systems:
Propulsion control system, steering gear control system, electric power system (including power management system), dynamic positioning system (IMO classes 2 and 3).

The list of example systems is not exhaustive.

4 Requirements on development and certification of computer-based system

4.1 General requirement

4.1.1 Life cycle approach with appropriate standards

Requirement:
A global top-down approach shall be undertaken in the design and development of both hardware and software and the integration in sub-systems, systems, and system of systems, spanning the complete system lifecycle. This approach shall be based on the standards as listed herein or other standards recognized by the Class Society.

E22 (cont)

Class Society's verification:
This is verified by the Class Society as a part of the quality management system verification described in paragraph 4.1.2

4.1.2 Quality management system

Systems integrators and system suppliers shall, in the development of computer-based systems for category II and category III, comply to a recognised quality standard such as ISO 9001; also incorporating principles of IEC/ISO 90003.
The quality management system shall as a minimum include the following topics, applicable for both category II and category III systems:

Table 4 Quality management system

Area		Role	
#	**Topic**	**System supplier**	**Systems integrator**
1	Responsibilities and competency of the staff.	x	x
2	The complete lifecycle of delivered software and of associated hardware	x	x
3	Specific procedure for unique identification of a computer-based system, it's components and versions.	x	
4	Creation and update of the vessel's system architecture		x
5	Organization set in place for acquisition of software and related hardware from suppliers	x	x
6	Organization set in place for software code writing and verification	x	
7	Organization set in place for system validation before integration in the vessel	x	
8	Specific procedure for conducting and approving of systems at FAT and SAT	x	x
9	Creation and update of system documentation	x	
10	Specific procedure for software modification and installation on board the vessel, including interactions with shipyard and owner	x	x
11	Specific procedures for verification of software code	x	
12	Procedures for integrating systems with other systems and testing of the system of systems for the vessel	x	x
13	Procedures for managing changes to software and configurations before FAT	x	
14	Procedures for managing and documenting changes to software and configurations after FAT	x	x
15	Checkpoints for the organization's own follow-up of adherence to the quality management system	x	x

Class Society's verification:
The quality management system may be verified by two alternative means:

E22 (cont)

1) The Class Society confirming that the quality management system is certified as compliant to a recognized standard by an organisation with accreditation under a national accreditation scheme.

2) The Class Society confirming compliance to a standard through a specific assessment of the quality management system. The documentation requirements will be defined per case.

4.2 Requirements on the system supplier

4.2.1 Define and follow a quality plan

Requirement:
The system supplier shall document that the quality management system is applied for the design, construction, delivery, and maintenance of the specific system to be delivered.
All applicable items described in paragraph 4.1.2 (for the system supplier role) shall be demonstrated to exist and being followed, as relevant.

Class Society's verification:
Category I: No documentation required
Category II and III: The quality plan shall be available during survey (FAT) or submitted for information upon request (FI).

4.2.2 Unique identification of systems and software

Requirement:
A method for unique identification of a system, its different software components and different revisions of the same software component shall be applied.
The method shall be applied throughout the lifecycle of the system and the software.

See also paragraph 7.1 for related technical requirements on the system in question.
The documentation of the method is typically a part of the quality management system, see paragraph 4.1.2

Class Society's verification:
Category I: Not required
Category II and III: Application of the identification system is verified as a part of the FAT (paragraph 4.2.7) and SAT (paragraph 4.3.6)

4.2.3 System description

Requirement:
The system's specification and design shall be determined and documented in a system description. In addition to serve as a specification for the detailed design and implementation, the purpose of the system description is to document that the entire system-delivery is according to the specifications and in compliance with applicable rules and regulations.

The system description shall contain information of the following:

- Purpose and main functions, including any safety aspects
- System category as defined

E22 (cont)

- Key performance characteristics
- Compliance with the technical requirements and Class Society rules
- User interfaces/mimics
- Communication and Interface aspects
    - Identification and description of interfaces to other vessel systems
- Hardware-arrangement related aspects:
    - Network-architecture/topology, including all network components like switches, routers, gateways, firewalls etc.
    - Internal structure with regards to all interfaces and hardware nodes in the system (e.g. operator stations, displays, computers, programmable devices, sensors, actuators, I/O modules etc)
    - I/O allocation (mapping of field devices to channel, communication link, hardware unit, logic function)
    - Power supply arrangement
    - Failure mode description

Guidance:
The information listed above is in this UR collectively referred to as the system description. It may however be divided into a number of different documents and models.

Class Society's verification:
Category I: The system description documentation shall upon request be submitted for information (FI).
Category II and III: The system description documentation shall be submitted for approval (AP).

4.2.4 Environmental compliance of hardware components

Requirement:
Evidence of environmental type testing according to IACS UR E10 regarding hardware elements included in the system and sub-systems shall be submitted to the Class Society.

Class Society's verification:
Category I: This requirement is not mandatory for category I systems. Reference to Type approval certificate or other evidence of type testing shall upon request be submitted for information (FI) see paragraph 3.2.
Category II and III: Reference to Type approval certificate or other evidence of type testing shall be submitted for information (FI).

4.2.5 Software code creation, parameterization, and testing

Requirement:
The software created, changed, or configured for the delivery project shall be developed and have the quality assurance activities assessed according to the selected standard(s) as described in the quality plan.

E22 (cont)

The quality assurance activities may be performed on several levels of the software-structure and shall include both custom-made software and configured components (e.g. software libraries) as appropriate.
The verification of the software shall as a minimum verify the following aspects based on black-box methods:

- Correctness, completeness and consistency of any parameterization and configuration of software components
- Intended functionality
- Intended robustness

For components in systems of Category II and III, the scope, purpose, and results of all performed reviews, analyses, tests, and other verification activities shall be documented in test reports.

Guidance:
Some of the methods utilized in this activity are sometimes referred to as “software unit test” or “developer test” and may also include verification methods like code-reviews and static- or dynamic code analysis.

Class Society’s verification:
Category I: No documentation required
Category II and III: Software test reports shall upon request be submitted for information (FI).

4.2.6 Internal system testing before FAT

Requirement:
The system shall as far as practicable be tested before the FAT. The main purpose of the system test is for the system supplier to verify that the entire system delivery is according to the specifications, approved documentation and in compliance with applicable rules and regulations; and further, that the system is completed and ready for the FAT.

The testing shall at least verify the following aspects of the system:

- Functionality
- Effect of faults and failures (including diagnostic functions, detection, alerts response)
- Performance
- Integration between software and hardware components
- Human-machine interfaces
- Interfaces to other systems

Faults are to be simulated as realistically as possible to demonstrate appropriate system fault detection and system response.
Some of the testing may be performed by utilizing simulators and replica hardware.

E22 (cont)

The test-environment shall be documented, including a description of any simulators, emulators, test-stubs, test-management tools, or other tools affecting the test environment and its limitations.
Test cases and test results shall be documented in test programs and test reports respectively.

Class Society's verification:
Category I: No documentation required
Category II and III: Internal system test report shall be made available during FAT or submitted upon request (FI)

4.2.7 Factory acceptance testing (FAT) before installation on board

Requirement:
A factory acceptance test (FAT) shall be arranged for the system in question. The main purpose of the FAT is to demonstrate to the Class Society that the system is completed and compliant with applicable classification rules, thus enabling issuance of a Society Certificate for the system.

The FAT test program shall cover a representative selection of the test items from the internal system test (described in paragraph 4.2.6), including normal system functionality and response to failures.

For category II and III systems, network testing to verify the network resilience requirements in paragraph 7.2.1 shall be performed. If agreed by all parties, the network testing may be performed as a part of the system test onboard the vessel.

The FAT shall as a rule be performed with the project specific software operating on the actual hardware components to be installed on board, with necessary means for simulation of functions and failure responses, however other solutions such as replica hardware or simulated hardware (emulators) may be agreed with the Class Society.

For each test-case it shall be noted if the test passed or failed, and the test-results shall be documented in a test report. The test report shall also contain a list of the software (including software versions) that were installed in the system when the test was executed.

Guidance:
For complex systems there may be a large difference in scope between the "Internal system testing before FAT" activity and the FAT, while for some systems the scope may be identical.

Class Society's verification:
Category I: FAT not required.
Category II and III: The FAT program shall be approved (AP) before the test is executed.
The FAT execution shall be witnessed by the Class Society.
The FAT report shall be submitted for information (FI).

Additional FAT documentation including e.g., user manuals and internal system test report shall be made available during FAT or submitted upon request for information (FI).

4.2.8 Secure and controlled software installation on the vessel

Requirement:

E22 (cont)

The initial installation and subsequent updates of the software components of the system shall be done according to a management of change procedure which has been agreed between the system supplier and the systems integrator.

The management of change procedure shall comply with the requirements in paragraph 6. Cyber security measures shall be observed as described in relevant IACS URs.

Class Society's verification:
Category I: Not required
Category II and III: The management of change procedure shall upon request be submitted for information (FI).

4.3 Requirements on the systems integrator

4.3.1 Responsibilities

For the purposes of this UR, the Shipyard is considered as the systems integrator in the development and delivery phase unless another organization or person is explicitly appointed by the Shipyard.

4.3.2 Define and follow a quality plan

Requirement:
The systems integrator shall document that the quality management system is applied for the installation, integration, completion, and maintenance of the systems to be installed on board. All applicable items described in paragraph 4.1.2 (for the systems integrator role) shall be demonstrated to exist and being followed, as relevant.

Class Society's verification:
Category I: No documentation required
Category II and III: The quality plan shall be made available during survey (at SAT/SOST) or upon request submitted for information (FI).

4.3.3 Determining the category of the system in question

Requirement:
For each system delivery to a particular vessel, it shall be decided which category the system falls under based on the failure effects of the system (as defined in paragraph 3). The category for a specific system must be conveyed to the relevant system supplier. The Class Society may decide that a risk-assessment is needed to verify the proper system category.

Class Society's verification:
Category I, II and III: The category for the different systems shall upon request be documented and submitted for approval (AP).

4.3.4 Risk assessment of the system

Requirement:
If requested by the Class Society, a risk assessment of a specific system in context of the specific vessel in question shall be performed and documented in order to determine the applicable category for the system.

Guidance:

E22 (cont)

IEC/ISO31010 “Risk management - Risk assessment techniques” may be used as guidance in order to determine method of risk assessment.

Class Society’s verification:
Category I, II and III: The risk assessment report shall upon request be submitted for approval (AP).

4.3.5 Define the vessel’s system-architecture

Requirement:
The system of systems (SoS) shall be specified and documented. This architecture specification provides the basis for category determination and development of the different integrated systems by allocating functionality to individual systems and by identifying the main interfaces between the systems. It shall also serve as a basis for the testing of the integrated systems on the vessel level (see paragraph 4.3.7).

The vessel’s system architecture shall at least contain description of:

- Overview of the total systems architecture (the system of systems)
- Each system’s purpose and main functionality
- Communication and interface aspects between different systems

Guidance:
See also UR E26 for diagram of security zones and conduits

Class Society’s verification:
Category I, II, and III: The vessel’s system architecture shall upon request be submitted for information (FI).

4.3.6 System acceptance test (SAT) onboard the vessel

Requirement:
A system acceptance test shall be arranged onboard the vessel. The main purpose of the system acceptance test (SAT) is to verify the system functionality, after installation and integration with the applicable machinery/electrical/process systems on board including possible interfaces with other control and monitoring systems.

For each test-case it shall be noted if the test passed or failed, and the test-results shall be documented in a test report. The test report shall also contain a list of the software (including software versions) that were installed in the system when the test was executed.

Class Society’s verification:
Category I: Not required.
Category II and III: The SAT program shall be submitted for approval (AP) before the test is executed.

The SAT execution shall be witnessed by the Class Society.
The SAT report shall be submitted for information (FI).

E22 (cont)

4.3.7 Testing of integrated systems on vessel-level (SOST)

Requirement:
Integration tests shall be conducted after installation and integration of the different systems in its final environment on board. The purpose of the tests is to verify the functionality of the complete installation (system of systems) including all interfaces and inter-dependencies in compliance with requirements and specifications.

The testing shall at least verify the following aspects of the system of systems:

- The overall functionality of the interacting systems as a whole
- Failure response between systems
- Performance
- Human-machine interfaces
- Interfaces between the different systems

Guidance:
For complex systems there may be a large difference in scope between the “System acceptance test (SAT) onboard the vessel” activity and the SOST, while for some systems the scope may be overlapping or identical. It is possible to combine the two activities into one when the test scope is similar.

Class Society’s verification:
Category I: Not required.
Category II and III: The SOST program shall submitted for approval (AP) before the test is executed.

The SOST execution shall be witnessed by the Class Society.
The SOST report shall be submitted for information (FI).

4.3.8 Change management

The systems integrator shall follow procedures for management of change to the system as described in paragraph 6 .

Class Society’s verification:
Category I: No documentation requirements
Category II and III: The management of change procedure shall upon request be submitted for information (FI).

5 Requirements on maintenance of computer-based systems

5.1 Requirements on the Vessel Owner

5.1.1 Responsibilities

For the purposes of this UR, the vessel owner is considered to be the systems integrator in the operations phase unless another organization or person is explicitly appointed by the owner.

E22 (cont)

Accordingly, the Class Society shall in a timely manner be informed by the owner about the appointed systems integrator which is responsible for implementing any changes to the systems in conjunction with system supplier(s).

5.2 Requirements on the Systems integrator

5.2.1 Change management

Requirement:
The systems integrator shall ensure that necessary procedures for software and hardware change management exist on board, and that any software modification/upgrade are performed according to the procedure(s). For details about change management please see paragraph 6 .

Changes to computer-based systems in the operational phase shall be recorded.
The records shall contain information about the relevant software versions and other relevant information as described in paragraph 6.1.1.

Class Society's verification:
Category I: No documentation requirements
Category II and III: See paragraph 6.12.

5.3 Requirements on the System Supplier

5.3.1 Change management

Requirement:
The system supplier shall follow procedures for maintenance of the system including procedures for management of change as described in paragraph 6.

Class Society's verification:
Category I: No documentation requirements
Category II and III: See paragraph 6.12.

5.3.2 Testing of changes before installation onboard

Requirement:
The system supplier shall make sure that the planned changes to a system have passed relevant in-house tests before the change is made to systems on board.

Class Society's verification:
Category I: No documentation requirements
Category II and III: See paragraph 6.12.

6 Management of change

6.1 General

Paragraph 6 provides requirements for the management of change throughout the lifecycle of a computer-based system. Different procedures for the management of change may be defined for specific phases in a system's lifecycle as the different phases typically involve different stakeholders. The Class Society's verification is described in paragraph 6.12.

E22 (cont)

6.2 Documented change management procedures

Requirement:
The organization in question shall have defined and documented change management procedures applicable for the computer-based system in question covering both hardware and software. After FAT, the system supplier shall manage all changes to the system in accordance with the procedure. Examples could be qualification of new versions of acquired software, new hardware, modified control logic, changes to configurable parameters.

The procedure(s) shall at least describe the activities listed in paragraphs 6.3 through 6.11. The outcome of the impact analysis in 6.8 will determine to what extent the activities in 6.3 to 6.12 shall be performed. Change records (described in paragraph 6.11) shall always be produced.

6.3 Agreement between relevant stakeholders

Requirement:
The management of change process shall be coordinated and agreed between the relevant stakeholders along the different stages of the lifecycle of the computer-based system.

Guidance:
Typically, the management of change address at least three different stages:

1) Development and internal verification before FAT; involving the system supplier and sub-suppliers.
2) From FAT to handover of the vessel to the owner; involving the system supplier, the systems integrator, the Class Society, and the owner.
3) In operation; involving the system supplier, service suppliers, the owner, and the Class Society

6.4 Approved software shall be under change management

Requirement:
If changes are required to a system after it has been approved by applicable stakeholders (typically the systems integrator and the Class Society at FAT) the modifications shall follow defined change management procedures.

6.5 Unique identification of system and software versions

Requirement:
The system supplier shall make sure that each system and software version is uniquely identifiable, see paragraph 4.2.2.

6.6 Handling of software master files

Requirement:
There shall be defined mechanisms for handling of the files that constitutes the master-files for a software component. Personnel authorities shall be clearly defined along with the tools and mechanisms used to ensure the integrity of the master files.

6.7 Backup and restoration of onboard software

Requirement:

E22 (cont)

It shall be clearly defined how to perform backup and restoration of the software components of a computer-based system onboard the vessel.

6.8 Impact analysis before change is made

Requirement:
Before a change to the system is made, an impact analysis shall be performed in order to:

- Determine the criticality of the change.
- Determine the impact on existing documentation.
- Determine the needed verification and test activities.
- Determine the need to inform other stakeholders about the change.
- Determine the need to obtain approval from other stakeholders (e.g. Class Society and or Owner) before the change is made.

6.9 Roll-back in case of failed software changes

Requirement:
When maintenance includes installation of new versions of the software in the system, it shall be possible to perform a rollback of the software to the previous installed version with the purpose of returning the system to a known, stable state.

Roll-backs shall be documented and analysed to find and eliminate the root cause.

6.10 Verification and validation of system changes

Requirement:
To the largest degree practically possible, modifications shall be verified before being installed onboard.

After installation, the modification(s) shall be verified onboard according to a documented verification program containing:

- Verification that the new functionalities and/or improvements have had the intended effect.
- Regression test to verify that the modification has not had any negative effects on functionality or capabilities that was not expected to be affected.

6.11 Change records

Changes to systems and software shall be documented in change records to allow for visibility and traceability of the changes. The change records shall contain at least the following items:

- The purpose for a change
- A description of the changes and modifications

E22 (cont)

- The main conclusions from the impact analysis (see paragraph 6.8)
- The identity and version of any new system or software version(s) (see paragraph 6.5)
- Test reports or tests summaries (see paragraph 6.10)

Documentation of the changes to software may be recorded in the planned maintenance system (PMS), in a software registry or equivalent.

6.12 Verification of change management by the Class Society

6.12.1 In operation (vessel in service) phase

The verification by the Class Society regarding the management of change in operation is generally performed during the annual survey of the vessel. Procedures for management of change and relevant change records (see paragraph 6.11) shall be made available at the time of survey.

In the cases where the change requires approval from the Class Society up front, the relevant procedures and documentation for the change in question may be verified at that time.

6.12.2 During newbuilding

The verification of management of change in the newbuilding phase is divided into two; Procedures are verified as a part of the verification of the quality management system (paragraph 4.1.2), while project specific implementation of the procedures are verified during FAT (4.2.7) and after FAT (6.12.1)

7 Technical requirements on computer-based systems

The paragraphs below contain technical requirements on computer-based systems. The compliance to these requirements shall be documented in the design documentation (see paragraph 4.2.3) and verified through the verification activities described in this UR.

7.1 Reporting of system and software identification and version

7.1.1 System identification

The system shall provide means to identify its name, version, identifier, and manufacturer. It is recommended that the system can automatically report the status of its software to a ship software logging system (SSLS) as specified in the international standard ISO 24060.

7.2 Data links

7.2.1 General requirements for category II and III systems

Loss of a data link shall be specifically addressed in risk assessment analysis/FMEA. See paragraph 4.2.3.

1) A single failure in data link shall not cause loss of vessel- functions of category III. Any effect of such failures shall meet the principle of fail-to-safe for the vessel-function(s) being served.

E22 (cont)

2) For vessel-functions of category II and III, any loss of functionality in the remote control system shall be compensated for by local/manual means.

3) The data link shall have means to prevent or cope with excessive communication rates.

4) Data links shall be self-checking, detecting failures or performance issues on the link itself and data communication failures on nodes connected to the link

5) Detected failures shall initiate an alarm.

7.2.2 Specific requirements for wireless data links

1) Category III systems shall not use wireless data links unless specifically considered by the Class Society on the basis of an engineering analysis carried out in accordance with an International or National Standard acceptable to the Society.

Other categories of systems may use wireless data links with the following requirements:

2) Recognised international wireless communication system protocols shall be employed, incorporating:

a. Message integrity. Fault prevention, detection, diagnosis, and correction so that the received message is not corrupted or altered when compared to the transmitted message.

b. Configuration and device authentication. Shall only permit connection of devices that are included in the system design.

c. Message encryption. Protection of the confidentiality and or criticality of the data content.

d. Security management. Protection of network assets, prevention of unauthorized access to network assets.

3) The internal wireless system within the vessel shall comply with the radio frequency and power level requirements of International Telecommunication Union and flag state requirements.

4) Consideration should be given to system operation in the event of port state and local regulations that pertain to the use of radio-frequency transmission prohibiting the operation of a wireless data communication link due to frequency and power level restrictions.

5) For wireless data communication equipment, tests during harbour and sea trials are to be conducted to demonstrate that radio-frequency transmission does not cause failure of any equipment and does not self-fail as a result of electromagnetic interference during expected operating conditions.

7.3 Verification of technical requirements by the Class Society

E22
(cont)

The implementation of the technical requirements provided in paragraph 7 is verified by the Class Society as part of the system description (paragraph 4.2.3), FAT (paragraph 4.2.7) and SAT (paragraph 4.3.6) described above.

E22 (cont)

Annex A: Summary of documentation submittal

Table 5 and Table 6 below summarise the documentation to be submitted to the Class Society.

Table 5 Summary of documentation submittal by the system supplier

Item		Responsible role	System category		
Paragraph reference	Document		Cat I	Cat II	Cat III
4.2.1	Quality plan	System supplier	-	FI on req.	FI on req.
4.2.3	System description	System supplier	FI on req.	AP	AP
4.2.4	Environmental compliance	System supplier	FI on req.	FI	FI
4.2.5	Software test reports	System supplier	-	FI on req.	FI on req.
4.2.6	System test report	System supplier	-	FI on req.	FI on req.
4.2.7	FAT program	System supplier	-	AP	AP
4.2.7	FAT report	System supplier	-	FI	FI
4.2.7	Additional FAT docs. (e.g. user manual, etc)	System supplier	-	FI on req.	FI on req.
4.2.8	Management of change procedure	System supplier	-	FI on req.	FI on req.

Legend: AP = Approval, FI = For Information, "-" = No requirement, on req. = Upon request from the Class Society

E22
(cont)

Table 6 Summary of documentation submittal by the systems integrator

Item		Responsible role	System category		
Paragraph reference	Document		Cat I	Cat II	Cat III
4.3.2	Quality plan	Systems integrator	-	FI on req.	FI on req.
4.3.3	List of system categorizations	Systems integrator	AP on req.	AP on req.	AP on req.
4.3.4	Risk assessment report	Systems integrator	AP on req.	AP on req.	AP on req.
4.3.5	Vessel's system architecture	Systems integrator	FI on req.	FI on req.	FI on req.
4.3.6	SAT program	Systems integrator	-	AP	AP
4.3.6	SAT report	Systems integrator	-	FI	FI
4.3.7	SOST program	Systems integrator	-	AP	AP
4.3.7	SOST report	Systems integrator	-	FI	FI
4.3.8	Change management procedure for software	Systems integrator	-	FI on req.	FI on req.

Legend: AP = Approval, FI = For Information, "-" = No requirement, on req. = Upon request from the Class Society

E22 (cont)

Annex B: Summary of test witnessing and survey

Table 7 below summarises the activities that shall be witnessed or surveyed by the Class Society.

The responsible role shall facilitate the activity.

Table 7 Summary of test witnessing and survey

Item		Responsible role	System category		
Paragraph reference	Activity		Cat I	Cat II	Cat III
4.2.7	FAT witnessing	System Supplier	-	x	x
4.3.6	SAT witnessing	Systems integrator	-	x	x
4.3.7	SOST witnessing	Systems integrator	-	x	x
6.12	Verification of changes	Systems integrator	-	x	x

Legend: “x” = Witnessing required, “-“ = Witnessing not required

End of Document

E23 (Feb 2007) Selection of low voltage circuit breakers on the basis of their short circuit capacity and co-ordination in service

Deleted Mar 2011

End of Document

E24 Harmonic Distortion for Ship Electrical Distribution System including Harmonic Filters

(June 2016)
(Rev.1
Dec 2018)

1. Scope

The requirements of this UR apply to ships where harmonic filters are installed on main busbars of electrical distribution system, other than those installed for single application frequency drives such as pump motors.

2. General

The total harmonic distortion (THD) of electrical distribution systems is not to exceed 8%.

This limit may be exceeded where all installed equipment and systems have been designed for a higher specified limit and this relaxation on limits is documented (harmonic distortion calculation report) and made available on board as a reference for the surveyor at each periodical survey.

3. Monitoring of harmonic distortion levels for a ship including harmonic filters

3.1 The ships are to be fitted with facilities to continuously monitor the levels of harmonic distortion experienced on the main busbar as well as alerting the crew should the level of harmonic distortion exceed the acceptable limits. Where the engine room is provided with automation systems, this reading should be logged electronically, otherwise it is to be recorded in the engine log book for future inspection by the surveyor.

Note:

1. This UR, except for Section 3.2, is to be uniformly implemented by IACS Societies:
   i. for ships contracted for construction on or after 1 July 2017 or
   ii. for ships where an application for a periodical or occasional machinery survey after the retrofit of harmonic filters is dated on or after 1 July 2017.

2. Section 3.2 is to be uniformly implemented by IACS Societies for ships contracted for construction before 1 July 2017, at any scheduled Machinery periodical survey having a due date on or after 1 July 2017.

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

4. UR E24 Rev.1, except for Section 3.2, is to be uniformly implemented by IACS Societies:
   i. for ships contracted for construction on or after 1 January 2020 or
   ii. for ships where an application for a periodical or occasional machinery survey after the retrofit of harmonic filters is dated on or after 1 January 2020.

E24 (cont)

3.2 As a minimum, harmonic distortion levels of main busbar on board such existing ships are to be measured annually under seagoing conditions as close to the periodical machinery survey as possible so as to give a clear representation of the condition of the entire plant to the surveyor. Harmonic distortion readings are to be carried out when the greatest amount of distortion is indicated by the measuring equipment. An entry showing which equipment was running and/or filters in service is to be recorded in the log so this can be replicated for the next periodical survey. Harmonic distortion levels are also to be measured following any modification to the ship's electrical distribution system or associated consumers by suitably trained ship's personnel or from a qualified outside source.

Records of all the above measurements are to be made available to the surveyor at each periodical survey.

4. Mitigation of the effects of harmonic filter failure on a ship's operation

Where the electrical distribution system on board a ship includes harmonic filters the system integrator of the distribution system is to show, by calculation, the effect of a failure of a harmonic filter on the level of harmonic distortion experienced.

The system integrator of the distribution system is to provide the ship owner with guidance documenting permitted modes of operation of the electrical distribution system while maintaining harmonic distortion levels within acceptable limits during normal operation as well as following the failure of any combination of harmonic filters.

The calculation results and validity of the guidance provided are to be verified by the surveyor during sea trials.

5. Protection arrangements for harmonic filters

Arrangements are to be provided to alert the crew in the event of activation of the protection of a harmonic filter circuit.

A harmonic filter should be arranged as a three phase unit with individual protection of each phase. The activation of the protection arrangement in a single phase shall result in automatic disconnection of the complete filter. Additionally, there shall be installed a current unbalance detection system independent of the overcurrent protection alerting the crew in case of current unbalance.

Consideration is to be given to additional protection for the individual capacitor element as e.g. relief valve or overpressure disconnector in order to protect against damage from rupturing. This consideration should take into account the type of capacitors used.

End of Document

E25 Failure detection and response of all types of steering gear control systems

(June 2016)
(Rev.1
Dec 2019)
(Rev.2
Mar 2022)

1. Application

1.1 This UR applies to Steering Gear Control System as defined in UR M42 Appendix 1 Item 1.

2. Failure detection

2.1 The most probable failures that may cause reduced or erroneous system performance shall be automatically detected and at least the following failure scenarios shall be considered:

(a) Power supply failure

(b) Earth fault on AC and DC circuits

(c) Loop failures in closed loop systems, both command and feedback loops (normally short circuit, broken connections and earth faults)

(d) Data communication errors

(e) Programmable system failures (Hardware and software failures)

(f) Deviation between rudder order and feedback*

* Deviation alarm shall be initiated if the rudder's actual position does not reach the set point within acceptable time limits for the closed loop control systems (e.g. follow-up control and autopilot). Deviation alarm may be caused by mechanical, hydraulic or electrical failures.

2.2 All failures detected shall initiate audible and individual visual alarm on the navigation bridge.

Note:

1. This UR is to be uniformly implemented by IACS Societies on ships contracted for construction (as defined in IACS PR29) on or after 1 July 2017.

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

3. Rev.1 of this UR is to be uniformly implemented by IACS Societies on ships contracted for construction on or after 1 January 2021.

4. Rev.2 of this UR is to be uniformly implemented by IACS Societies on ships contracted for construction on or after 1 July 2023.

E25
(cont)

3. System response upon failure

3.1 The failures (as defined but not limited to those in 2.1) likely to cause uncontrolled movements of rudder are to be clearly identified. In the event of detection of such failure, the rudder is to stop in the current position without manual intervention or, subject to the discretion of the Classification Society, is to return to the midship/neutral position. For mechanical failures such as sticking valves and failure of static components (pipes, cylinders), the system response without manual intervention is not mandatory, and the operator can follow instructions on the signboard in case of such failures, in accordance with UR M42.13.

Note: For hydraulic locking failure, refer also to UR M42.12.2 and 42.13.

End of document

E26 Cyber resilience of ships

(Apr 2022)

1. Introduction

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

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

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

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

1.1 Structure of this UR

Table 1: Structure of this UR

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

Note:

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

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

E26
(cont)

1.2 Aim and purpose

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

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

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

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

1.3 Scope of applicability

This UR applies to:

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

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

- Propulsion
- Steering
- Anchoring and mooring
- Electrical power generation and distribution
- Fire detection and extinguishing systems
- Cargo handling system (limited to safety-related elements)
- Bilge and ballast systems, loading/unloading control systems, loading computer
- Boiler control system
- Scrubber control system and other systems needed for compliance with class or international regulations to prevent pollution to the environment
- Watertight integrity and flooding detection
- Lighting (e.g. emergency lighting, low locations, navigation lights, etc.)
- Any other OT system whose disruption or functional impairing may pose risks to ship operations (e.g. LNG monitoring and control system, relevant gas detection system etc.)

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

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

For navigation and radiocommunication systems, standard such as IEC 61162-460 or IEC 63154 can be used as alternatives to this UR, as long as the application of such standards

E26 (cont)

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

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

- passenger or visitor servicing and management systems,
- passenger-facing networks
- administrative networks
- crew welfare systems
- any other systems connected to OT systems, either permanently or temporarily (e.g. during maintenance).

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

1.3.1 System Category

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

1.3.2 IACS Documents on Computer Based Systems and Cyber Resilience

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

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

IACS UR E27 Cyber resilience of on-board systems and equipment includes requirements for cyber resilience for on-board systems and equipment.

IACS Recommendation 166 Recommendation on Cyber Resilience: non-mandatory recommended technical requirements that stakeholders may reference and apply to assist with the delivery of cyber resilient ships, whose resilience can be maintained throughout their service life. IACS Recommendation 166 on Cyber Resilience is intended for ships contracted for construction after its publication and may be used as a reference for ships already in service prior to its publication. For ships to which this UR applies as mandatory instrument, when both this UR and Recommendation 166 are used, should any difference in requirements addressing the same topic be found between the two instruments, the requirements in this UR shall prevail.

E26
(cont)

2. Definitions

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

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

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

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

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

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

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

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

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

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

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

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

1. General

1.1 Introduction

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

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

1.2 Limitations

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

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

1.3 Scope

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

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

Note:

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

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

E27 (cont)

1.3.1 Information and Communication Technology (ICT)

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

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

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

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

1.4 Definitions & Abbreviations

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

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

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

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

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

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

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

E27 (cont)

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

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

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

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

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

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

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

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

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

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

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

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

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

E27
(cont)

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

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

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

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

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

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

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

E27 (cont)

2. Security Philosophy

2.1 Systems and Equipment

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

2.1.2 An Equipment may be one of the following:

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

2.2 Cyber Resilience

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

2.3 Compensating Countermeasures

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

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

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

2.4 Essential Systems Availability

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

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

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

E27 (cont)

3. Documentation

3.1 System Documentation

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

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

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

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

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

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

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

g) Plans for maintenance of system

h) Recovery Plan

i) System Test Plan

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

k) Change Management Plan

3.2 Inventories

3.2.1 The following details shall be documented:

a) Name

b) Brand/Manufacturer (supplier)

c) Model or reference, some devices contain several references

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

E27
(cont)

3.3 Software Inventory

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

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

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

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

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

E27
(cont)

4 System Requirements

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

4.1 Required security capabilities

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

Table 1

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

E27
(cont)

		a) Limit the use of portable and mobile devices only to those permitted by design b) Restrict code and data transfer to/from portable and mobile devices Note: Port limits / blockers (and silicone) could be accepted for a specific system (IEC 62443-3-3/SR 2.3)
11	Mobile code	The CBS shall control the use of mobile code such as java scripts, ActiveX and PDF. (IEC 62443-3-3/SR 2.4)
12	Session lock	The CBS shall be able to prevent further access after a configurable time of inactivity or following activation of manual session lock. (IEC 62443-3-3/SR 2.5)
13	Auditable events	The CBS shall generate audit records relevant to security for at least the following events: access control, operating system events, backup and restore events, configuration changes, loss of communication. (IEC 62443-3-3/SR 2.8)
14	Audit storage capacity	The CBS shall provide the capability to allocate audit record storage capacity according to commonly recognized recommendations for log management. Auditing mechanisms shall be implemented to reduce the likelihood of such capacity being exceeded. (IEC 62443-3-3/SR 2.9)
15	Response to audit processing failures	The CBS shall provide the capability to prevent loss of essential services and functions in the event of an audit processing failure. (IEC 62443-3-3/SR 2.10)
16	Timestamps	The CBS shall timestamp audit records. (IEC 62443-3-3/SR 2.11)
17	Communication integrity	The CBS shall protect the integrity of transmitted information. Note: Cryptographic mechanisms shall be employed for wireless networks. (IEC 62443-3-3/SR 3.1)
18	Malicious code protection	The CBS shall provide capability to implement suitable protection measures to prevent, detect and mitigate the effects due to malicious code or unauthorized software. It shall have the feature for updating the protection mechanisms (IEC 62443-3-3/SR 3.2)
19	Security functionality verification	The CBS shall provide the capability to support verification of the intended operation of security functions and report when anomalies occur during maintenance (IEC 62443-3-3/SR 3.3)
20	Input validation	The CBS shall validate the syntax, length and content of any input data via untrusted networks that is used as process control input or input that directly impacts the action of the CBS. (IEC 62443-3-3/SR 3.5)
21	Deterministic output	The CBS shall provide the capability to set outputs to a predetermined state if normal operation cannot be maintained as a result of an attack. The predetermined state could be: – Unpowered state

E27
(cont)

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

E27 (cont)

4.2 Additional security capabilities

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

Table 2

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

E27
(cont)

5 Product Design and Development Requirements

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

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

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

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

5.2 (IEC 62443-4-1/SUM-2) A process shall be employed to ensure that documentation about product security updates is made available to users (which could be through establishing a cyber security point of contact or periodic publication which can be accessed by the user) that includes but is not limited to:

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

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

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

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

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

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

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

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

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

E27 (cont)

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

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

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

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

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

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

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

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

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

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

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

   iii. setting/changing/deleting its value;

e) Instructions and recommendations for the use of all security-related tools and utilities that support administration, monitoring, incident handling and evaluation of the security of the product;

f) Instructions and recommendations for periodic security maintenance activities;

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

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

E27
(cont)

Annex I

Requirements:

I. IACS UR E10: Test Specification for Type Approval

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

III. IACS UR E26: Cyber Resilience of Ships

Credits:

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

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

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

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

End of Document

E26 (cont)

"Primary Essential Services" and "Secondary Essential Services": Primary Essential Services are those services which need to be in continuous operation to maintain propulsion and steering; Secondary Essential Services are those services which need not necessarily be in continuous operation to maintain propulsion and steering but which are necessary for maintaining the vessel's safety.

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

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

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

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

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

Network segment: A collection of nodes that share the same network address plan. A network segment is a broadcast domain.

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

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

Physical network segment: The same as "Network segment". The physical components are not shared by other network segments.

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

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

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

Ship Designer/Shipyard: The person or organization:

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

E26 (cont)

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

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

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

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

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

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

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

E26
(cont)

3. Goals and organization of requirements

3.1 Primary goal

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

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

3.2 Sub-goals per functional element

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

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

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

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

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

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

3.3 Organization of requirements

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

For each requirement, a rationale is given.

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

E26
(cont)

4. Requirements

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

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

- Shipowner/Company
- Ship Designer/Shipyard
- System Integrator
- Supplier
- Classification Society

4.1 Identify

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

4.1.1 Inventory of CBSs and networks onboard

4.1.1.1 Requirement:

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

4.1.1.2 Rationale:

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

4.1.1.3 Requirement details

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

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

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

E26
(cont)

4.1.1.3.1 Hardware

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

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

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

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

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

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

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

4.1.1.3.2 Software

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

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

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

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

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

4.2 Protect

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

4.2.1 Security Zones

4.2.1.1 Requirement:

All CBSs in the scope of applicability of this UR shall be grouped into security zones with well-defined security control policy and security capabilities. Security zones shall either be isolated (i.e. air gapped) or connected to other security zones or networks by means

E26 (cont)

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

Only explicitly allowed traffic shall traverse a security zone boundary.

4.2.1.2 Rationale:

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

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

4.2.1.3 Requirement details

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

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

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

Navigational and communication systems shall not be in same security zone as machinery or cargo systems.

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

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

It shall be possible to manually isolate a security zone without affecting the primary functionality of the CBSs in the zone.

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

4.2.2 Network protection safeguards

4.2.2.1 Requirement:

Networks connecting CBSs in the scope of applicability of this UR shall be protected by firewalls or equivalent means as specified in section 4.2.1. The networks shall also be protected against the occurrence of excessive data flow rate and other events which could impair the quality of service of network resources.

The CBSs in scope of this UR shall be implemented in accordance with the principle of Least Functionality, i.e. configured to provide only essential capabilities and to prohibit or restrict the

E26
(cont)

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

4.2.2.2 Rationale:

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

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

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

4.2.2.3 Requirement details

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

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

4.2.3.1 Requirement:

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

4.2.3.2 Rationale:

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

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

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

4.2.3.3 Requirement details

Malware protection shall be implemented on CBSs in the scope of applicability of this UR. On CBSs having an operating system for which industrial-standard anti-virus and anti-malware software is available and maintained up-to-date, anti-virus and anti-malware software shall be installed, maintained and regularly updated, unless the installation of such software impairs

E26 (cont)

the ability of CBS to provide the functionality and level of service required (e.g. for Cat.II and Cat.III CBSs performing real-time tasks).

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

4.2.4 Access control

4.2.4.1 Requirement:

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

4.2.4.2 Rationale:

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

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

4.2.4.3 Requirement details

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

4.2.4.3.1 Physical access control

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

4.2.4.3.2 Physical access control for visitors

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

E26
(cont)

4.2.4.3.3 Physical access control of network access points

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

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

4.2.4.3.4 Removable media controls

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

4.2.4.3.5 Management of credentials

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

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

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

4.2.4.3.6 Least privilege policy

Any user, program, or process allowed to access CBS and networks in the scope of applicability of this UR shall have only the bare minimum privileges necessary to perform its function. Processes having access to systems and networks onboard shall operate at privilege levels no higher than necessary to accomplish their intended task.

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

4.2.5 Wireless communication

4.2.5.1 Requirement

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

E26 (cont)

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

4.2.5.2 Rationale

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

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

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

4.2.5.3 Requirement details

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

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

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

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

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

4.2.6 Remote access control and communication with untrusted networks

4.2.6.1 Requirement:

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

4.2.6.2 Rationale:

Onboard CBSs have become increasingly digitalized and connected to the internet to perform a wide variety of legitimate functions. The use of digital systems to monitor and control onboard CBSs makes them vulnerable to cyber incidents. Attackers may attempt to access onboard CBSs through connectivity with the internet and may be able to make changes that affect a CBS's operation or even achieve full control of the CBS, or attempt to download information from the ship’s CBS. In addition, since use of legacy IT and OT systems that are no longer supported and/or rely on obsolete operating systems affects a lot cyber resilience,

E26 (cont)

special care should be put to relevant hardware and software installations on board to help maintain a sufficient level of cyber resilience when such systems can be remotely accessed, also keeping in mind that not all cyber incidents are a result of a deliberate attack.

4.2.6.3 Requirement details

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

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

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

4.2.6.3.1 Design

CBSs in the scope of applicability of this UR shall:

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

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

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

4.2.6.3.2 Additional requirements for remote maintenance

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

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

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

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

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

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

E26 (cont)

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

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

4.2.7 Use of Mobile and Portable Devices

4.2.7.1 Requirement:

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

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

4.2.7.2 Rationale:

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

4.2.7.3 Requirement details

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

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

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

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

4.3 Detect

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

4.3.1 Network operation monitoring

4.3.1.1 Requirement:

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

E26
(cont)

4.3.1.2 Rationale:

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

4.3.1.3 Requirement details

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

- Monitoring and protection against excessive traffic
- Monitoring of network connections
- Monitoring and recording of device management activities
- Monitoring or protection against connection of unauthorized devices

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

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

4.3.2 Diagnostic functions of CBS and networks

4.3.2.1 Requirement:

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

4.3.2.2 Rationale:

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

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

4.3.2.3 Requirement details

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

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

E26
(cont)

4.4 Respond

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

4.4.1 Incident response plan

4.4.1.1 Requirement:

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

4.4.1.2 Rationale:

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

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

4.4.1.3 Requirement details

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

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

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

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

E26 (cont)

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

4.4.2 Local, independent and/or manual operation

4.4.2.1 Requirement:

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

4.4.2.2 Rationale:

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

4.4.2.3 Requirement details

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

If communication to the remote control system or other CBS's is arranged by networks, segmentation and protection safeguards as described in 4.2.1 and 4.2.2 shall be implemented. This implies that the local control and monitoring system shall be considered a separate security zone.

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

4.4.3 Network isolation

4.4.3.1 Requirement:

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

4.4.3.2 Rationale:

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

4.4.3.3 Requirement details

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

E26 (cont)

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

4.4.4 Fallback to a minimal risk condition

4.4.4.1 Requirement:

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

4.4.4.2 Rationale:

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

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

4.4.4.3 Requirement details

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

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

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

The ability of a system to fall back to a minimal risk condition shall be considered from the design phase by the Supplier and the Shipyard / Ship Designer / System Integrator.

4.5 Recover

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

4.5.1 Recovery plan

4.5.1.1 Requirement:

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

E26
(cont)

4.5.1.2 Rationale:

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

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

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

4.5.1.3 Requirement details

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

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

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

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

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

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

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

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

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

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

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

(6) Current configuration information for all components.

E26 (cont)

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

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

4.5.2 Backup and restore capability

4.5.2.1 Requirement:

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

4.5.2.2 Rationale:

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

4.5.2.3 Requirement details

4.5.2.3.1 Restore capability

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

Data shall be restorable from a secure copy or image.

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

4.5.2.3.2 Backup

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

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

4.5.3 Controlled shutdown, reset, roll-back and restart

4.5.3.1 Requirement:

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

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

E26 (cont)

4.5.3.2 Rationale:

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

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

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

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

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

4.5.3.3 Requirement details

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

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

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

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

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

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

E26
(cont)

5. Test Plan for performance evaluation and testing

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

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

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

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

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

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

5.1 During design and construction phases:

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

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

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

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

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

E26 (cont)

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

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

5.2 Upon ship commissioning:

a. The Shipyard and the incoming Shipowner shall together verify that the information contained in the final version of the Test Plan is updated and placed under change management; that it is aligned with the latest configurations of CBSs and networks connecting such systems together onboard the ship and to other CBSs not onboard (e.g., ashore); and that the tests documented in the Test Plan are sufficiently detailed as to allow verification of the installation and operation of measures adopted for the fulfilment of relevant requirements on the final configuration of CBSs and networks onboard.

b. The Shipyard shall document verification tests or assessments of security controls and measures in the fully integrated ship, maintaining change management for configurations, and noting in the documented test results where safety conditions may be affected by specific circumstances or failures addressed in the Test Plan.

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

5.3 During the operational life of the ship:

a. The Shipowner, with the support of Systems Integrator and Suppliers, shall keep the Test Plan up to date and aligned with the CBSs onboard the ship and the networks connecting such systems to each other and to other CBSs not onboard (e.g. ashore). The Shipowner shall update the Test Plan considering the changes occurred on CBSs and networks onboard, possible emerging risks related to such changes, new threats, new vulnerabilities and other possible changes in the ship’s operational environment.

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

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

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

E26
(cont)

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

6.1 Requirement:

A risk assessment shall be carried out in case any of the CBSs falling under the scope of applicability of this UR is excluded from the application of relevant requirements. The risk assessment shall provide evidence of the acceptable risk level associated to the excluded CBSs. A concise list of excluded applications of relevant requirements is to be generated and maintained with the CBS documents onboard the ship (e.g. the execution of test plans and any relevant updated test plans).

6.2 Rationale

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

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

6.3 Requirement details

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

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

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

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

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

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

- Asset vulnerabilities;

E26 (cont)

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

6.4 Acceptance criteria

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

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

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

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

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

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

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

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

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

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

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

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

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

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

E26
(cont)

Appendix – Summary of actions and documents

Legend*

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

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

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

Document	Reference Requirement	Phase	Supplier	Shipyard System Integrator	Shipowner Company	Class
Identify						
Inventory of hardware and software of the CBSs in the scope of applicability of this UR and of the networks connecting such systems to each other and to other CBSs onboard or ashore	Inventory of CBSs and software onboard	**Design**	Provide			Approve
		Construction		Maintain		Info
		Commissioning		Provide		Approve
		Operation			Maintain	
		Survey			Make avail.	Check

E26 (cont)

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

E26 (cont)

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

E26 (cont)

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

E26
(cont)

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

End of document