

E22

(Dec
2006)
(Corr.1
Oct
2007)
(Rev.1
Sept
2010)

Unified Requirements for the On Board Use and Application of Programmable Electronic Systems

1. Scope

These Requirements apply to the use of programmable electronic systems which provide control, alarm, monitoring or safety functions which are subject to classification requirements.

Aids to Navigation and loading instruments are excluded.

Note: For loading instrument / stability computer, REC No. 48 may be considered.

2. Requirements applicable to programmable electronic systems

2.1 General

2.1.1 Programmable electronic systems are to fulfil the requirements of the system under control for all normally anticipated operating conditions, taking into account danger to persons, environmental impact, damage to vessel as well as equipment, usability of programmable electronic systems and operability of non computer devices and systems, etc.

2.1.2 When an alternative design or arrangements deviating from these requirements are proposed, an engineering analysis is required to be carried out in accordance with a relevant International or National Standard acceptable to the Society, see also SOLAS Ch II-1/F, Reg. 55.

Note: As a failure of a category III system may lead to an accident with catastrophic severity, the use of unconventional technology for such applications will only be permitted exceptionally in cases where evidence is presented that demonstrates acceptable and reliable system performance to the satisfaction of the Society.

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.
- 2-3. 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.

E22 (cont)

2.2 System categories

2.2.1 Programmable electronic systems are to be assigned into three system categories as shown in Table I according to the possible extent of the damage caused by a single failure within the programmable electronic systems.

Consideration is to be given to the extent of the damage directly caused by a failure, but not to any consequential damage.

Identical redundancy will not be taken into account for the assignment of a system category.

Table I System categories

Category	Effects	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 function for informational / administrative tasks
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.	- Alarm and monitoring functions - Control functions which are necessary to maintain the ship in its normal operational and habitable conditions
III	Those systems, failure of which could immediately lead to dangerous situations for human safety, safety of the vessel and / or threat to the environment.	- Control functions for maintaining the vessel's propulsion and steering - Safety functions

2.2.2 The assignment of a programmable electronic system to the appropriate system category is to be made according to the greatest likely extent of direct damage. For examples see Table II.

Note: Where independent effective backup or other means of averting danger is provided the system category III may be decreased by one category.

E22 (cont)

Table II Examples of assignment to system categories

System category	Examples
I	Maintenance support systems Information and diagnostic systems
II	Alarm and monitoring equipment Tank capacity measuring equipment Control systems for auxiliary machinery Main propulsion remote control systems Fire detection systems Fire extinguishing systems Bilge systems Governors
III	Machinery protection systems / equipment Burner control systems Electronic fuel injection for diesel engines Control systems for propulsion and steering Synchronising units for switchboards

The examples listed are not exhaustive.

2.3 Data Communication links

2.3.1 These requirements apply to system categories 2 II and 3 III using shared data communication links to transfer data between distributed programmable electronic equipment or systems.

2.3.2 Where a single component failure results in loss of data communication means are to be provided to automatically restore data communication.

2.3.3 Loss of a data communication link is not to affect the ability to operate essential services by alternative means.

2.3.4 Means are to be provided to ~~ensure~~ protect the integrity of data and provide timely recovery of corrupted or invalid data.

2.3.5 The data communication link shall be self-checking, detecting failures on the link itself and data communication failures on nodes connected to the link. Detected failures shall initiate an alarm.

2.3.6 System self-checking capabilities shall be arranged to initiate transition to the least hazardous state for the complete installation in the event of data communication failure.

2.3.7 The characteristics of the data communication link shall be such as to transmit that all necessary information in adequate time and overloading is prevented.

2.4 Additional requirements for wireless data links

2.4.1 These requirements are in addition to the requirements of 2.3.1 to 2.3.7 and apply to system category II using wireless data communication links to transfer data between distributed programmable electronic equipment or systems. For system category III, the use of wireless data communication links is to be in accordance with 2.1.2.

E22
(cont)

2.4.2 Functions that are required to operate continuously to provide essential services dependant on wireless data communication links shall have an alternative means of control that can be brought in action within an acceptable period of time.

2.4.3 Wireless data communication shall employ recognised international wireless communication system protocols that incorporate the following:

- (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 the data content;
- (d) Security management. Protection of network assets, prevention of unauthorised access to network assets.

2.4.4 The wireless system shall comply with the radio frequency and power level requirements of International Telecommunications Union and flag state requirements.

Note: 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.

2.4 2.5 Protection against modification

~~2.4.1~~ 2.5.1 Programmable electronic systems of category II and III are to be protected against program modification by the user.

~~2.4.2~~ 2.5.2 For systems of category III modifications of parameters by the manufacturer are to be approved by the Society.

~~2.4.3~~ 2.5.3 Any modifications made after performance of the tests witnessed by the Society as per item 6 in Table III are to be documented and traceable.

3. Documents to be submitted

3.1 For the evaluation of programmable electronic systems of category II and III, documents according to IEC 60092-504 paragraph 10.11 are to be submitted.

3.2 When alternative design or arrangement is intended to be used, an engineering analysis is to be submitted in addition.

~~3.23~~ 3 For all tests required in accordance to the system category a test plan shall be submitted and the tests shall be documented.

~~3.34~~ Additional documentation may be required for systems of category III. The documentation is to include a description of the methods of test and required test results.

3.5 For wireless data communication equipment, the following additional information shall be submitted:

- (a) Details of manufacturers recommended installation and maintenance practices;

E22 (cont)

- (b) Network plan with arrangement and type of antennas and identification of location;
- (c) Specification of wireless communication system protocols and management functions; see 2.4.3
- (d) Details of radio frequency and power levels;
- (e) Evidence of type testing in accordance with UR E10;
- (f) On-board test schedule, see 7.3.

3.46 ~~Necessary~~ Documents for the evaluation of programmable electronic systems of category I are to be submitted if requested.

3.57 Modifications shall be documented by the manufacturer. Subsequent significant modifications to the software and hardware for system categories II and III are to be submitted for approval.

Note: A significant modification is a modification which influences the functionality and / or safety of the system.

4. Tests and Evidence

4.1 Tests and evidence are to be in accordance with Table III. Definitions and notes relating to Table III are given in Appendix 1.

Table III Tests and evidence according to the system category

M	=	Evidence kept by manufacturer and submitted on request
S	=	Evidence checked by the Society
W	=	To be witnessed by the Society
*	=	The level of witnessing will be determined during the assessment required by 2.1.2

No.	Tests and evidence	System Category		
		I	II	III
1.	Evidence of quality system			
	Quality plan for software		M	M
	Inspection of components (only Hardware) from sub-suppliers		M	M
	Quality control in production		M	M
	Final test reports	M	M	S
	Traceability of software	M	M	S
2.	Hardware and software description			
	Software description		M	S
	Hardware description		M	S
	Failure analysis for safety related functions only			S
3.	Evidence of software testing			
	Evidence of software testing according to quality plan		M	S
	Analysis regarding existence and fulfilment of programming procedures for safety related functions			S

E22
 (cont)

4.	Hardware tests			
	Tests according to <u>Unified Requirement E 10</u>		W	W
5.	Software tests			
	Module tests		M	S
	Subsystem tests		M	S
	System test		M	S
6.	Performance tests			
	Integration test		M	W
	Fault simulation		W	W
	Factory Acceptance Test (FAT)	M	W	W
7.	On-board test			
	Complete system test	M	W	W
	Integration test		W	W
	<u>Operation of wireless equipment to demonstrate electromagnetic compatibility</u>		<u>W</u>	<u>W*</u>
8.	Modifications			
	Tests after modifications	M	S/W	S/W

Appendix 1

E22
(cont)**Definitions and notes relating to Table III, Tests and Evidence****1. Evidence of quality system**

1.1 Quality plan for software

A plan for software lifecycle activities is to be produced which defines relevant procedures, responsibilities and system documentation, including configuration management.

1.2 Inspection of components (only Hardware) from sub-suppliers

Proof that components and / or sub-assemblies conform to specification.

1.3 Quality control in production

Evidence of quality assurance measures on production.

1.4 Final test reports

Reports from testing of the finished product and documentation of the test results.

1.5 Traceability of software

Modification of program contents and data, as well as change of version has to be carried out in accordance with a procedure and is to be documented.

2. Hardware and software description

2.1 Software description

Software is to be described, e.g.

- Description of the basic and communication software installed in each hardware unit
- Description of application software (not program listings)
- Description of functions, performance, constraints and dependencies between modules or other components.

2.2 Hardware description

Hardware is to be described, e.g.

- System block diagram, showing the arrangement, input and output devices and interconnections
- Connection diagrams
- Details of input and output devices
- Details of power supplies

2.3 Failure analysis for safety related functions only (e.g. FMEA)

The analysis is to be carried out using appropriate means, e.g.

- Fault tree analysis

E22
(cont)

- Risk analysis
- FMEA or FMECA

The purpose is to demonstrate that for single failures, systems will fail to safety and that systems in operation will not be lost or degraded beyond acceptable performance criteria when specified by the Society.

3. Evidence of software testing

3.1 Evidence of software testing according to quality plan

Procedures for verification and validation activities are to be established, e.g.

- Methods of testing
- Test programs producing
- Simulation

3.2 Analysis regarding existence and fulfilment of programming procedures for safety related functions

Specific assurance methods are to be planned for verification and validation of satisfaction of requirements, e.g.

- Diverse programs
- Program analysis and testing to detect formal errors and discrepancies to the description
- Simple structure

4. Hardware tests

Tests according Unified Requirement E 10 "Test Specification for Type Approval" will normally be a type approval test.

Special consideration may be given to tests witnessed and approved by another IACS member society.

5. Software tests

5.1 Module tests

Software module tests are to provide evidence that each module performs its intended function and does not perform unintended functions.

5.2 Subsystem tests

Subsystem testing is to verify that modules interact correctly to perform the intended functions and do not perform unintended functions.

5.3 System test

System testing is to verify that subsystems interact correctly to perform the functions in accordance with specified requirements and do not perform unintended functions.

6. Performance tests

6.1 Integration tests

E22
(cont)

Programmable electronic system integration testing is to be carried out using satisfactorily tested system software, and as far as practicable intended system components.

6.2 Fault simulation

Faults are to be simulated as realistically as possible to demonstrate appropriate system fault detection and system response. The results of any required failure analysis are to be observed.

6.3 Factory Acceptance Test (FAT)

Factory acceptance testing is to be carried out in accordance with a test program accepted by the Society. Testing is to be based on demonstrating that the system fulfils the requirements specified by the Society.

7. On-board tests**7.1 Complete system test**

Testing is to be performed on the completed system comprising actual hardware components with the final application software, in accordance with an approved test program.

7.2 Integration tests

On board testing is to verify that correct functionality has been achieved with all systems integrated.

7.3 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 itself fail as a result of electromagnetic interference during expected operating conditions.

Note: Where electromagnetic interference caused by wireless data communication equipment is found to be causing failure of equipment required for Category II or III systems, the layout and / or equipment shall be changed to prevent further failures occurring.

8. Modifications**8.1 Tests after modifications**

Modifications to approved systems are to be notified in advance and carried out to the Society's satisfaction, see paragraph 3.57 of this UR.

End of Document
