E22 Computer-based systems

(Dec 2006) (Corr.1 Oct 2007) (Rev.1 Sept 2010) (Rev.2 June 2016) (Rev.3 June 2023) (Corr.1 Sep 2025)

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 10007:2017 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 0.

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)

The following diagram (Figure 1) shows the hierarchy and relationships of a typical computer-based system.

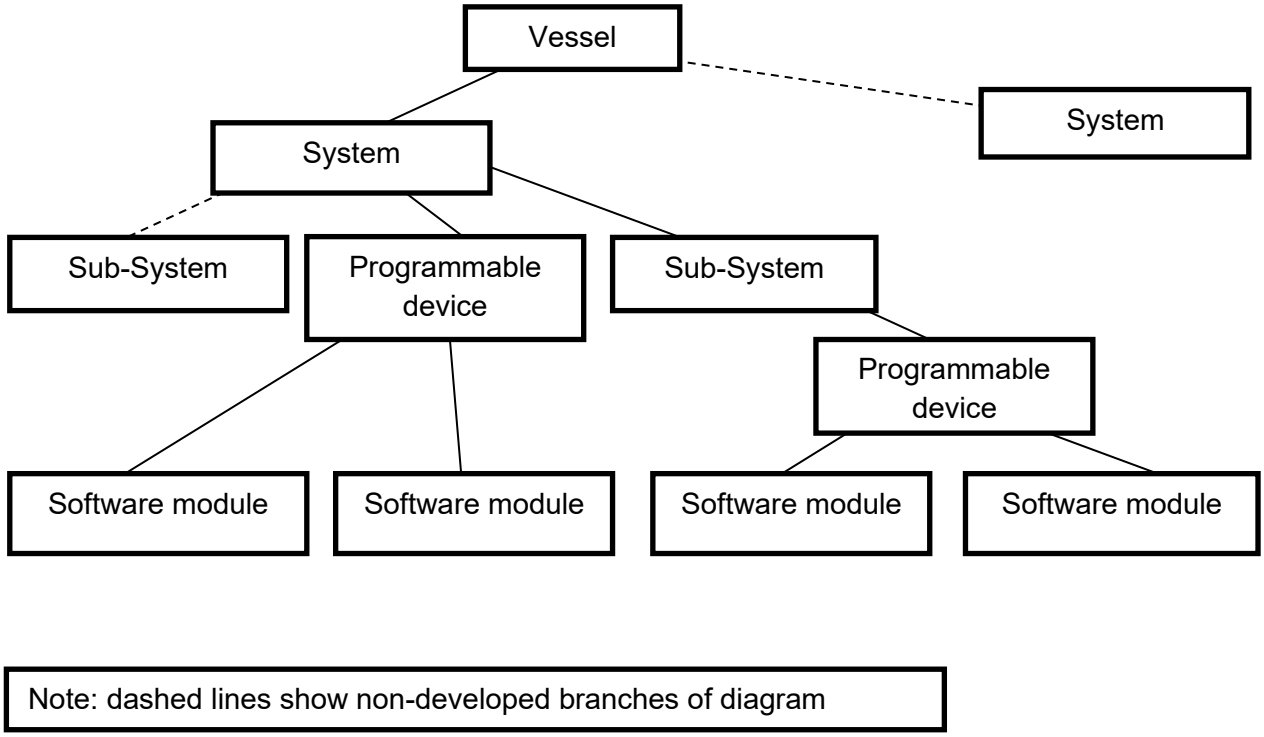


Figure 1 - Illustrative System Hierarchy

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
- Key performance characteristics

E22 (cont)

- 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.

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.

E22 (cont)

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.

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.

E22 (cont)

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 above4.2.6), 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:
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.

E22 (cont)

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:
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).

E22 (cont)

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).

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.

E22 (cont)

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 below.

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.
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

E22 (cont)

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 below.

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 6.11 below6.1.1.

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.

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.

E22 (cont)

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:
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.

E22 (cont)

- 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
- 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

E22 (cont)

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), SAT (4.3.6), and SOST (4.3.7) activities.

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.

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.

E22
(cont)

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

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