Polski Rejestr Statków

RULES

PUBLICATION NO. 9/P

REQUIREMENTS FOR COMPUTER BASED SYSTEMS

2017
July

Publications P (Additional Rule Requirements) issued by Polski Rejestr Statków complete or extend the Rules and are mandatory where applicable.

GDAŃSK

Publication No. 9/P – Requirements for Computer Based Systems – July 2017, based on the IACS Unified Requirements E22 (Rev.2 June 2016, Complete Revision)

The *Publication* was approved by the PRS Board on 28 June 2017 and enters into force on 1 July 2017.

© Copyright by Polski Rejestr Statków S.A., 2017

PRS/OP, 06/2017

CONTENTS

page

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. The requirements focus on the functionality of the software and on the hardware supporting the software. These requirements apply to the use of computer based systems which provide control, alarm, monitoring, safety or internal communication functions which are subject to classification requirements.

1.2 Exclusion

Navigation systems required by SOLAS Chapter V, Radio-communication systems required by SOLAS Chapter IV, and vessel loading instrument/stability computer are not in the scope of this requirement.

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

1.3 References

For the purpose of application of this UR, the following identified standards can be used for the development of hardware/software of computer based systems. Other industry standards may be considered:

– IEC 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems
– ISO/IEC 12207: Systems and software engineering - Software life cycle processes
– ISO 9001:2008 Quality Management Systems - Requirements

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. 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.
   – ISO/IEC 90003: Software engineering – Guidelines for the application of ISO 9001:2008 to computer software
   – IEC 60092-504: Electrical installations in ships – Part 504: Special features – Control and instrumentation
   – ISO/IEC 25000: Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – Guide to SQuaRE
   – ISO/IEC 25041: Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – Evaluation guide for developers, acquirers and independent evaluators
   – IEC 61511: Functional safety – Safety instrumented systems for the process industry sector
   – ISO/IEC 15288: Systems and software engineering – system life cycle process

2 DEFINITIONS

2.1 Stakeholders

2.1.1 Owner

The Owner is responsible for contracting the system integrator and/or suppliers to provide a hardware system including software according to the owner's specification. The Owner could be the Ship Builder Integrator (Builder or Shipyard) during initial construction. After vessel delivery, the owner may delegate some responsibilities to the vessel operating company.

2.1.2 System integrator

The role of system integrator shall be taken by the yard unless an alternative organisation is specifically contracted/assigned this responsibility. The system integrator is responsible for the integration of systems and products provided by suppliers into the system invoked by the requirements specified herein and for providing the integrated system. The system integrator may also be responsible for integration of systems in the vessel.

If there are multiple parties performing system integration at any one time a single party is to be responsible for overall system integration and coordinating the integration activities. If there are multiple stages of integration different System Integrators may be responsible for specific stages of integration but a single party is to be responsible for defining and coordinating all of the stages of integration.

2.1.3 Supplier

The Supplier is any contracted or subcontracted provider of system components or software under the coordination of the System Integrator or Shipyard. The supplier is responsible for providing programmable devices, sub-systems or systems to the system integrator. The supplier provides a description of the software functionality that meets the Owner's specification, applicable international and national standards, and the requirements specified herein.

2.2 Objects

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

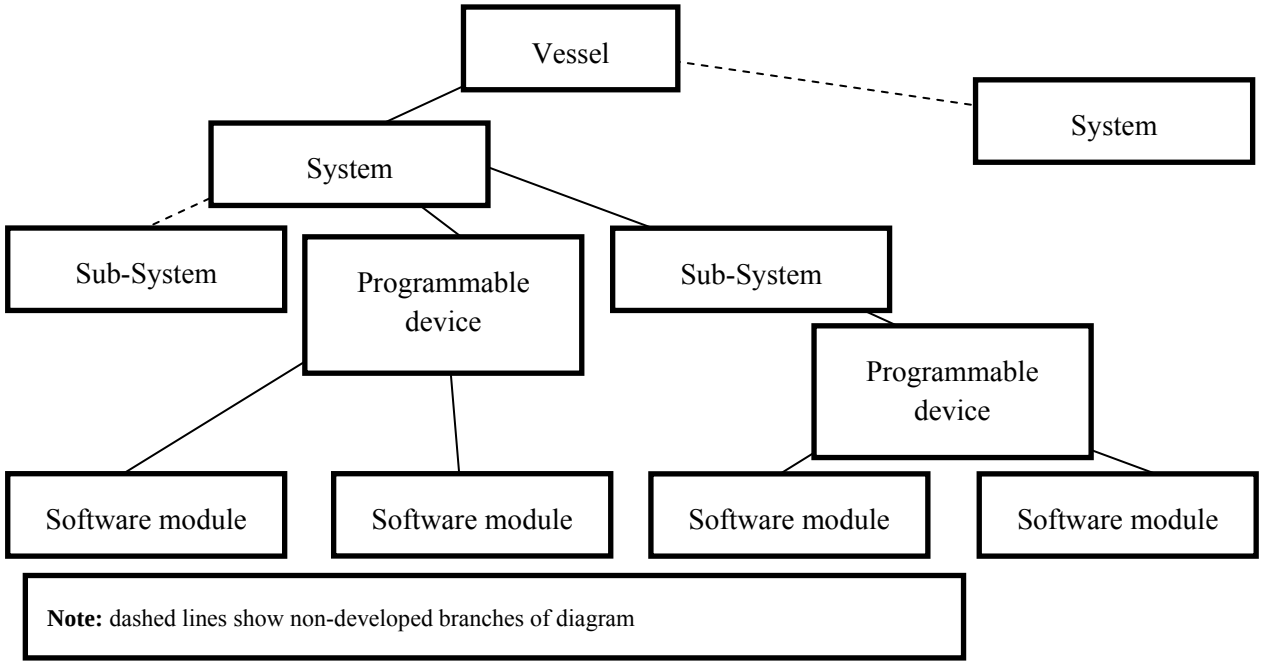

Fig. 1 Illustrative System Hierarchy

2.2.1 Object definitions

2.2.1.1 Vessel

Ship or offshore unit where the system is to be installed.

2.2.1.2 System

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

2.2.1.3 Sub-system

Identifiable part of a system, which may perform a specific function or set of functions.

2.2.1.4 Programmable device

Physical component where software is installed.

2.2.1.5 Software module

A module is a standalone piece of code that provides specific and closely coupled functionality.

2.3 System categories

The following table (Table 1) shows how to assign system categories based on their effects on system functionality.

Table 1
System categories

Category	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 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 – Vessel safety functions

The following systems typically belong to Category III, the exact category being dependent on the risk assessment for all operational scenarios:

- Propulsion system of a ship, meaning the means to generate and control mechanical thrust in order to move the ship (devices used only during manoeuvring are not in the scope of this requirement such as bow tunnel thrusters)
- Steering system control system
- Electric power system (including power management system)
- Ship safety systems covering fire detection and fighting, flooding detection and fighting, internal communication systems involved in evacuation phases, ship systems involved in operation of life saving appliances equipment
- Dynamic positioning system of equipment classes 2 and 3 according to IMO MSC/Circ.645
- Drilling systems

The following systems typically belong to Category II, the exact category being dependent on the risk assessment for all operational scenarios:

- Liquid cargo transfer control system
- Bilge level detection and associated control of pumps
- Fuel oil treatment system
- Ballast transfer valve remote control system
- Stabilization and ride control systems
- Alarm and monitoring systems for propulsion systems

The example systems are not exhaustive.

2.4 Other terminology

2.4.1 Simulation tests

Control 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.

3 REQUIREMENTS FOR SOFTWARE AND SUPPORTING HARDWARE

3.1 Life cycle approach

A global top to bottom approach shall be undertaken regarding software and the integration in a system, spanning the software lifecycle. This approach shall be accomplished according to software development standards as listed herein or other standards recognized by the Class Society.

3.1.1 Quality system

System integrators and suppliers shall operate a quality system regarding software development and testing and associated hardware such as ISO 9001 taking into account ISO 90003.

Satisfaction of this requirement shall be demonstrated by either:

– The quality system being certified as compliant to the recognized standard by an organisation with accreditation under a national accreditation scheme, or
– The Class Society confirming compliance to the standard through a specific assessment.

This quality system shall include:

3.1.1.1 Relevant procedures regarding responsibilities, system documentation, configuration management and competent staff.

3.1.1.2 Relevant procedures regarding software lifecycle and associated hardware:

– Organization set in place for acquisition of related hardware and software from suppliers
– Organization set in place for software code writing and verification
– Organization set in place for system validation before integration in the vessel

3.1.1.3 Minimum requirements for approval of Quality system:

– Having a specific procedure for verification of software code of Category II and III at the level of systems, sub-systems and programmable devices and modules
– Having check points for the Class Society for Category II and III systems (see Annex for the minimum check points[1] 1)
– Having a specific procedure for software modification and installation on board the vessel defining interactions with owners

3.1.1.4 Quality Plan

A document, referred to herein as a Quality Plan, shall be produced that records how the quality management system will be applied for the specific computer based system and that includes, as a minimum, all of material required by paragraphs 3.1.1.1 to 3.1.1.3 inclusively.

3.1.2 Design phase

3.1.2.1 Risk assessment of system

This step shall be undertaken to determine the risk to the system throughout the lifecycle by identifying and evaluating the hazards associated with each function of the system. A risk assessment report shall upon request be submitted to the Class Society:

This document shall normally be submitted by the System Integrator or the Supplier, including data coming from other suppliers.

[1] Examples of check points can be a required submittal of documentation, a test event, a technical design review meeting, or peer review meeting.

IEC/ISO31010 “Risk management – Risk assessment techniques” may be applied in order to determine method of risk assessment. The method of risk assessment shall be agreed by the society.

Based on the risk assessment, a revised system category might need to be agreed between Class and the system supplier.

Where the risks associated with a computer based system are well understood, it is permissible for the risk assessment to be omitted, however in such cases the supplier or the system integrator shall provide a justification for the omission. The justification should give consideration to:

- How the risks are known
- The equivalence of the context of use of the current computer based system and the computer based system initially used to determine the risks
- The adequacy of existing control measures in the current context of use

3.1.2.2 Code production and testing

The following documentation shall be provided to the Class Society for Category II and III systems:

- Software modules functional description and associated hardware description for programmable devices. This shall be provided by Supplier and System Integrator.
- Evidence of verification (detection and correction of software errors) for software modules, in accordance with the selected software development standard. Evidence requirements of the selected software standard might differ depending on how critical the correct operation of the software is to the function it performs (i.e. IEC 61508 has different requirements depending on SILs, similar approaches are taken by other recognized standard). This shall be supplied by the Supplier and System Integrator.
- Evidence of functional tests for programmable devices at the software module, sub-system, and system level. This shall be supplied by the Supplier via the System Integrator. The functional testing shall be designed to test the provisions of features used by the software but provided by the operating system, function libraries, customized layer of software and any set of parameters.

3.1.3 Integration testing before installation on board

Intra-system integration testing shall be done between system and sub-system software modules before being integrated on board. The objective is to check that software functions are properly executed, that the software and the hardware it controls interact and function properly together and that software systems react properly in case of failures. 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. Functional and failure testing can be demonstrated by simulation tests.

For Category II and III systems:

- Test programs and procedures for functional tests and failure tests shall be submitted to the Class Society. A FMEA may be requested by the Class Society in order to support containment of failure tests programs.
- Factory acceptance test including functional and failure tests shall be witnessed by Class Society.

Following documentation shall be provided:

(i) Functional description of software
(ii) List and versions of software installed in system
(iii) User manual including instructions for use during software maintenance
(iv) List of interfaces between system and other ship systems
(v) List of standards used for data links
(vi) Additional documentation as requested by the Class Society which might include an FMEA or equivalent to demonstrate the adequacy of failure test case applied

3.1.4 Approval of programmable devices for Category II and III systems

Approval of programmable devices integrated inside a system shall be delivered to the system integrator or supplier. Approval can be granted on case by case basis, or as part of a product type approval, so long as above mentioned documents have been reviewed/approved (as per annex) and the

required tests have been witnessed by the Class Society (also see paragraph 4 regarding hardware environmental type tests). Documentation should address the compatibility of the programmable device in the ship's application, the necessity to have on board tests during ship integration and should identify the components of system using the approved programmable devices.

3.1.5 Final integration and on board testing

Simulation tests are to be undertaken before installation, when it is found necessary to check safe interaction with other computerized systems and functions that could not be tested previously.

On board tests shall check that a computer based system in its final environment, integrated with all other systems with which it interacts is:

- Performing functions it was designed for
- Reacting safely in case of failures originated internally or by devices external to the system
- Interacting safely with other systems implemented on board vessel

For final integration and on board testing of Category II and III systems:

- Test specifications shall be submitted to the Class Society for approval
- The tests shall be witnessed by the Class Society

3.2 Limited approval

Sub-systems and programmable devices may be approved for limited applications with service restrictions by the Class Society when the ship system where they will be integrated is not known. In this case, requirements about Quality systems under paragraph 3.1.1 might need to be fulfilled as required by the Class Society. Additional drawings, details, tests reports and surveys related to the Standard declared by the Supplier may be required by the Class Society upon request.

Sub-systems and programmable devices may in this case be granted with a limited approval mentioning the required checks and tests performed.

3.3 Modifications during operation

3.3.1 Responsibilities

Organizations in charge of software modifications shall be clearly declared by Owner to the Class Society. A System integrator shall be designated by the Owner and shall fulfil requirements mentioned in paragraph 3.1. Limited life cycle steps may be considered for modifications already considered and accepted in the scope of initial approval. The level of documentation needed to be provided for the modification shall be determined by the Class Society.

At the vessel level, it is the responsibility of Owner to manage traceability of these modifications; the achievement of this responsibility shall be supported by system integrators updating the Software Registry. This Software Registry shall contain:

- List and versions of software installed in systems required in paragraph 3.1.3
- Results of security scans as described in paragraph 3.4

3.3.2 Change management

The owner 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. All changes to computer based systems in the operational phase shall be recorded and be traceable.

3.4 System security

Owner, system integrator and suppliers shall adopt security policies and include these in their quality systems and procedures.

For Category I, II, and III systems, physical and logical security measures shall be in place to prevent unauthorized or unintentional modification of software, whether undertaken at the physical system or remotely.

Prior to installation, all artefacts, software code, executables and the physical medium used for installation on the vessel are to be scanned for viruses and malicious software. Results of the scan are to be documented and kept with the Software Registry.

4 REQUIREMENTS FOR HARDWARE REGARDING ENVIRONMENT

Evidence of environmental type testing according to UR E10 regarding hardware elements included in the system and sub-systems shall be submitted to the Class Society for Category I, II and III computer based systems. This requirement is not mandatory for Category I computer based systems not considered by Class.

5 REQUIREMENTS FOR DATA LINKS FOR CATEGORY II AND III SYSTEMS

5.1 General requirements

5.1.1 Loss of a data link shall be specifically addressed in risk assessment analysis.

5.1.2 A single failure in data link hardware shall be automatically treated in order to restore proper working of system. For Category III systems a single failure in data link hardware shall not influence the proper working of the system.

5.1.3 Characteristics of data link shall prevent overloading in any operational condition of system.

5.1.4 Data 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.

5.2 Specific requirements for wireless data links

5.2.1 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.

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

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

- Message integrity. Fault prevention, detection, diagnosis, and correction so that the received message is not corrupted or altered when compared to the transmitted message.
- Configuration and device authentication. Shall only permit connection of devices that are included in the system design.
- Message encryption. Protection of the confidentiality and or criticality of the data content.
- Security management. Protection of network assets, prevention of unauthorized access to network assets.

5.2.2.2 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.

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.

5.2.2.3 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 its self-fail as a result of electromagnetic interference during expected operating conditions.

Annex – Documents for class society and test attendance

Ⓐ Submitted (For Approval) Ⓘ Provided (For Information) Ⓦ Witness

[1] Additional documentation may be required upon request

[2] Upon request

[3] If in the scope of Class requirement

Requirement	SUPPLIER INVOLVED	SYSTEM INTEGRATOR INVOLVED	OWNER INVOLVED	CATEGORY I[1]	CATEGORY II	CATEGORY III
Quality Plan	X	X		Ⓐ[2]	Ⓐ	Ⓐ
Risk assessment report		X		Ⓘ[2]	Ⓘ[2]	Ⓘ[2]
Software modules functional description and associated hardware description	X (if necessary)	X			Ⓘ	Ⓘ
Evidence of verification of software code	X (if necessary)	X			Ⓘ	Ⓘ
Evidence of functional tests for elements included in systems of Category II and III at the level of software module, sub-system and system	X	X			Ⓘ	Ⓘ
Test programs and procedures for functional tests and failure tests including a supporting FMEA or equivalent, at the request of the Class Society		X			Ⓐ	Ⓐ
Factory acceptance test event including functional and failure tests	X	X			Ⓦ	Ⓦ
Test program for simulation tests for final integration		X			Ⓐ	Ⓐ
Simulation tests for final integration		X			Ⓦ	Ⓦ
Test program for on board tests (includes wireless network testing)		X			Ⓐ	Ⓐ
On board integration tests (includes wireless network testing)		X			Ⓦ	Ⓦ

Requirement	SUPPLIER INVOLVED	SYSTEM INTEGRATOR INVOLVED	OWNER INVOLVED	CATEGORY I[1]	CATEGORY II	CATEGORY III
- List and versions of software installed in system - Functional description of software - User manual including instructions during software maintenance - List of interfaces between system and other ship systems		X			Ⓘ	Ⓘ
Updated Software Registry		X	X		Ⓘ	Ⓘ
Procedures and documentation related to Security Policy					Ⓘ	Ⓘ
Test reports according to UR E10 requirements	X	X		Ⓐ[3]	Ⓐ	Ⓐ