INTERNATIONAL STANDARD

ISO 17894

First edition
2005-03-15

Ships and marine technology — Computer applications — General principles for the development and use of programmable electronic systems in marine applications

Navires et technologies marines — Applications informatiques — Principes généraux pour le développement et l'utilisation des systèmes électroniques programmables pour applications marines

Reference number
ISO 17894:2005(E)

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO 17894 was prepared by Technical Committee ISO/TC 8, *Ships and marine technology*, Subcommittee SC 10, *Computer applications*.

Introduction

Systems which include programmable electronic systems (PES) are not exact substitutes for the electromechanical systems and/or crew tasks which they replace. A new technology is involved, which can provide opportunities for integration of traditional system components (including crew tasks) and more complex behaviour. This allows increases in efficiency and safety through improved monitoring, better situational awareness on the bridge, etc. However, PES are complex products and, like all products, they can contain defects. These defects cannot be seen. Software does not respond to traditional engineering methods for the testing of soundness. The combination of complexity, replacement of a combination of mechanical and crew functions with computer hardware and software, and industry practice in developing and maintaining marine PES leads to a wide range of potential defects which cannot be guarded against by prescriptive standards.

The use of a PES in the management, monitoring or control of a ship may have several effects:

- potential to enhance the ability and efficiency of the crew;
- changes in the organization of work through the automation of lower-level tasks;
- integration of systems through use of several systems by one seafarer;
- shift in the role of the crew towards the management of many linked, complex PES;
- shift of the crew's perception of the ship to that presented by the interfaces of the PES;
- layers of embedded and/or application software interposed between the crew and the ship;
- physical interconnection of ship systems through the use of computer networks.

The overall effect of the use of PES is that the ship becomes one **total system** of inter-linked PES and crew which work together to fulfil the operator's business goals for the ship. In order for this total system to be dependable, both the design of the PES and the management of its use have to support the safe and effective performance of the crew as a critical component of the total system. Such a **human-centred** approach has to be based on a thorough knowledge of the particular skills, working environment and tasks of the crew using the PES. The total system concept is described further in A.2.

In the traditional approach to maritime safety, ship systems are built to and operated against precise, prescriptive standards. These standards were developed in response to feedback about incidents or risky behaviour of previous ship systems. This approach is appropriate for relatively simple systems in a time of slow technical innovation. However, suppliers and operators nowadays want to innovate with complex, new solutions. In addition, the base technologies for PES are evolving very quickly. The assurance of dependability in this case cannot rely on knowledge of previous systems. The solution is for the developer and operator to assess the risks from and to the particular ship, its systems, crew and its operating philosophy, and to address these specific risks in the design and operation of the PES. Components of the system can then either be re-designed or operated in such a way as to minimize these risks. The quality of construction, operation and maintenance of the system to be sure of the achievement of a required level of dependability of the PES is also defined.

This International Standard is based on best practice in PES development as stated in existing marine, electrical and electronic, IT, ergonomics and safety standards. It is not intended to replace any of these standards. It presents a synoptic view of the requirements of these standards as a framework of principles for the development of dependable PES.

Ships and marine technology — Computer applications — General principles for the development and use of programmable electronic systems in marine applications

1 Scope

This International Standard provides a set of mandatory principles, recommended criteria and associated guidance for the development and use of dependable marine programmable electronic systems for shipboard use. It applies to any shipboard equipment containing programmable elements which may affect the safe or efficient operation of the ship. It contains information for all parties involved in the specification, operation, maintenance and assessment of such systems. The principles and guidance in the document are largely based on requirements in national and International Standards. The source standards and their contribution to this International Standard are presented in the bibliography.

NOTE This International Standard does not directly address performance, test or test results requirements associated with specific types of equipment or functions. In such instances existing application or component standards may be applied, e.g. IEC 60945, in respect of navigation and radio-communications equipment. The responsible body (e.g. National Administration, Classification Society or other contracted party) will determine the applicability of this International Standard, and its specific requirements where any potential conflict arises.

2 Conformance

An organization demonstrating compliance to this International Standard shall provide evidence of how its system fulfils the principles stated in Clause 7. The evidence shall be to the satisfaction of an independent assessor. This can be achieved through compliance with the criteria given in Clause 7 or by an alternative means which is to the satisfaction of an independent assessor.

NOTE The criteria for assessment are given in an itemized list below each principle in Clause 7.

3 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 9000:2000, *Quality management systems — Fundamentals and vocabulary*

ISO 9241-2, *Ergonomic requirements for office work with visual display terminals (VDTs) — Part 2: Guidance on task requirements*

ISO 9241-10, *Ergonomic requirements for office work with visual display terminals (VDTs) — Part 10: Dialogue principles*

ISO 9241-11, *Ergonomic requirements for office work with visual display terminals (VDTs) — Part 11: Guidance on usability*

ISO 10007, *Quality management systems — Guidelines for configuration management*

ISO 13407, *Human-centred design processes for interactive systems*

ISO/IEC 2382-1, *Information technology — Vocabulary — Part 1: Fundamental terms*

ISO/IEC 9126-1, *Software engineering — Product quality — Part 1: Quality model*

ISO/IEC 12207, *Information technology — Software life cycle processes*

ISO/IEC 12207:1995/Amd.1:2002, *Information technology — Software life cycle processes — Amendment 1*

ISO/IEC 12207:1995/Amd.2:2004, *Information technology — Software life cycle processes — Amendment 2*

IEC 61069-1, *Industrial-process measurement and control — Evaluation of system properties for the purpose of system assessment — Part 1: General considerations and methodology*

IEC 61508-4, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 4: Definitions and abbreviations*

IEEE 610.12, *Standard glossary of software engineering terminology*

BS 4778-3.1, *Quality vocabulary. Availability, reliability and maintainability terms. Guide to concepts and related definitions*

BS 4778-3.2, *Quality vocabulary. Availability, reliability and maintainability terms. Glossary of international terms*

4 Terms and definitions

For the purposes of this document, the following terms and definitions apply. The following referenced definitions are stated here since there is some inconsistency between the listed standards and also because the listed definitions are used frequently in this document. Annex A elaborates the concepts behind key terms used in this International Standard.

4.1
context of use
the users, goals, tasks, equipment (hardware, software and materials), and the physical and social environments in which a product is used

[ISO 9241-11]

NOTE See A.2 for an elaboration of this term as used in this International Standard.

4.2
dangerous failure
failure which has the potential to put the safety-related system into a hazardous or fail-to-function state

[IEC 61508-4]

NOTE Whether or not the potential is realized may depend on the architecture of the system; in systems with multiple channels to improve safety, a dangerous failure is less likely to lead to the overall dangerous or fail-to-function state.

4.3
dependability
the extent to which a system can be relied upon to perform exclusively and correctly a task under given conditions at a given instant of time or over a given time interval, assuming that the required external resources are provided

[IEC 61096-5]

4.4
failure
the termination of the ability of an item to perform a required function

[IEC Guide 50(191)]

NOTE An error is that part of the system state which is liable to lead to failure. A failure occurs because the system is erroneous [IEC 61508-4]. Error is a discrepancy between a computed, observed or measured value or condition and the true, specified, or theoretically correct value or condition. (IEC Guide 50(191); [BS 4778])

4.5
fault
the state of an item characterized by inability to perform a required function, excluding the inability during preventive maintenance or other planned actions, or due to lack of external resources

[IEC Guide 50(191)]

4.6
fault tolerance
the attribute of an item that makes it able to perform a required function in the presence of certain given sub-item faults

[IEC 61508-4, IEC Guide 50(191), BS 4778]

4.7
hazard
a situation that could occur during the lifetime of a product, system or plant that has the potential for human injury, damage to property, damage to the environment, or economic loss

[BS 4778]

4.8
programmable electronic system
a system based on one or more programmable electronic devices, connected to (and including) input devices (e.g. sensors) and/or output devices/final elements (e.g. actuators), for the purposes of control, protection or monitoring

[IEC 61508-4]

NOTE 1 The term PES includes all elements in the system, including power supplies, extending from sensors or other input devices, via data highways or other communicating paths, to the actuators, or other output devices.

NOTE 2 See A.1 for an elaboration of this term as used in this International Standard.

4.9
risk
the probable rate of occurrence of a hazard causing harm and the degree of severity of the harm

[IEC 51]

NOTE See A.3 for an elaboration of this term as used in this International Standard.

4.10
software
all or part of the programs, procedures, rules and associated documentation of an information-processing system

[ISO 2382-1:1993]

4.11
system life cycle
the activities occurring during a period of time that starts when a system is conceived and ends when the system is no longer available for use

[IEC 61508-4]

4.12
task
the smallest indivisible part of an activity when it is broken down to a level best understood and performed by a specific user

[BS 4778]

NOTE There is a distinction between task and function. Function is defined as an elementary operation performed by the system which, combined with other elementary operations (system functions), enables the system to perform a task [IEC 61096-1]. Functions are an attribute of systems whereas tasks are performed by users within work systems.

4.13
usability
the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use

[ISO 9241-11]

4.14
user
The individual interacting with the system, [ISO 9241-10 and -2] or person, who uses software to perform some task

[IEEE 610.12]

NOTE 1 For a COTS product, the user will include the designer who customizes the product to fulfil required functions in a specific system. Throughout the life of a system, those who customize or maintain the PES will also be users of some aspects of the system.

NOTE 2 Individuals or groups that are affected by the output, operation or existence of a PES but who do not directly interact with the PES are classed as stakeholders.

NOTE 3 In the annexes to this International Standard, the term “user” is occasionally extended to refer to all prospective or actual users. This usage may include, for example, stakeholders such as maintenance staff, owner management and different (other) groups of users.

4.15
validation
confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled

[ISO 9000:2000]

NOTE Validation demonstrates that the PES, before or after installation, meets the requirements for the PES.

4.16
verification
confirmation, through the provision of objective evidence, that specified requirements have been fulfilled

[ISO 9000:2000]

NOTE In the context of this International Standard, verification is the act of demonstrating that deliverables for a specific life cycle stage meet the inputs to that stage.

5 Symbols and abbreviated terms

COTS	commercial off the shelf
PES	programmable electronic system
PE	programmable electronic devices
SIL	safety integrity level
V&V	verification and validation

6 Use of this International Standard

This International Standard contains a high level set of principles for the development and use of marine PES. These principles are not grouped beyond a split between product and process. The lack of grouping of the principles is intended to prevent readers concluding that a particular principle will only apply in a particular case.

The terms used are defined but can be interpreted. This range of interpretation is intentional and is intended to be a strength of the approach. It allows the principles and associated assessment criteria (listed below each principle) to be interpreted for a broad range of PES. This is important because this International Standard is intended to apply to all PES. The range of business requirements for ships and their systems is broad and multi-dimensional and, as described in the Introduction, all systems form part of the total system of the ship. An assessor, developer or user of a marine PES can place emphasis on particular principles depending on the context of use of the PES.

During assessment the criteria given as sub-items to each of the principles in Clause 7 are interpreted at the minimum level necessary for the integrity of the PES. Therefore, those wishing to apply the standard may not need to fully address all recommendations for all PES, but the underlying intent of the criteria should be considered for all PES. Risk and context of use should be taken into account at all times, including assessment.

The guidance given in Annex B provides advice on interpretation of the principles for both low-risk and high-risk PES. Specific advice on measures to be taken in different risk situations is available in the supporting standards.

Organizations will have varying degrees of responsibility for different areas of compliance. Degree of risk, practicalities and stage in the life cycle will all be factors in agreeing the interpretation and application of the principles in any particular project. The principles should be treated as the general safety requirements for all PES.

Owners need to consider and document the context of use which they wish to create for PES onboard. They should then allocate the functions which they wish to be implemented by PES and define the user requirements of these systems.

Ship builders, or other integrators of PES in a newbuilding/modification, should apply the principles to their own work and to each sub-contractor and equipment supplier.

Buyers of marine PES should recognize that some part of the operation of their ships is mediated by computer software. The principles in this document should be applied to the use and maintenance of PES throughout the life of the ship in order to minimize any risk arising from this particular technology.

Implementation of the approach to development and operation of PES described in this International Standard require support from management. In most cases, organizations will have a PES development and/or support life cycle in place already. How closely this matches up with the life cycle and outputs described in Annexes C and D of this International Standard will have an impact on how easily it can be accepted.

Annex B contains a general commentary on each principle and also provides specific guidance for particular participants or stages in the life cycle. Annex E illustrates the issues, actions and responsibilities associated with use of the standard throughout the life cycle of a system. A list of the principles is given in Annex F.

Implementation of the requirements of this International Standard requires cooperation, thought and shared responsibility both by PES developers, operators and the organization which is to assess this conformance. The assessor should work from the principles down to the evidence which is required in order to give assurance that the particular PES meets the principles. The parties being assessed should work up from the requirements of the particular PES to the evidence and V&V plan required by the assessor. The result will be agreed evidence, a test/support programme for the hardware, software, data, documentation and training, and assigned responsibility for the provision of evidence and fulfilment of requirements. A generic life cycle and list of project outputs that may be used as a basis for the specification of evidence are given in Annexes C and D.

Readers of this International Standard are expected to have some familiarity with the concepts of quality management, systems, safety and software engineering, and human factors. The Bibliography lists standards and other documents that address these topics. In order to gain a clear understanding of the relationship between this general systems standard and equipment- or application-specific standards, such as those for navigation equipment, readers are advised to study the annexes, in particular A, B.1 & B.2, C and E before reading the requirements given in Clause 7.

7 Principles for marine PES

7.1 Intention for marine PES

The PES shall be demonstrably suitable for the user and the given task in a particular context of use. It shall deliver correct, timely, sufficient and unambiguous information to its users and other systems. The hardware and software of the PES shall respond correctly throughout its life cycle.

This can be achieved if the following principles are fulfilled by the PES and its associated elements throughout its life.

7.2 Product principles for marine PES

7.2.1 First principle

P1 The PES shall be free from unacceptable risk of harm to persons or the environment.

a) The risk from hazards arising from both the intrinsic (physical) properties of the PES and its functional behaviour should be reduced to an acceptable level. These may include mechanical, electrical, thermal, noise/vibration, fire and explosion, chemical, biological, radiation and occupational health.

b) The acceptable risk associated with the PES should be based on its intended use, covering all defined operating conditions, and reasonably foreseeable misuse.

7.2.2 Second principle

P2 In the event of failure, the PES shall remain in or revert to the least hazardous condition.

a) Means should be provided to detect dangerous failures before they lead to a hazardous condition.

b) The PES should remain in, or revert to, a safe state when dangerous failures occur.

c) Means should be provided to notify users of failures.

7.2.3 Third principle

P3 The PES shall provide functions which meet user needs.

a) The functional requirements of the PES should be achieved for all defined operating conditions.

b) The set of functions provided should be appropriate for the task. This includes functions for monitoring, controlling, reporting, protecting and information processing as appropriate.

c) Suitable means should be provided to select and execute functions as and when required.

d) The functions provided should take account of user characteristics.

7.2.4 Fourth principle

P4 Functions shall be appropriately allocated between users and PES.

a) Functions that are outside the capabilities and limitations of human operators should be allocated to the PES.

b) The complexity of user allocated functions should be matched to user skills and abilities.

c) The functions allocated to the user should form a meaningful set in terms of the task goals and user workload.

7.2.5 Fifth principle

P5 The PES shall be tolerant of faults and input errors.

a) Incorrect or abnormal inputs from external systems should be rejected or corrected by the PES as appropriate.

b) The PES interface should assist the user in avoiding input errors and in detecting input errors where they are made and alert the user when they occur.

c) The PES should minimize the corrective actions needed to achieve results despite faults and input errors.

d) The PES should have specific features to detect and take actions to tolerate

1) residual design faults in the hardware and software; and

2) environmental stresses.

e) The operation of protective functions and equipment should not be interfered with by failures in other functions and equipment.

7.2.6 Sixth principle

P6 The PES shall maintain specified levels of accuracy, timeliness and resource utilization when used under specified operational and environmental conditions.

a) The PES should maintain the accuracy, frequency and duration of all outputs at the required levels for each specified operational and environmental condition.

b) The PES should maintain the required speed of response and the processing durations for all provided functions.

7.2.7 Seventh principle

P7 Unauthorized access to the PES shall be prevented.

a) Unauthorized operation or reconfiguration of the PES should be prevented.

b) Data, software and hardware should be protected from unauthorized modification.

7.2.8 Eighth principle

P8 The PES shall be acceptable to the user and support effective and efficient operation under specified conditions.

a) The PES interface should take account of the task environment and performance requirements, and the characteristics and competence of typical users.

b) The amount of information presented to the user should be designed to be understandable, accurate and acceptable under all operational circumstances.

c) Unnecessary operational sequences should be avoided.

d) The operation of the complete system should meet defined requirements for effectiveness and efficiency of operation under representative task conditions.

e) The complete system should meet defined requirements for acceptability to typical users.

7.2.9 Ninth principle

P9 The operation of the PES shall be consistent and shall correspond to user expectations of the underlying process.

a) The user's model (the required properties, behaviours and analogies to physical or other devices) of the PES should be defined.

b) I/O devices, formats and dialogues should be matched to user characteristics and tasks.

c) The behaviour and appearance of the interface should be consistent.

d) The codes and symbols used in the interface should be defined and consistent.

e) Feedback and explanation should be accurate, understandable and relevant.

f) The interaction with, and interface and behaviour of the system should match the expectations of representative users

7.2.10 Tenth principle

P10 The interaction between the PES and the user shall be controllable by the user.

a) The safe limits to operator control of the interface should be defined and reconciled with the expected range of user characteristics.

b) Output, feedback and explanation should be adjustable to suit user characteristics and the task needs.

c) Alternative representations of input/output data should be available to suit the needs of user groups.

d) The user should be able to control the sequence and speed of interaction with the PES in order to achieve safe and effective control.

e) If interrupted, the user should be able to safely restart a dialogue.

f) Alternative interaction methods should be provided to support safe operation by the expected range of users.

7.2.11 Eleventh principle

P11 The PES shall support proper installation and maintenance, including repair and modification.

a) The PES structure should be modular and hierarchical with simple interfaces to other equipment.

b) Interchangeable PES components should be straightforward to change with:

   1) simple, loosely coupled interfaces to other components; and

   2) unambiguous identification.

c) The PES should support effective diagnosis to identify faulty components.

d) The PES should support inspection and testing following repair or modification.

e) Specified times to restore the PES to a functioning state after failure should be achieved.

7.3 Life cycle principles for marine PES

7.3.1 General

The successful realization and use of a dependable marine PES requires a systematic approach throughout the life of the PES. The key requirements for any approach which aims to meet the product principles given in 7.2 are described below.

7.3.2 Twelfth principle

P12 All PES life cycle activities shall be planned and structured in a systematic manner.

NOTE Adequate shipboard maintenance support in terms of spares, maintenance procedures and trained personnel is a specific issue covered by this principle.

a) Life cycle phases should be defined and contain elementary tasks with specified inputs, outputs and activities.

b) Life cycle phases should be organized and structured into a methodical sequence which provides for iteration.

c) Plans to cover all life cycle activities should be prepared as appropriate and followed.

7.3.3 Thirteenth principle

P13 The required level of safety shall be realized by appropriate activities throughout the life cycle.

a) Hazards associated with the PES should be identified at all stages of production for all operational conditions and for reasonably foreseeable misuse.

b) The risks associated with each hazard should be estimated and evaluated for acceptability.

c) Risks should be reduced to an acceptable level by hazard elimination or by implementing specified protective measures.