BS ISO 17894:2005

BSI Standards Publication

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

bsi.

...making excellence a habit.™

National foreword

This British Standard is the UK implementation of ISO 17894:2005.

The standards listed in Clause 2 (normative references) include source documents for terms and definitions reproduced in Clause 3 and, in accordance with D.1.4 of the ISO/IEC Directives, Part 2 (2004), these references are informative. The UK committee would like to emphasize that this standard can be applied as a stand alone document and no other publication is indispensible to its application. However, the bibliography lists seven 'primary standards' that are extensively cited in informative Annex B and that these are helpful in the application of BS ISO 17894:2005.

The UK participation in its preparation was entrusted to Technical Committee SME/32, Ships and marine technology - Steering committee.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

ISBN 978 0 580 74561 4

ICS 35.240.60; 47.020.99

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 July 2011.

Amendments issued since publication

Date	Text affected

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)

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.

d) Personnel should be informed of assigned safety responsibilities in a timely manner.

e) A description of the hazards and risk management results should be created and maintained throughout the life cycle.

f) Safety requirements for the PES should be specified in terms of safety functions to be provided and the integrity required of each safety function.

g) Requirements of applicable legislation, standards and regulations should be addressed when determining hazards, risks and safety requirements.

h) The level of safety achieved by the PES should be judged by an appointed, independent assessor.

i) Justification of the level of safety achieved should be documented and be traceable to the safety requirements.

7.3.4 Fourteenth principle

P14 Human-centred activities shall be employed throughout the life cycle.

a) The life cycle of the PES should be iterative such that it meets clearly defined user tasks and goals.

b) The PES should take account of applicable knowledge from the human sciences.

c) User characteristics should be taken into account throughout the life cycle of the PES by teams with appropriate multi-disciplinary skills.

d) Evolution of the PES is to be led by user feedback obtained by appropriate means from:

   1) users from all interest groups;

   2) representative users; and

   3) direct user experience of the system and prototypes.

7.3.5 Fifteenth principle

P15 Verification and validation activities shall be employed throughout the life cycle.

a) Each life cycle phase should be concluded by a verification activity.

b) Personnel responsible for verification or validation activities should be independent from those personnel responsible for the life cycle outputs which are being verified or validated.

c) The PES should be validated against the PES requirements.

d) The criteria, techniques and tools used for verification and validation activities should be specified.

e) All safety functions should be tested with test cases that are traceable to safety requirements.

f) All modifications to the PES should be verified and validated.

7.3.6 Sixteenth principle

P16 All parties involved in life cycle activities shall have and use a quality management system.

a) The quality system should accord with an appropriate standard or Code of Practice.

b) Quality activities should be performed throughout the life cycle.

c) The independence requirements for roles associated with quality, safety, verification, validation and assessment activities should be specified and observed.

7.3.7 Seventeenth principle

P17 Existing requirements for marine systems shall be taken into account throughout the life cycle.

a) Applicable legislation, standards and regulations for the PES should be identified.

b) Conformance of the PES to the requirements in applicable legislation, standards and regulations should be demonstrated.

7.3.8 Eighteenth principle

P18 Suitable documentation shall be produced to ensure that all PES life cycle activities can be performed effectively.

a) Documentation should be accurate, unambiguous, comprehensible, suitable for its intended purpose and produced in a timely manner.

b) Conformance of the PES to specified requirements should be traceable.

c) The required documentation from each life cycle phase should be defined, produced and brought under document control.

NOTE This includes description of the PES, PES requirements, description of hazards and risk management results, plans, verification and validation specifications and results, design documentation, user manuals, installation and maintenance manuals.

d) Records of life cycle activities should be retained to demonstrate their successful achievement.

e) User manuals should include procedures for normal and abnormal operating conditions.

7.3.9 Nineteenth principle

P19 Persons who have responsibilities for any life cycle activities shall be competent to discharge those responsibilities.

a) Personnel competence should include appropriate training, knowledge, experience and qualifications for their assigned duties.

b) Personnel competencies should be justified and documented.

c) Personnel competencies should be maintained.

d) The competence and culture of teams should support team members in achieving project and/or system goals.

7.3.10 Twentieth principle

P20 The PES configuration shall be identified and controlled throughout the life cycle.

a) The structure and breakdown of the PES in terms of configured components should be clearly identified.

b) The documentation defining the functional and physical characteristics of the PES components, including modifications, should be identified and traceable to the components.

c) The stages in the life cycle at which components are brought under configuration control should be defined.

d) The current approved PES configuration covering hardware, software and data elements should be identifiable for each of the relevant life cycle stages.

e) The current inspection and test status of PES components should be clearly evident.

f) All modifications to the PES configuration should be under configuration control.

g) The PES configuration documentation should be retained in a manner which prevents degradation due to environmental effects.

Annex A
(informative)

Terms and concepts used in this International Standard

A.1 Programmable electronic system

A Programmable Electronic System (PES) in this context is any shipboard system based on one or more sets of Programmable Electronic (PE) devices that are connected to input devices and output devices for the purposes of implementing control, safety or monitoring. This wide definition corresponds to that in [IEC 61508-4] and is equivalent to the [MSC/CIRC.891] definition of a computer-based system. Operations and maintenance staff are not included in themselves, but requirements on them are, such as: manning levels, personal competencies, specific training needs, instructions/warnings for use and instructions for maintenance.

The PE element of the system includes any microelectronic device based on a central processing unit and associated memory. This includes devices such as a microprocessor, a minicomputer unit, a programmable logic controller (PLC) or the programmable electronics on a 'smart' sensor. Any number of PE elements may be present in the PES and they may exist at several places, for example in a distributed control system with network controllers and local PLCs.

The input/output elements comprise three main groups: those for human interface functions, those for external systems interface functions, and those for functions relating to the equipment under control (EUC). The elements for the equipment under control include all sensors and actuators and their associated communication paths to the PE elements. Similarly, the human interface elements comprise the input devices (keyboards, trackerballs, push buttons), output devices (VDU displays, mimic panels, warning lights, printers) and associated user documents and training. The third group is comprised of those interfaces to external systems communicating to the PES but not part of the EUC. These may be serial communication, wireless links or hard-wired inputs.

Finally, it is stressed that the documentation also forms part of the PES. This is particularly important for the software components of a PES. Documentation includes specifications as well as operating instructions or procedures.

Figure A.1 illustrates the scope of a PES in relation to its surroundings. The surrounding environment to the PES comprises its context of use. This includes the operations/maintenance staff, the EUC and external systems. Note that

a) the EUC and external systems may also be computer-based or contain components that are computer-based; and

b) power supplies and other utility supplies, e.g. air, are within the scope of the PES.

The PES definition given is the most general and comprehensive case. For a particular instance, the PES being developed or assessed may not include some of these elements. This may either be because they are not required, e.g. a simple PES may have no interfaces to external systems, or it may be because they are part of the installation but are excluded from the scope of supply or excluded from the assessment scope.

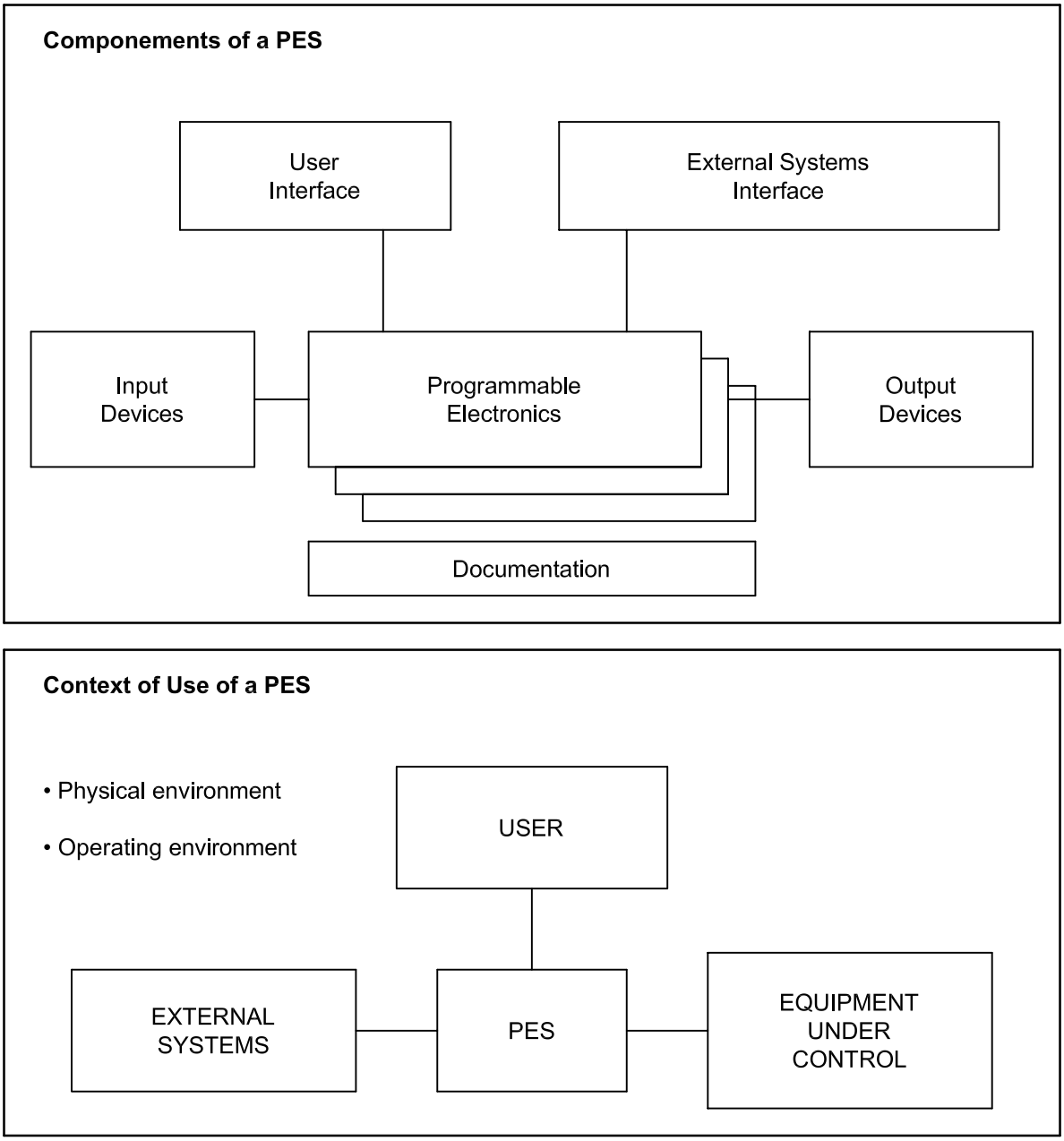

Figure A.1 — PES structure and boundaries

A.2 Context of use

Programmable electronic systems operate within a broader **total system** of equipment under control, other systems (external systems), the users of the system, the work being done by those users, a physical environment and an operating environment which includes the staff development and management systems for the ship. All of these components together (as shown in Figure A.2) achieve the business goal for the PES as intended by the operator of the ship. In order to achieve goals effectively and safely, the total system has to be designed as an integrated whole. During the life of a ship, the design of this total system will be spread amongst several interested parties and may change many times. The party responsibility for the dependability of the system and its components will also change.

To design, test or maintain a PES in a manner which will be cost-effective and safe, the PES developer and/or owner should be aware of the effect of the other elements in the total system which affect the design of the

functions and behaviour of the PES, its devices and its interfaces. A convenient way of summarizing all the other elements of the total system is as a statement of the **context of use** of the PES.

It is convenient to divide the context of use of a PES into the following elements (taking the example of the automatic control of track and speed) that is the

a) hardware and software infrastructure in which the PES is to operate (for example, details of networked industrial PCs running Windows XP),

b) systems with which the PES has to exchange data and commands (for example, details formats and protocols, of the navigation and engine control software),

c) physical environment in which the PES is to operate (for example, bridge and engine room, lighting, noise and vibration levels, humidity and temperature),

d) characteristics of the intended end-users (their skills, training, physical abilities, level of responsibility, etc.) (for example, STCW95 deck officers with one year's experience on Windows and recent courses on use of the navigation and engine management systems),

e) tasks the end-users are to perform, including maintenance of the PES (for example, determine voyage, set and change way points, override system), and

f) organizational and social environment in which the users are to use the PES (for example, type of ship, crew complement, applicable port state legislation, special notations and certificates, incentive structures, safety management procedures).

When assessing the risk associated with a PES, all aspects of the total system should be taken into account. Risks cannot be described unless the tasks of the users and their effect on the ship and its mission are known. In particular, if there is to be closed-loop control (where hardware or software takes action and the user may supervise after the event, e.g. machinery control) or open-loop control (where the user takes executive action based on information received, e.g. navigation). The latter type is frequently called man-in-the-loop control and requires the likelihood of the user taking the correction action to be included in the risk assessment.

When testing a PES, the context of use should be taken into account and the differences between the context of use and the context of evaluation should be taken into account when assessing the results of any tests. The context of evaluation during a factory acceptance test is obviously further from the context of use than that for the sea trials. However, even sea trials may not take account of day-to-day system requirements, configurations and the behaviour of typical users.

The providers of COTS products (such as PLCs or operating systems) may not find it possible to define the context of use of their generic products in full. In this case a generic context of use that identifies the potential diversity of each element may be defined. A generic context of use is not acceptable for the design and testing of specific PES for use in a particular ship or for particular shipboard applications.

A document specifying the context of use provides useful guidance to the designers of a PES on how and where the PES will be used. The specification of the context of use is the main reference document for usability engineers when planning tests of the system and when selecting users for these tests.

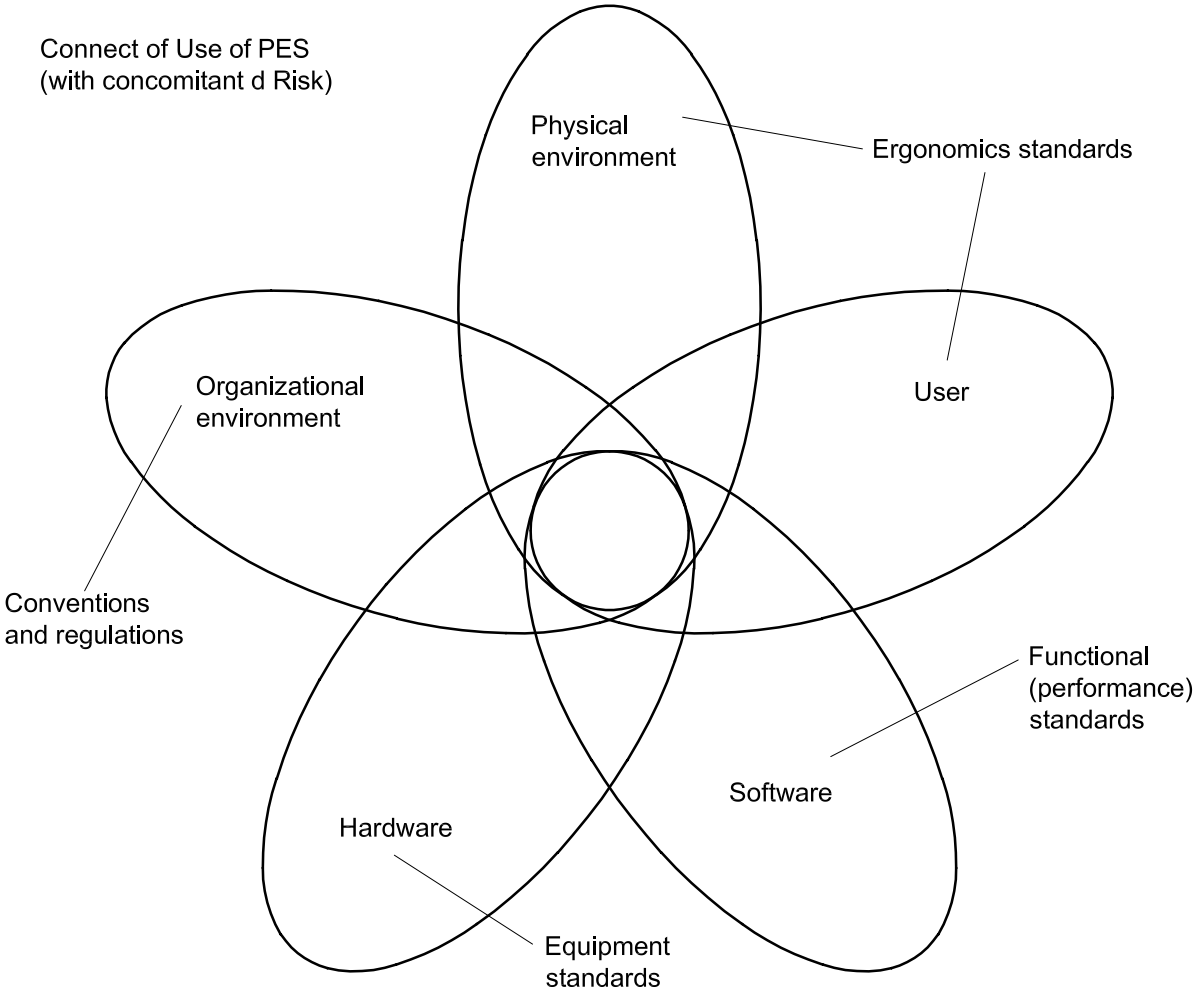

Figure A.2 — Components of the total system and related standards

A.3 Risk assessment

It may be possible with an uncontrolled development process to produce a safe system. However, the probability of this occurring is relatively small and there is inherent risk in depending upon that outcome. For a PES that does not provide any business or safety functions (e.g. a crew or passenger entertainment system), such a low level of assurance may be acceptable. In the marine sector, most PES onboard ships fulfil mission- or safety-related functions and will therefore have an impact, to greater or lesser degree, on ship safety. For these PES, a higher degree of assurance of dependability is needed.

The standards behind the guidance presented in this International Standard provide detailed descriptions of measures and techniques to provide specified levels of assurance for all aspects of a PES. Each PES in an integrated ship environment is operating within a specific context of use and as such it is necessary to assess the level of risk associated with each particular PES. This allows an appropriate development life cycle to be defined and followed in order to provide the needed assurance that the PES will behave dependably.

For a lower-risk PES, the controls applied, the level of V&V, the development measures and techniques that are necessary will be less rigorous than for PES whose operation presents a higher risk to the ship, the crew or the environment. Typical examples of higher-risk systems may include control systems for propulsion and steering, PES used for navigation or communications, loading instruments, fire detection systems and alarm systems. Examples of lower-risk PES may include passenger information systems or hotel management software. The actual risk posed by a particular PES depends upon its specific context of use and the hazards involved. General risk classifications may not be valid where new hazards or combinations of hazards are present.

A.4 Systems engineering

The goal of system engineering is to deliver a desired **operational capability** to the owner. For complex, computer-based products, effort spent on mass-production and distribution make little difference to the traditional supplier's target of time to market. The real objectives are timely delivery and continued support of the right operational capability. Supplying a better service and shortening the development time depends on efficiency and effectiveness in defining and checking both the requirements and the design. Capturing and organizing requirements is one of the main tasks of systems engineering, since requirements act as a reference point for what the users need and good system requirements are the foundation for any dependable product. Like all foundations, requirements call for early work in return for later benefits. Throughout development and operational life, informed trade-offs and compromises are needed to safely reconcile requirements with what is feasible. Even on one-off developments, lessons are learnt which can be applied to the next project.

Systems engineering provides a set of concepts and processes for the management of risk in the definition of complex systems, through decomposition into defined and realizable components with specified interfaces. It bridges the abstract, early stages of a project and the precise detail of implementation. It establishes what is feasible and creates the architecture for the system to be produced, allocating functions to components (hardware, software and users) to give the most effective, efficient and safe system and life cycle, achieving the optimum balance between identified qualities, costs and risks by trading off attributes between components. Each component is developed as an entity, both coherent in itself and cohesive with the system, fitting within the overall design framework. The components are integrated into a complete system and their operation as a system is analysed for emerging changes to the requirements.

Systems engineering handles the whole life cycle in a balanced way. At all times, it involves trade-offs between the competing factors of performance, risk and cost. It ensures that designs are practicable and also meet the user requirements. A holistic approach is used, without bias towards specific sub-systems or technology. A system engineer continuously reviews the development for risk from end-to-end, confirming decisions only when the risks are acceptable. At each process boundary, a review or a test allows progress to be monitored and a commitment made to the next stage. These boundaries act as quality milestones, controlling the gradual transformation from a high-risk idea into a complete product. The life cycle defines the order in which information must be produced. Although a simple, sequential life cycle is a logical way of expressing many core concepts about development, it is not practical for systems engineering of large-scale, realistic systems. Before committing to a project, an organization needs to be sure that it is affordable, technically feasible and acceptably safe, as well as providing users with the quality that they need. While quality is dependent on user requirements, we need to understand the design in order to obtain realistic values of cost and risk. System engineering cycles (“iterates”) through requirements and design until a consistent, practical compromise can be reached.

Systems engineering is different from specialist disciplines, such as mechanical engineering or training. Technical coordination is a core element of its work. Each specialist discipline tends to think that a development will work only if it follows the philosophy of its own discipline. Systems engineering provides the framework for the work of all disciplines, remaining independent of discipline and product type. It translates user needs into technical issues and then negotiates with project management about the cost and schedule impacts. It depends on communication across the disparate groups and organizations involved in a development. It is not a role for a specialist group of people, but a small part of the work of every individual working in the project team.

System engineering has both managerial and technical aspects, since a single poor technical decision can have significant effects on a product, or even a company. Systems engineering always defines the requirements and creates the architecture. Project management has a wider but intrinsically less creative role. Its prime function is to ensure that everything is done, but not necessarily to do it. Project management without system engineering is meaningless, since successful management requires trade-off between variables such as cost, schedule, quality and performance. The technical components of this information are acquired by systems engineering. Because time and resources are easy to measure, management sometimes attempts to control projects without the key element of requirements. However, there is little point in meeting cost and budget targets without producing a useful product.

Annex B
(informative)

Guidance on the principles for marine PES

B.1 Introduction

The guidance in this annex is in the form of commentary to explain each principle in the marine context. General commentary on the background to the principle is followed by specific guidance which explains or elaborates upon interpretations of the principle for particular types of PES, stage in the development process or role in the life cycle of the PES. The guidance is supported by references to the relevant parts of standards, codes and guides in which more detailed requirements may be found.

The intention of this annex is to provide clarification of the principles for the wide range of readers of this document. Criteria for the achievement of each principle are listed in Clause 7. These should be studied prior to reference to this annex. Further detail in support of the principles and criteria, or descriptions of particular requirements and procedures may be found in the referenced standards. Full references to these standards can be found in the Bibliography.

B.2 Intention

B.2.1 General

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

B.2.2 Commentary

The need to provide objective evidence of conformance to the principles is expressed in this intention. How this is done is not prescribed because there are many ways to present a clearly argued case which demonstrates conformance. Some of the major sources of evidence may include specifications, design documentation, results of analyses and tests, service history experience, procedures and work instructions, existing certifications, appeal to custom and practice in the marine sector, and the physical characteristics of the PES itself.

The intention emphasizes the need for the PES to provide appropriate behaviour. This is both in external communications to operators and other systems as well as in direct task functions. Attention to this behaviour throughout the life cycle is required, whether through controlling requirements creep, evaluating the scope for operator error in using the PES, or in careful implementation of modifications under maintenance conditions.

The philosophy of the standard is that the overall intention and all of the subordinate principles apply to the PES, and the total system within which it operates throughout its life. It should be read and interpreted in this context. It will be found that the principles interact and support each other when applied in this way. **There is no ordering or priority between the principles or the assessment criteria.**

All principles apply to the whole PES throughout its life. All criteria are intended to apply throughout the life of any PES, but may be interpreted to different degrees depending on the stage in the life cycle, the type of system and the required level of integrity.

Similarly, all principles apply to all types of PES. Although this is well understood for bespoke PES developments, it may not be for COTS PES or for PES built from COTS components. To demonstrate suitability within the defined context of use, COTS PES should still meet each of the principles. This may be particularly challenging for the supplier of standalone COTS, which can have very wide application, or for a system integrator or systems engineer who may have to demonstrate the overall dependability of a PES comprising many disparate COTS products.

B.2.3 Specific guidance

The requirement to consider the risk associated with the operation of any particular PES is part of correct operation. This is made clear in the first principle.

When using a PES, a user will perform two levels of task — first, the ship operation(s) supported or mediated by the PES and the equipment under control; second, the extra task of using the PES itself. A clear distinction should be made between these two activities when defining requirements for, designing or testing the PES. The general intention is to make the ship's operation as effective and safe as possible by designing the use of the PES to place the smallest additional mental or physical workload on the operator.

B.3 Safety

B.3.1 First principle

B.3.1.1 General

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

B.3.1.2 Commentary

This is the general requirement for the safety of marine PES. The acceptable safety levels against which the risk is justified are determined case by case using, as a reference, the methods and measures proposed by IMO or those that reflect the best current practice in the marine sector.

Analysing and evaluating risk can only be sensibly accomplished within a specific context of use for the PES. This context should be clearly defined and understood by all involved parties. The evaluation of risk should ensure that reasonably foreseeable misuse of the PES is taken into account, as well as the evaluation of normal usage. Any novel or unusual features of the PES may themselves pose specific hazards and will need careful attention.

A key aspect of this principle is that hazards associated with the PES are known and understood. This includes both the intrinsic hazards arising from the physical properties of the PES and hazards arising from its functional behaviour. Risk reduction features external to the PES can be used to ensure safety levels are acceptable. These may include warning notices, issuing personal protective equipment to users, working to create special procedures or training for use.

The analysis and evaluation of risk should include each element of the PES. This is because each element has its own level of risk that should be determined and minimized (or eliminated altogether) when it is used in the construction of the PES. The external risk reduction features noted above may also be needed for elements of the PES.

B.3.1.3 Specific guidance

All involved parties have obligations in respect of this principle, but these may vary widely depending upon the PES, its context of use and the responsibilities for its development, supply and maintenance.

For example, the owner or operator should address top-level hazards in respect of the overall ship and its major systems. This also includes the provision of risk reduction measures external to the PES. Suppliers

should demonstrate that they have supplied equipment that is physically safe, that the safety implications of using the equipment are clear and that its failure behaviour is understood. This can be difficult in some cases. For example, for a general purpose COTS product which is not specifically developed for safety-related applications. Procurers should make clear whether the intended application is safety-related and, where this is not done, the procurer should request such information.

Foreseeable misuse of the PES should be taken into account in addressing safety. This again requires systematic analysis, possibly including in-service experience of the PES or of similar PES. Misuse covers a variety of situations. For example, a PES may be type-approved to be suitable for general marine applications but not for installation on reciprocating machinery. If vibrations can cause the PES to fail to an unsafe state, then the risk associated with such installation may need to be assessed. To take another example, if the output from a positioning system is meant to be cross-checked with data from other systems before use, the possibility that the manual cross-check may not be made should be considered. In some circumstances, for example warships, the degree of misuse that the system has to tolerate may be large and the definition of unacceptable will require careful interpretation.

The principle implies that the safety requirements (for example the SIL) for the PES and its components should be determined and used to manage the degree of V&V for the PES. In particular, suppliers of COTS products will need to determine a target SIL that is appropriate for the intended application or set of applications. It may be effective for a supplier to have a range of otherwise similar products that are assessed to different levels of integrity and hence are appropriate for different applications.

The guidance in this International Standard only provides advice for level of integrity, i.e. it discusses only “high”- and/or “low”- risk PES and does not give specific guidance for individual SILs. Such detailed guidance is found in the referenced standards, in particular in the table of measures and techniques in [IEC 61508-1], [IEC 61508-2] and [IEC 61508-3].

B.3.1.4 Source references

[IEC 61069-1] §4.3.6, §4.3.7, [IEC 61508-1] §7.4, §7.5.2.2, [MSC/CIRC.891] §3.1.1, §4.1.2, §4.7

B.3.2 Second principle

B.3.2.1 General

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

B.3.2.2 Commentary

This requirement is concerned with failures where the PES ceases to provide the required functions. This can result from major faults within the PES or due to operational or environmental conditions outside its design envelope. In either case, the PES should move to a defined state that minimizes risk for the prevailing conditions and the equipment being controlled or monitored. There is a need to ensure that dangerous failures are suitably detected and handled appropriately. The degree and scope of such measures will depend upon the interpretation of “dangerous” as identified through the risk level of the PES.

The need here is for careful consideration at all relevant levels, including the whole ship, of failure scenarios and their concomitant hazards. The appropriate safe condition for the PES to revert to may be quite complex to determine because it may be different under different environmental or operational conditions. Since the scope of this International Standard is a single PES, the state of other systems in the event of failure of the PES is addressed by P1.

Movement to a safe state may be achieved by automatic or manual means as appropriate. Automatic actions such as independent, hard-wired, emergency stops or programmed shutdowns are commonly used and are appropriate for many situations, for example where rapid response is needed to a well-defined failure mode. Movement to a safe state can also be achieved through manual means, but for high-risk PES there should be evidence of a careful assessment of the reliability of such means with respect to the criticality of the hazard. In all cases, the manual response actions required to move a PES into a safe state should be clear to users.

B.3.2.3 Specific guidance

As an example, the shutdown condition may not always be the least hazardous condition for certain failure modes. Where considered necessary, it may be safer to maintain propulsion and continue running an engine with low lubrication oil pressure, despite the risk of engine damage. Conversely, due to the risk of catastrophic damage, a shutdown would always be necessary when an overspeed situation is detected. This boundary is flexible in cases such as warship systems, where reversionary modes of operation are required even when the level of risk from continued operation is high. The context of use and task requirements for the PES (particularly the third and eighth principles) will provide guidance on the particular trade-offs for the specific application and the type of design necessary to satisfy this and the other product principles (particularly the fifth principle).

Analyses and tests at all levels can provide useful evidence against this principle. An owner or yard should ensure that, as far as possible, realistic scenarios are considered and evaluated or tested at the overall ship level. For example, during manoeuvring, engine shutdowns are undesirable. A component supplier would need to demonstrate that failure modes for the component are known, such that their effects on the PES behaviour can be determined. In-service history data, for example in the form of problem reports, may provide similar evidence in demonstrating that failures resulted in safe conditions or successful protective actions.

One means of ensuring that users are always able to react appropriately to maintain a safe environment is to include a fault list in the system documentation. This list specifies the different failures that the PES may exhibit, including the worst conditions of work and which states are the least hazardous.

B.3.2.4 Source references

[IEC 61069-1] §4.3.6, [IEC 61508-7] Annex B and Annex C, [MSC/CIRC.891] §4.7.1, §4.7.2, §4.8.4

B.4 Functionality

B.4.1 Third principle

B.4.1.1 General

P3 The PES shall provide functions which meet user needs.

B.4.1.2 Commentary

In this context, the user is not just the immediate operating personnel, but any party (stakeholder) affected by the PES during any part of its life cycle. This includes, for example, ship owners, installation staff and maintenance personnel.

User needs can be both explicit and implicit. They are requirements which cover all functional aspects of the PES. For example, for a protection system, this may involve specific safety functions. Furthermore, it is important to understand that these needs may change during the life of the PES. For example, an existing system may be enhanced to provide change of use. A clear means of demonstrating user acceptance should be available.

This principle focuses on “what” the PES does rather than the non-functional “how” it does it. There is a need to define the operating envelope of the PES, since functions cannot be provided under all possible conditions and circumstances. However, appropriate functions may still need to be provided under abnormal operating conditions and a degree of user selection of functions may be needed.

Users have particular abilities and skills. Some of these characteristics are broadly the same for all humans, some depend on a variety of factors such as size, age, culture, level of stress, degree of fatigue, the operational environment, experience and training. Providing functions which are designed to fit these (possibly dynamic) user characteristics is one of the user needs for the PES.

B.4.1.3 Specific guidance

The characteristics of the users and their base level of expertise in using the system will need to be specified or assumed. This helps to determine the need for individualization or learning features provided by the PES. However, the application and the complexity of the PES should also be considered. For example, a local monitoring panel of an alarm system may be usable without any tailoring by engine-room operators; however, a menu-driven graphical VDU interface in a centralized system for alarm display and acceptance may require specific training as well as the provision of on-line help facilities.

It is helpful to record a description of users, tasks, operating environment and computer environment in a single document which is part of the requirements for the system. Such a document is called the context of use statement or context of use.

For systems which support or exactly replace traditional systems, general knowledge about the functions to be supported may suffice as a basis of design. For new operational concepts or new technology, modelling and analysis of intended user activities in order to elicit the requirements for the PES would be expected.

The responsibility to define functions lies with the owner. The responsibility to refine the description of functions and to analyse the cost and practicality of delivering these functions lies with the systems engineer. The role of systems engineer therefore needs to be defined and allocated early in the life cycle. The role of systems engineer is not limited to ensuring that equipment can be interconnected.

B.4.1.4 Source references

[IEC 61069-1] §4.3.2, §4.3.4, §4.3.5, §4.3.6, §4.3.7, [MSC/CIRC.891] §5.2.1, §5.4.2, §6.4, [ISO 9126-1] §6.1, [ISO 9241-10] §3.1.1, §3.2, §3.7, §3.8

B.4.2 Fourth principle

B.4.2.1 General

P4 Functions shall be appropriately allocated between users and PES.

B.4.2.2 Commentary

Careful consideration should be given to this allocation. Automation of some tasks, although possible, may not be desirable in the overall system context. Tasks that may be suitable for automation include, for example, those that require response rates greater than human reaction times, those that require large amounts of repetitive sorting or organizing of data and tasks that pose direct contact hazards to humans (e.g. work with toxic materials or hot surfaces).

One key aspect is that the set of user tasks should not just be those left over after automating as many as possible, with the expectation that the flexibility of the user will make the PES work overall. The set of user tasks should form a meaningful job, with special attention to safety-related functions (such as alarm acceptance or protective shutdowns) and their achievement under stress conditions. A hazard analysis may be used to determine if tasks should be left to the operator. For example, those tasks which are safety-critical and whose successful performance could be jeopardized by PES failures. In this case, adequate means to verify successful performance of the task should be provided.

The functions allocated to users need to be combined into well-balanced tasks which address the issues of physical workload (too many things to do) and mental workload (too much to think about). Well-designed tasks give the user the best chance to make the primary contribution to the efficient and safe operation of the ship. Well-designed tasks have a mixture of activities for each user which minimize boredom, fatigue and excessive workload and offer opportunities for learning. Typical types of activity include simple routines, expertise or rule-based work, and more complex activities which require problem-solving or analytical effort. Long-term focus on one type of activity should be avoided if possible. Good task design requires early collaboration between the operators, the designers and the integrator of the PES.

B.4.2.3 Specific guidance

As an example of function allocation, manual control of the oxygen level in the outflow from an inert gas generator may not be appropriate, given the protracted time period that operator attention is needed.

Safety functions such as the confirmation of release of carbon dioxide from a fire-extinguishing system has to be a manual function, because an automated system will not have information about the presence of crew in the flooded space.

The base level of user expertise should be specified and taken into account. For operators, the existence and provision of that expertise on board the ship needs to be realistically assessed. For suppliers, the possibility of inadequately trained users may help advise the allocation of functions. There are existing approaches for defining base expertise, such as national schemes for certification of competency. IMO initiatives, such as the ISM code and STCW95, help to focus attention in this area.

When selecting COTS products, the purchaser should ensure either that their required allocation of function matches with the designed allocation of function within the COTS product, or develop procedures for operation which take account of the designed allocation of function.

The operational philosophy and the resulting allocation of functions between the technology and the user should be assessed throughout the operational life of the ship. This should be based on longer-term studies as well as testing and initial trials. PES can be designed to allow some degree of flexibility to accommodate re-allocation. Remedial user training or extension of user help facilities may also be considered. See the commentary on the fourteenth and nineteenth principles (B.8.3 and B.9.4) regarding the competence of users with respect to new technology and operational concepts.

The role of adequate feedback and explanation to the user should be taken into account in helping to meet this principle. See 7.2.9 e).

B.4.2.4 Source references

[IEC 61069-1] §4.3.2, [MSC/CIRC.891] §3.1.2, §4.8.3, [ISO 13407] §5.3, [ISO 9241-10] §3.2

B.5 Performance and dependability

B.5.1 Fifth principle

B.5.1.1 General

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

B.5.1.2 Commentary

This principle is concerned with problems occurring within the PES, where the PES is still able to provide some or all of the required functions. For severe or catastrophic failures, the second principle is more relevant (this requires the PES to move to or remain in a safe condition).

This principle should not be taken to mean that the PES must continue to provide all functions under all internal fault conditions or for all abnormal inputs. Fault tolerance is the ability to provide or maintain (required) functions in the presence of specified fault conditions. This includes user mistakes or errors in data from other systems connected to the PES and also environmental anomalies or even physical damage.

Tolerant actions may be automatic or may be manual, i.e. requiring user intervention to achieve the desired actions. In the latter case, the user needs to be made aware that action is required. The integrity of tolerant actions is frequently achieved through the use of duplicated or redundant elements in the design of the total system.

Particular care should be taken to ensure that safety-related functions have adequate independence. This means ensuring that explicit protective functions or general control functions with dangerous failure modes are not affected by failures in other non-safety-related functions or equipment. There are several ways this can be demonstrated. It may include, for example, physical separation of equipment; use of diverse technologies; sharing only common parts or services whose failures will not be dangerous; or provision of separate operational, maintenance or test procedures.

B.5.1.3 Specific guidance

Low-level components of a PES, for example communications protocols, correct errors in input as part of their normal operation. In this case, the user is usually informed only when design parameters have been exceeded. At “higher” levels in the PES (levels nearer to command or control input where error is a less usual event), faults and errors should be brought to the attention of the user.

The user should be made aware of mistakes in inputs, even in situations where the PES has corrected the error, for example where an out-of-bounds input has been detected. This is to maintain the users' awareness of the situation and assist in avoiding future input errors.

If the PES can provide a large list of simultaneous or near-simultaneous faults, the presentation of error information to the user should be designed to minimize the risk of “user overload”. This situation is most likely to occur where a PES has a capacity for dealing with a large quantity of information and issues. In such cases, a function that prioritizes the scale or sequence of faults may be useful, or indeed necessary.

High-level COTS PES will have been designed to support a particular approach to user control. When selecting such products, the purchaser should provide user training to ensure that the intended approach to control matches the approach of the COTS product.

B.5.1.4 Source references

[IEC 61069-1] §4.3.4, §4.3.6, [MSC/CIRC.891] §4.1.1, §4.3, §4.6, §4.7, §4.8, §5.3.3, [IEC 61508-2] §7.4.6.1

[IEC 61508-7] Annex B and Annex C, [ISO 9241-10] §3.2, §3.6

B.5.2 Sixth principle

B.5.2.1 General

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

B.5.2.2 Commentary

This principle focuses on the performance of the PES in achieving its functions or “how” it achieves them. The key aspects include the following:

— *Specified levels*, meaning the performance requirements should be understood by all parties, typically through documented definitions of the levels or tolerances to be achieved. This may involve global targets, e.g. fluctuation targets for power supplies, or detailed levels, e.g. response times for critical alarms. In some cases, the acceptance criteria for levels may be by benchmark testing to set acceptable limits, e.g. for network or processor loading.

— *Specified operational and environmental conditions*, again means a common understanding of the context of use of the PES should be reached. These conditions may involve abnormal or failure conditions.

— *Maintain*, means the performance levels should be achieved for both the service life of the PES (i.e. maintained over time) and for changes in the prevailing conditions. It does not mean the performance level should be the same for all the specified conditions, but that the specified levels, which may be degraded, e.g. for high temperatures or in the event of a blackout, are actually achieved.

Special attention is needed to time-critical functions whether safety-related or those with significant operational implications. The timeliness of these functions in terms of response, duration and frequency should be clearly and precisely specified and demonstrably achieved.

Demonstration of achievement through testing includes careful treatment of the physical conditions actually used for the tests and how representative they are of actual conditions. Any extrapolations of performance into untested conditions should be carefully justified.

B.5.2.3 Specific guidance

In 7.2.6 b), the term “speed of response” means the speed of control response of the PES. This may not always be related to the speed of interaction with the user.

The possibility of saturation loading of networks should be evaluated carefully, especially the response and throughput rates for functions and data, both under conditions associated with high risk to the ship or crew, and under conditions where high network loading could be the cause of hazards. Examples include: several units disconnecting from and reconnecting to the network, common mode failures, cascade failures, responses to broadcast messages.

The correctness of date/time stamping functions should be achieved throughout the life of the PES. In particular, their performance in unusual situations needs to be assured, e.g. at leap day changes.

B.5.2.4 Source references

[IEC 61069-1] §4.3.2, §4.3.3, §4.3.4, §4.4, [MSC/CIRC.891] §3.1, §3.2, §5.2, [ISO 9126-1] §6.2 §6.4

B.5.3 Seventh principle

B.5.3.1 General

P7 Unauthorized access to the PES shall be prevented.

B.5.3.2 Commentary

A clear understanding of the security threats to the PES is needed and the appropriate countermeasures, whether physical or procedural, need to be implemented and effective. The typical issues to address include accidental or malicious operation of the PES. For software, this would also mean considering the ability to alter programs or data. Such threats may arise from external systems connected to the PES and not just the direct operator or user. Indeed, for marine systems, the software may not be accessible to the crew.

Although in general hardware equipment is more difficult to alter or reconfigure than software, appropriate measures should be in place to prevent such modifications or reconfiguration of the PES.

A range of measures is available and can be used as necessary, depending upon whether the PES is high-risk or low-risk. Ultimately, the sanction of authority is established through appropriate procedural means, but the key aspect of “permission” can be implemented through simple physical means such as passwords, virus-checking utilities or physical locking of equipment cubicles.

B.5.3.3 Specific guidance

For example, for suppliers the identification of authorized users for high-risk PES may be a useful technique. This may be done by listing names or by identifying grades/roles of personnel.

The effectiveness of security measures should be demonstrated and should include test results with specific security test cases, or service history records of successful operation with no security breaches.

B.5.3.4 Source references

[IEC 61069-1] §4.3.4, [MSC/CIRC.891] §3.1.6, §5.2.4

B.6 Operability

B.6.1 Eighth principle

B.6.1.1 General

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

B.6.1.2 Commentary

In order to be sure that a PES is operable, the usability of the system should be established with representative users performing realistic tasks in a context of evaluation which is closely related to the real context of use of the PES.

The level of assurance of usability will depend on the required level of dependability of the PES. For low-risk PES, an assessment by user representatives or usability experts against a standard list of usability criteria can be sufficient. For PES which are of greater significance to the operation of the ship tests by real users, a subjective debrief as to the quality of use of the system is recommended. For PES used in safety-related operations, quantitative measurements of user performance on key tasks in the exact context of use are recommended. The level of assurance of usability can be determined from the risks associated with the total system.

Measurements of usability should be made against targets derived from the safety and user requirements for the PES. Three broad classes of subjective or objective measurement are required: effectiveness, efficiency and acceptability. These parameters will be measured in different ways, depending on the particular functions performed by the system and the user's tasks. Typical measures include the understandability of information and accuracy and speed of user response. Acceptability is measured as the end users' satisfaction with their use of the system. When selecting tasks from which to take these measures, it is important to take account of the overall role of the PES and the concept of its use in operation and maintenance.

The performance required should be assessed for both normal and abnormal conditions. For unspecified conditions, the fifth principle applies to user behaviour just as much as to the software or hardware of the system.

The “user” here refers not only to the direct operators of the installed PES; it can include all prospective or actual end users of the system. This may include, for example, maintenance staff, owner management and different groups of operators.

B.6.1.3 Specific guidance

When developing a system that has to meet targets for usability, it is advisable to test early versions or prototypes with representative users in order to be sure that design solutions are sufficiently usable. In order to meet performance targets, the expected competence of, and range of competence in, users has to be taken into account during design. It is the responsibility of the owners to specify the intended competence of the crew and to initiate re-design if this changes during the life of the PES. The nineteenth principle addresses the issue of maintenance of required levels of competence.

In an ideal case, factory and sea trials of the usability of the PES should be performed with representatives from the crew(s) who will sail with the ship. In the worst, but more typical, case of evaluation with “expert users” and/or supplier representatives, the assessor should take account of the differences in training and experience between the trial subjects and a typical crew. This is best done in a formal way with lists derived from a defined context of evaluation.

User trials should include simulations of difficult situations for crew, such as emergency operation, extreme weather, high workload, night conditions (for bridge equipment) and partial failure of equipment. A common failure in testing is not to include conditions with low probability but with high impact.

COTS present a particular problem, because user trials are likely to have been made with users with very different experience or training. Claims of usability for COTS should therefore be treated with caution.

The owners are responsible for the definition and negotiation of usability requirements. The systems engineer is responsible for ensuring that the whole system meets these targets.

B.6.1.4 Source references

[IEC 61069-1] §4.3.5, [ISO 9126-1] §7, [MSC/CIRC.891] §3.1.5, §4.8.1, §5, §6, [ISO 9241-10] §3.1.1, §3.2 §3.3, §3.4, §3.5, §3.7, §3.8

B.6.2 Ninth principle

B.6.2.1 General

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

B.6.2.2 Commentary

PES for use in the marine environment generally support or perform a function related to the management or operation of a ship. Knowledge of the operation of the ship gives the crew who use the PES certain expectations about the way in which the PES will assist them in carrying out their tasks. When these expectations are met, they will work more effectively and make fewer errors.

Lack of situational awareness is the most significant factor in human error. In monitoring or control tasks, PES which match user expectations for displays of information and dialogue with the system give the highest degree of situational awareness. The system should enable the user to

1) know what the system is doing,

2) know what it is going to do, and

3) explain the relationship between input and output.

Items 1-3 above cover different aspects of situational awareness. The design may need to address each aspect separately.

At a finer level of detail, it is important to ensure that information and other codes (such as messages, symbols, abbreviations and colours), system navigation activities (such as moving from screen to screen, getting help, menus, buttons and keys), and the issuing of commands (such as selection, control actions, confirmations and undo) behave in the same way both within and across systems. Inconsistencies between these items at best slow the use of any PES and at worst can lead to errors resulting in unsafe operation.

B.6.2.3 Specific guidance

During the early phase of PES development, it is important to define and specify the operational concept which the PES will present to the user. An operational concept based on behaviours familiar to the users, for example taken from the performance of mechanical systems in earlier ships or taken from other PES or from general stereotypes, will be easier to learn and will support the user in predicting the response of the PES in abnormal conditions. For example, the users of high-risk PES, such as alarm and manoeuvring systems, need to be able to explain the relationship between input and output for the total system of PES, equipment and ship.

During the development phase, it is important to follow general ergonomics standards and specific project style guides for the look and feel of the interface and the functions of the system in order to ensure consistency. It is also important to ensure consistency of the detail of the implementation to the operational concept for the total system.

The implementation of measures to detect and correct for faults should take account of the required integrity of the PES and its context of use. A range of techniques is available with varying degrees of coverage of faults. The design implications of specific techniques will need to be investigated, especially with scaling effects with larger PES where fault coverage may be provided at several levels.

When integrating PES in a new building, or introducing new systems into an existing ship, inconsistency between PES should be avoided. This reduces learning effort and avoids user errors arising from misinterpretation of information or performance of a command sequence from one system on a system where it has possibly unsafe consequences.

During operational use of PES, it is important to maintain consistency of behaviour and look and feel through upgrades or other changes to a system, unless, of course, the change is to remove aspects of a system which are found to be inoperable.

When decommissioning a PES, it is useful to document the successful aspects of the system for use in specifying new or replacement systems.

B.6.2.4 Source references

[IEC 61069-1] §4.3.5, [ISO 9126-1] §6.3, [MSC/CIRC.891] §5.1, §5.2, §5.3, §5.4, §6, [ISO 9241-10] §3.3, §3.5

B.6.3 Tenth principle

B.6.3.1 General

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

B.6.3.2 Commentary

Users of PES in marine applications will differ in background, training and general ability with PES. There is a risk inherent in not allowing for these differences in the design of PES. PES may be misused, or not used at all, if there is insufficient flexibility for users to do their jobs. Design for adequate controllability is based on knowledge of the range of users, their training and skills, the range of tasks to be performed with the functions provided by the PES and the task performance requirements in terms of speed, accuracy and support.

Interpretation of “controllable by the user” should be done within the context of the task to be accomplished and the functions allocated to the user. Allowing the user to slow down the response of the PES or to limit the output so that critical information is hidden may not be appropriate. However, the user should not be dominated by the PES for tasks which are under the user's direct control. That is, the user should be able to manage interaction with the PES for such tasks. Any modification of safety-related commands or information in this way would require a reassessment of the integrity of the PES. The risks associated with inexperienced users should be considered in this respect.

B.6.3.3 Specific guidance

To aid controllability, PES consoles should incorporate ergonomic features such as adequate physical space for movement. The PES should be designed to guide each group of users through dialogues, make information accessible and provide redundant displays and controls were necessary.

Typical areas where flexibility is required are: level of feedback or explanation, re-entry to data entry sequences, alternative ways of gaining access to functions and level of information provided to the user, and ways of grouping items for common control actions. On occasion, different user groups may require different representations of information, such as graphical or textual display of equipment status. For example, some

users may need a message that details the way a particular pump is running; others will only need to see a change in a screen symbol.

In some cases, it may be necessary to design PES which can be semi-permanently customized by particular groups of users or even individual users. In these cases, there should always be a quick means to return the interface to a standard set-up, and non-standard set-ups should be protected by suitable access control. Checks should be made that customization does not allow the interface to be changed to such an extent that the safe operation of the ship is jeopardized. This can be a problem for complex control systems, such as a dynamic positioning system.

Group or personal configurations for safety-related systems are a potential source of risk, but allow users of different levels of experience to operate efficiently and also avoid the risks inherent in providing expert-level facilities to inexperienced or untrained users, where there is more risk of apparently routine actions causing different system actions. Such set-ups should be protected by access control. Changes to parameters should be recorded by the PES and made available on request.

B.6.3.4 Source references

[IEC 61069-1] §4.3.5, [EN 894-1] §4.3, [MSC/CIRC.891] §5.1, §5.2.2, [ISO 9241-10] §3.3, §3.4

B.7 Non-task-related properties

B.7.1 Eleventh principle

B.7.1.1 General

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

B.7.1.2 Commentary

A well-structured, modular design will assist in meeting this principle. The notion of loose coupling between modules in the PES can help, i.e. where modules are physically and functionally distinct from one another. This is particularly important for software components where such an approach will assist successful integration and controlled modification of the software.

Consideration should be given to the problem of adequate shipboard support to the PES when at sea, when specialist equipment and staff will not be readily available. There may be a need for an adequate supply of shipboard spares and appropriate training of engineering crew in maintenance of the PES.

The competence of crew to perform on-board maintenance and repair will need careful attention. Specific guidance should be given on repairs and on which components can be replaced and which require attention by the supplier's service staff.

B.7.1.3 Specific guidance

Modularization and effective modification are supported by a careful allocation of function between both the PES and other systems, and (at a lower level) the components (hardware, software and further sub-systems) from which the PES itself is constructed. This is achieved by hierarchical definition of the system architecture and iterative trading-off of requirements between system elements to achieve optimum design. Modules should be loosely coupled, but internally tightly cohesive to allow for ease of technology insertion and management of change. Interfaces between modules should be well documented.

Documentation and training should take account of routine and reasonably-foreseeable maintenance and, in the event of failure, should include sufficient advice to ensure adherence to the second principle.

The indication of faulty components can take many forms; the key issue is to match the level of indication to the replacement/repair approach. For example in a standalone I/O station or cubicle, it may be adequate to

indicate only which circuit board is faulty, rather than try to indicate which circuit or component(s) have failed. Local and remote indication may differ, for example by local LEDs and remote audible and VDU-based display. The competence of the crew to make changes or other investigative work will need careful attention, and provision of correct and suitable documentation (including procedures for installation, operation and maintenance) from the manufacturers.

B.7.1.4 Source references

[IEC 61069-1] §4.3.7, [ISO 9126-1] §6.5 §6.6, [MSC/CIRC.891] §3.2.2, §3.2.3, §4.4, §6.1, [ISO/IEC 15288] §5.5.4, §D

B.8 Life cycle activities

B.8.1 Twelfth principle

B.8.1.1 General

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

B.8.1.2 Commentary

The role of a life cycle for the engineering of systems is now well established and is being recognized in the marine sector. Although a life cycle covers all activities from cradle to grave of a PES, the importance of the specification phase is a particular aspect to be addressed by all parties.

The principle emphasizes that the life cycle to be followed should be defined and that it forms a methodical basis for developing, operating and maintaining the PES. The fundamental importance of planning to implement the life cycle effectively is also clear. Planning should cover all aspects that are relevant to the PES, including safety and quality issues, and should be achieved in a timely manner. Furthermore, plans should be "live" and revisited as necessary throughout the life cycle to ensure that re-planning is timely and effective.

The life cycle typically includes the following activities as appropriate: requirements definition and analysis, design, implementation, integration, verification, transition to use, validation, operation, maintenance and decommissioning. However, the role of support activities should also be defined. Support activities include: quality assurance, planning functions, configuration management and independent assessments.

Clearly planned and structured activities that are performed in a systematic manner contribute significantly to ensuring the PES is suitable for use. They facilitate audit and review activities, particularly those performed by independent parties, in providing assurance that the PES meets its requirements.

B.8.1.3 Specific guidance

This principle and the other life cycle principles are applicable to all organizations concerned with the dependability of the PES. Thus, other parties to the PES supplier, such as the owner, the ship operator and the yard, will need to consider their responsibilities and demonstrate a systematic, planned approach to selected activities.

The life cycle plans should include a specification for the integration of the total system. This plan should address not only the programme of activities and tests associated with bringing the PES into an operational state, but also the tests required to assess the compliance of the total system in its context of use with its concept, requirements and design intent. This includes all aspects of dependability for the PES, integrated with its users and its organizational and physical environment.

Prototyping is a widely used technique in computer-based systems development. Its primary use is as a tool to help investigate and validate PES requirements or preliminary design solutions. This role can be abused and prototype code is sometimes used in the delivered system. As such, it is particularly important to plan any prototyping activity carefully, so that the purpose and use of the prototype system is known and understood,

that the development controls to be applied are defined, and that the results of prototype testing are suitably reported.

B.8.1.4 Source references

[IEC 61069-1] §4.3, [MSC/CIRC.891] §3.3.1, [IEC 61508-1] §7.1 §7.8 §7.9, §7.16 §7.18 §8, [ISO 13407] §5 §7, [ISO 9001] §5.5 §5.6 §8, [ISO 15288] §5, [ISO/IEC 15288]

B.8.2 Thirteenth principle

B.8.2.1 General

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

B.8.2.2 Commentary

The basic approach should be risk-based, where hazards are identified, the associated risks assessed and, if necessary, risk-reduction measures taken to achieve an acceptable safety level which takes account of the particular technology, functions and context of use of the PES. Alternative approaches based on prescriptive safety requirements may, however, have been taken and retrospective assessments should take account of this. In these cases, it will be important to demonstrate that safety targets for the PES are known and understood and based on statutory requirements or best current practice in the marine sector. It will be important to obtain clear agreement on these targets and their acceptance by the involved organizations.

The range of possible activities is extensive. The justification of the safety level achieved could be argued from the results of analyses, calculations, expert consensus, phase verification activities and validation tests. This can include, for example, analysis of service history evidence or testing of certain components. In general, it is expected that only adherence to specific development and verification procedures can lead to confidence that the PES will meet the required level of integrity (see the specific guidance below). For PES in high-risk applications, the need to separate design, verification and validation responsibilities becomes important.

An independent assessment of the safety achieved is required by this principle. The level of independence, however, will depend upon the criticality of the PES application. For example, it may be appropriate to appoint an external third party assessor to evaluate a particularly high-risk PES with novel features or technologies. In other cases, the independence may come from within the same team, but from someone not involved in the development or modification of the PES itself. For PES used in non-safety-related functions, this principle will relate only to ensuring that the intrinsic hazards arising from the PES are adequately addressed.

A hazard and risk management description should be maintained throughout the life cycle. It is the principal means of documenting progress on the resolution of hazard/risk issues, and the scope of the activities described will depend upon the stage of the life cycle that has been reached.

B.8.2.3 Specific guidance

Re-assessment of the criticality of PES may be needed based on its actual in-service use and any subsequent modification, as this may affect the risk classification of the PES. Re-assessment will definitely be needed where the PES is being used outside its original intended use. Major modifications or retrofit programmes in particular should be carefully considered.

Safety requirements should be specified in terms of safety functions to be provided and the integrity required of each safety function. Such a safety specification can then be maintained by organization(s) responsible for operating and maintaining the PES.

Detailed guidance on development and verification procedures to be followed can be found in the referenced standards, in particular in the table of measures and techniques in IEC 61508-1, IEC 61508-2 and IEC 61508-3.

A ship's ISM certification information may provide evidence of control for some aspects of operational safety for the PES.

It is important to realize that the assessor's role is not to participate in design, test or verification activities, but to judge the level of safety achieved based on the evidence available. This may or not require detailed scrutiny of some development activities, depending upon such factors as the target safety level and the degree of control over development. An example is an installation and commissioning phase where a large number of modifications are being implemented under time pressures. Detailed scrutiny may be necessary, unless sufficient confidence has been established in the modification process.

B.8.2.4 Source references

[IEC 61508-1] §4.5, §4.6, §6.2, §7.4, §7.5, §7.6, §7.8, §7.16, §8, [ISO 9000-3] §7.3.2, §7.3.3

B.8.3 Fourteenth principle

B.8.3.1 General

P14 Human-centred activities shall be employed throughout the life cycle.

B.8.3.2 Commentary

The basic approach should take account of the needs of the end users of the PES. Being user-centred entails early and continued focus on the requirements of the people who are going to use the system throughout its life. This is achieved in different ways, depending on the stage in the life cycle.

In the concept phase of the PES, the way in which the technology and crew should combine as a total system should be considered. The impact on the crew performing the jobs which will be required in order to achieve system goals should be assessed by consultation with those already performing similar work. In the requirements phase, the context in which the system will be used and the business, task and system ergonomic requirements should be developed and verified with representative end users through the use of suitable demonstration and discussion methods. In the development phase, the user perspective should be taken account of through the use of existing human factors knowledge, such as relevant ergonomics standards, user representation in the design team and evaluation of partial and complete prototypes with typical end users. Feedback should be collected throughout the life of the system in order to verify that it is performing according to expectations and to check for problems which affect the efficiency, effectiveness or health and safety of the users.

When collecting input and feedback, it is important to ensure that information comes as directly as possible from the end users of the PES. In the ideal case, sufficient end users to avoid individual bias/preference are given hands-on experience of prototypes or similar systems, and their opinions collected in a structured manner. Advice may also be sought from “user representatives” of the various types often found in PES development projects, e.g. sales staff, purchasing officers, secondees to the project, project staff with prior experience at sea, etc., if they have relevant and up-to-date knowledge.

B.8.3.3 Specific guidance

Human-centred design addresses more than the physical and cognitive ergonomics of the PES. The health, safety and well-being of the seafarer, the effect of use and misuse of the PES on the safety of the ship, the number of people required to operate ship systems, their training and survival in the case of catastrophic failure of the ship or its systems, are all considered when human-system issues are addressed in design and operation. The integration of these issues into the broader design process is a large part of the human-centred design process.

Developers should take account of the user's viewpoint when analysing the needs for a PES and during the development of a PES.

Providers of PES components should address general ergonomics issues and as far as possible identify the systems in which their components may be used.

Those responsible for the integration of the system should include the tasks of the user in the design and testing of the total system. Rather than consider the crew as separate from the technology, systems engineers should design complete **worksystems** of technology, operating philosophy and competent crew to achieve mission goals with safety and efficiency.

Operators should be aware of the level of computer literacy in their crews and provide training to match skills to the technology provided. Because of the long life of a ship and many of its systems, there are likely to be changes in the type and experience of seafarers. In addition, changes in regulation may change crew responsibility (see principle seventeen). These changes need to be allowed for in the design of PES, either by revision of the design to match changing user competence and need, or through flexibility in the initial design.

Owners should monitor the performance of PES through occasional review of the opinions and/or performance of typical users. Such reviews are most useful when performed in the following cases: shortly after delivery or revision of systems, when taking on a new ship, in order to set a benchmark before major revisions, and after near-misses or incidents in which the PES may have been a contributing factor.

B.8.3.4 Source references

[ISO 13407] §5.2, §5.3, §5.4, §5.5, §7.3, §7.4, [ISO 9241-10] §3.1.1

B.8.4 Fifteenth principle

B.8.4.1 General

P15 Verification and validation activities shall be employed throughout the life cycle.

B.8.4.2 Commentary

Verification is particularly important for the software components of a PES, and a wide range of techniques is available. Although dynamic execution, i.e. testing, is universally applied, only a small subset of possible paths through the software is typically exercised. Further confidence in the correctness of the software can be gained by applying static techniques at a low level. Code walkthrough or inspections can be applied to software for low-risk PES, whilst for high-risk PES more rigorous techniques include detailed static code analysis or software fault-tree analysis. The independence of the verifier(s) should be clear, especially for inspection activities. For all verifications, there should be clear criteria for success, for example stating the expected results for each test case or citing a coding standard for code inspections.

For software validation, the role of modelling or simulation in providing key validation evidence should not be overlooked, since this usually allows a wider range of test scenarios to be explored. For example, network saturation conditions may not be achievable in a test situation and network response and throughput times under these conditions may have to be assessed from analysis or simulation. Similarly, the behaviour of high-risk PES may be demonstrated by analysing a Finite State Machine or Petri Net model of the software.

Specific verification of user requirements should be performed. This may include the preparation and evaluation of prototype designs, usability trials and evaluations and validation tests under realistic conditions with representative users. Information concerning the in-service performance of the PES during maritime operations should be collected.

B.8.4.3 Specific guidance

The required level of independence for a verifier will depend (as does the independence of the safety assessor outlined in B.8.2) upon the criticality of the PES application. It may be appropriate to appoint an Independent V&V (IV&V) team from an external department or even a separate organization to validate a particularly high risk. In other cases, for example code reviews of low-risk PES, sufficient assurance may be

gained from using program designers from the same team to review an individual's work or even using self-checking by the individual against a defined checklist.

For PES in operation, the usability may change with a new crew or if training is changed. There is a need to re-assess usability if major changes are made to any part of the total system. Conversely, the competence of new crews or crew members to use the PES to dependably discharge their responsibilities needs to be checked.

Information on the performance of PES during their life cycle should be collected and analysed by the operator and/or the producer of the PES. This information should address problems in use, for example failures or conflicts with other PES or tasks. The information should cover technical problems and usability or applicability problems from the user perspective.

B.8.4.4 Source references

[MSC/CIRC.891] §3.3.2, §7.1, §7.3, §7.4, [IEC 61508-1] §7.1, §7.14, §7.18, §9.1.2, [ISO 9126] §5, [ISO 13407] §5.4, §7.4.4, §7.5, [ISO 9000-3] §7.3.2, §7.3.1, §7.3.4, §7.3.5 §7.3.6 §7.5.1 §8, [ISO 9001] §7.2.2, §7.3.4, §7.4, §8, [ISO 9241-10]

B.9 Quality system

B.9.1 Sixteenth principle

B.9.1.1 General

P16 All parties involved in life cycle activities shall have and use a quality management system.

B.9.1.2 Commentary

A quality system is an important means of providing assurance that specified requirements have been met. It should be appropriate for the size and complexity of the organization concerned, and its scope should include those activities relevant to the PES. Key evidence here is that the quality system is defined, e.g. through documented procedures, and that it is effectively implemented, for example through the existence of quality records.

Systematic errors, either software or hardware, during design as well as manufacturing, are minimized to an acceptable level through activities managed by the use of a quality management system. Quality activities should be defined in a quality plan. The level of detail and complexity of quality management activities should be a function of the required integrity for the PES under development. The plan should make clear how the quality system requirements are to be applied for the specific PES.

This principle is applicable to all parties involved in the PES. This extends to supporting organizations such as safety management organizations, in-service maintenance providers, and to sub-contract suppliers of products or services.

B.9.1.3 Specific guidance

The inherent complexity of software makes its behaviour difficult to assure by traditional methods based on test results alone. Although highly complex, layered, networked PES based on COTS products may exhibit failures which appear to be random (as a result of communication errors, version incompatibilities, dynamic configuration effects, etc.), software is not subject to random failure but only systematic failure due to design faults. Evidence of fault avoidance through a systematic process of design and construction is therefore particularly relevant to software components. A quality system is the key element to providing such evidence. Specific guidance on quality assurance activities and techniques for software is contained in the referenced standards.

Quality system certification by accredited assessment bodies is widely used and can form suitable evidence against this principle. However, the scope of the certification should be relevant and the quality system should be actually applied to the PES in question.

An often overlooked aspect of quality systems is preventive actions based on statistical data to feedback lessons learnt from earlier iterations through life cycle phases. Although such actions usually have longer-term intent, they can be effectively used to improve the development, production or maintenance of a specific PES. For example, an analysis of defects found during unit testing may highlight weaknesses in the requirements specification phase or in the design review process. These weaknesses could be addressed before the phases are revisited when implementing modifications.

B.9.1.4 Source references

[IEC 61069-1] §4.3.7, [IEC 61508-1] §4.1, §7.1.3.2, [ISO 9000-3] §4.1 §5 §6, [ISO 9001] §4 §5 §6, [ISO 9241-10]

B.9.2 Seventeenth principle

B.9.2.1 General

P17 Existing requirements for marine systems shall be taken into account throughout the life cycle.

B.9.2.2 Commentary

A range of existing requirements can apply to any particular marine PES. These include legislative requirements at the international and national levels, e.g. SOLAS and STCW conventions. The applicability of specific technical requirements for classification purposes also needs to be considered, and Societies' Rules and Regulations are publicly available for use or reference.

A further source of requirements is application-specific standards published at national or international levels. These may include both application-related requirements, such as the specific functions to be provided, as well as technology-related requirements, such as measures to assure that PES components are suitable for use. For example, the special requirements for navigation and communication equipment are defined in IEC 60945.

It should be demonstrated with traceable evidence which standards, regulative or legislative requirements are to be met by the PES, and it should be clearly defined if conformance is required. This is particularly important since conformance to such requirements may be subject to certification by external bodies.

B.9.2.3 Specific guidance

The applicability and importance of the different marine requirements will vary depending upon the specific organization involved. For example, a ship owner or a yard will give special attention to legislation (such as SOLAS) covering the PES in its context of use, especially where significant operational impact is expected. Similarly, STCW may effectively place specific requirements on the relationship between the user and some types of PES. For a supplier, the range of existing or draft technical standards, such as IEC 61209, IEC 61162 and IEC 60092-504, may be more important.

Existing certifications or reports that are relevant to the PES can form useful evidence against this principle through the independent assurance they provide. This can include certifications for type approval purposes or for quality management system approval, as well as reports from one-off analyses or studies. Conformance to relevant national legislation, for example EU directives, may also be considered. Some regulatory requirements change with time. The design of the PES may need to allow for change to retain compliance.

B.9.2.4 Source references

[IEC 61069-1] §4.3.7, [IEC 61508-1] §7.2.2.4, §7.4.2.9, [ISO 13407] §7.2, §8

B.9.3 Eighteenth principle

B.9.3.1 General

P18 Suitable documentation shall be produced to ensure that all PES life cycle activities can be performed effectively.

B.9.3.2 Commentary

Each phase of the PES life cycle should be characterized by means of “entry” and “exit” criteria. Suitable documentation should be produced within each phase in accordance with a plan of submissions. The documentation should demonstrate the fulfilment of the entry/exit criteria, with particular emphasis on functional, operational, safety and quality requirements.

This principle also requires the production and retention of suitable records of life cycle activities. These should demonstrate the successful achievement of such activities, in particular of those related to assuring safety and quality of the PES.

This principle is particularly important to software components, due to their intangible nature. Software is normally viewed as merely the source code or its equivalent. However, the ISO definition of software (see 4.10) is wider than this and includes all associated documentation, such as design descriptions, user manuals, etc.

Software has no physical properties, so it is the description and demonstration of functional behaviour that is crucial. In this respect, it is important, especially for high-risk PES, to achieve clear traceability between documents. This could be, for example, between different levels of design description or from validation test cases to specific requirements clauses. For the purpose of tracing requirements, it is recommended to establish a requirements tracking system, which relates every PES requirement to the documentation in which it is addressed, throughout the PES life cycle.

B.9.3.3 Specific guidance

The nature of software makes its behaviour difficult to assure by traditional methods based on test results alone. Documentary evidence of a systematic process of design and construction is therefore particularly relevant to software components. For example, the existence of a complete and traceable set of design descriptions would be an important body of evidence, but these should be supported with suitable verification records showing an effective process of production.

The documentation responsibilities of the organizations involved need to be clear, especially with regard to how handover through the supply chain will be accomplished. For example, during in-service support and/or modification after delivery and commissioning.

Although other principles cover requirements for operation, maintenance and configuration control activities, it is this principle that governs the need to update related documents, to keep change records and to record the results of re-testing following changes.

A checklist for the main PES life cycle documents is given in Annex D.

B.9.3.4 Source references

[IEC 61069-1] §4.3.5, [MSC/CIRC.891] §3.3, §5.1, [IEC 61508-1] §7.1, §7.4, §7.5, §7.14, §7.18, §8.2, §9, [ISO 13407] §7.4, §7.5, [ISO 9001] §7.3, §5.5.7

B.9.4 Nineteenth principle

B.9.4.1 General

P19 Persons who have responsibilities for any life cycle activities shall be competent to discharge those responsibilities.

B.9.4.2 Commentary

This is generally a well-understood area. Personnel should be able to meet their assigned responsibilities and competence can be demonstrated through appropriate selection, education, training and/or experience. The principle applies to all personnel in the life cycle and includes the competencies of the users of the PES. Users involved in trials should also have appropriate background and training (i.e. such users should be representative of the competence of the actual user groups).

The range of required competencies includes the application area, safety techniques, specific technologies to be used and the legal and regulatory requirements. The appropriate mix of competence, whether through education, training or experience, should be demonstrated for the personnel groups involved. Some key competencies may be necessary for every individual, whilst in other cases only one individual may be competent, for example, one person in a PES development team with detailed knowledge of applicable SOLAS requirements. The main thing is to ensure that no one is required to work outside of their competence range and level.

The responsibilities of key roles (e.g. crew, safety assessor, system integrator, systems engineer, PES developer, safety manager, maintainer etc.) and how these responsibilities are to be discharged should be defined for each PES.

The management of complex and/or hazardous situations at all stages in the life cycle is usually achieved by a team rather than by one person. The design and operation of suitable teams and the selection and training of staff to contribute to these teams needs to be appropriately planned, resourced and managed.

B.9.4.3 Specific guidance

For higher-risk PES, the competence levels of the personnel involved in both development and operation should be commensurately higher. This should include more rigorous justification of the levels and demonstration of their achievement. An independent safety assessor would require such confirmation of competence. Higher-risk PES in this case include those with novel features or technology. This may be novel in general, such as the use of neural nets, or novel to the organization, such as the use of an existing product in a new application.

Competence may be defined in different ways, depending on the size of an organization. In large organizations, corporate schemes and training are available to develop suitable skilled staff. In smaller organizations, externally-operated schemes, such as professional development schemes, may be more appropriate. Experience without assessment of skills is common, but may be a risk in a fast-changing technical environment such as PES development. The use of competence definitions for general roles or staff grades may be useful. Such definitions, whether in-house or from national licensing schemes (a marine example is the UK certification scheme for ships staff) form useful benchmarks against which the team working on the PES can be compared.

What may not be as well understood is the effect of changing technology on the supply of crew. See the guidance on the fourth and fourteenth principles (B.4.2 and B.8.3) regarding the technical specification for user training. It is the responsibility of the operator to ensure the provision of suitable numbers of staff competent to use the PES throughout its service life.

B.9.4.4 Source references

[IEC 61069-1], [IEC 61508-1] §5, [ISO 9000-3] §6.2.2, [ISO 9001] §6.2.2

B.9.5 Twentieth principle

B.9.5.1 General

P20 The PES configuration shall be identified and controlled throughout the life cycle.

B.9.5.2 Commentary

Special attention should be given to the software aspects of this principle, since they can be poorly addressed. The basic requirement is to be clear on which software components comprise the PES and which specific versions are relevant to a given installation or build (configuration identification). This requirement also applies to COTS components, such as operating systems or library files, that are part of the delivered software.

The range and depth of software configuration activities will vary throughout the life cycle. For example, in the early part of the life cycle, it may be mainly concerned with document control of functional specifications, but in later phases, evidence of configuration control during testing or modification to live systems would be needed.

In this respect, a common understanding is needed of the responsibilities of all interested parties, particularly regarding configuration records; such as where and how they are maintained.

B.9.5.3 Specific guidance

The level of detail for the identification of PES should be driven by the complexity and structure of the system and the use made of the information. For example, an operator may only need to know and record the release level of the entire software system, whereas a supplier would keep full configuration details on all the component parts.

Data files, for instance directories, correction factors, trip levels and set point information, may need to be retained between successive versions of software. Configuration management should include such legacy data.

The benefits of a unified configuration management system covering hardware, software and data should be considered.

B.9.5.4 Source references

[MSC/CIRC.891] §3.3.3, [ISO 9000-3] §7.3.7 §7.5.1 §7.5.3, [ISO 9001] §7.5.1, [ISO 10007]

Annex C
(informative)

Guidance on the life cycle of marine PES

C.1 Introduction

The **life cycle** is a mechanism to assist in the production and operation of a system. A life cycle proceeds through a series of **stages**. Each stage is achieved by the performance of one or more **processes**. Processes use and generate work products or **outputs**, many of which comprise information in the form of **documentation**. The lists given in this annex present the main technical stages and processes in the life cycle of a PES.

The philosophy behind the principles stated in Clause 7 is that PES dependability can be achieved through attention to the assessment of risk and focus on quality and user issues throughout the life of the PES. As a result, many of the principles place requirements on the life cycle of the PES. These life cycle principles can be met in a number of different ways. Guidance on one approach is outlined below. This is based on a generic life cycle with defined objectives and outputs for each stage. The approach emphasizes processes and documentation which relate to the fulfilment of the principles, and is particularly suitable for a safety-related marine PES. It is also suitable for PES that are considered non-safety related, since it provides a mechanism for justifying the absence of hazards associated with the PES.

C.2 Life cycle stages

The technical stages in the PES life cycle are shown in Figure C.1. The description of each stage, given in terms of the objectives, major activities, inputs and outputs is in Tables C.1 and C.2 below. Three main processes (management, verification and validation) are also shown. These are enacted at each stage in the life cycle. Defects in the PES are identified through the verification and validation processes. These should therefore begin at the earliest stage in the life cycle, be applied to all stages in the life cycle and continue throughout the life cycle.

The repetition of life cycle stages arising from defects identified during verification and validation is not shown in Figure C.1. Where such iteration is needed, it can be to any previous stage, including the beginning of the life cycle. Iteration for minor problems or changes may only involve returning to the start of the current stage, whilst more major problems may require returning to the “define requirements” or even the “identify need” stage. Early identification of mismatch between the requirements and the developing PES is important because the cost of remedying defects increases approximately 10 times for every stage of separation between the defect and its correction. Iteration in the later stages of the life cycle, when the PES is in operation (for example through modification of the PES or its operating procedures) or is being replaced, is highlighted by the dashed lines in Figure C.1.

The dotted boxes around groups of processes indicate the typical allocation of responsibility during the life cycle. In practice, each stage may be performed by a different combination of competent organizations.

This life cycle and the accompanying descriptions are based largely on the requirements for the technical elements of PES life cycles given in IEC 61508-1 to 3, ISO 13407, BSI 5515 and IEE 1990. This clause does not cover the business, negotiation, personnel, quality and risk management activities required in the development and operation of a PES. These are addressed for man-made systems in ISO/IEC 15288, and are addressed for software in ISO/IEC 12207 *Software life cycle processes* (and its amendments).

The emboldened items in the outputs column of Tables C.1 and C.2 are described in Annex D.

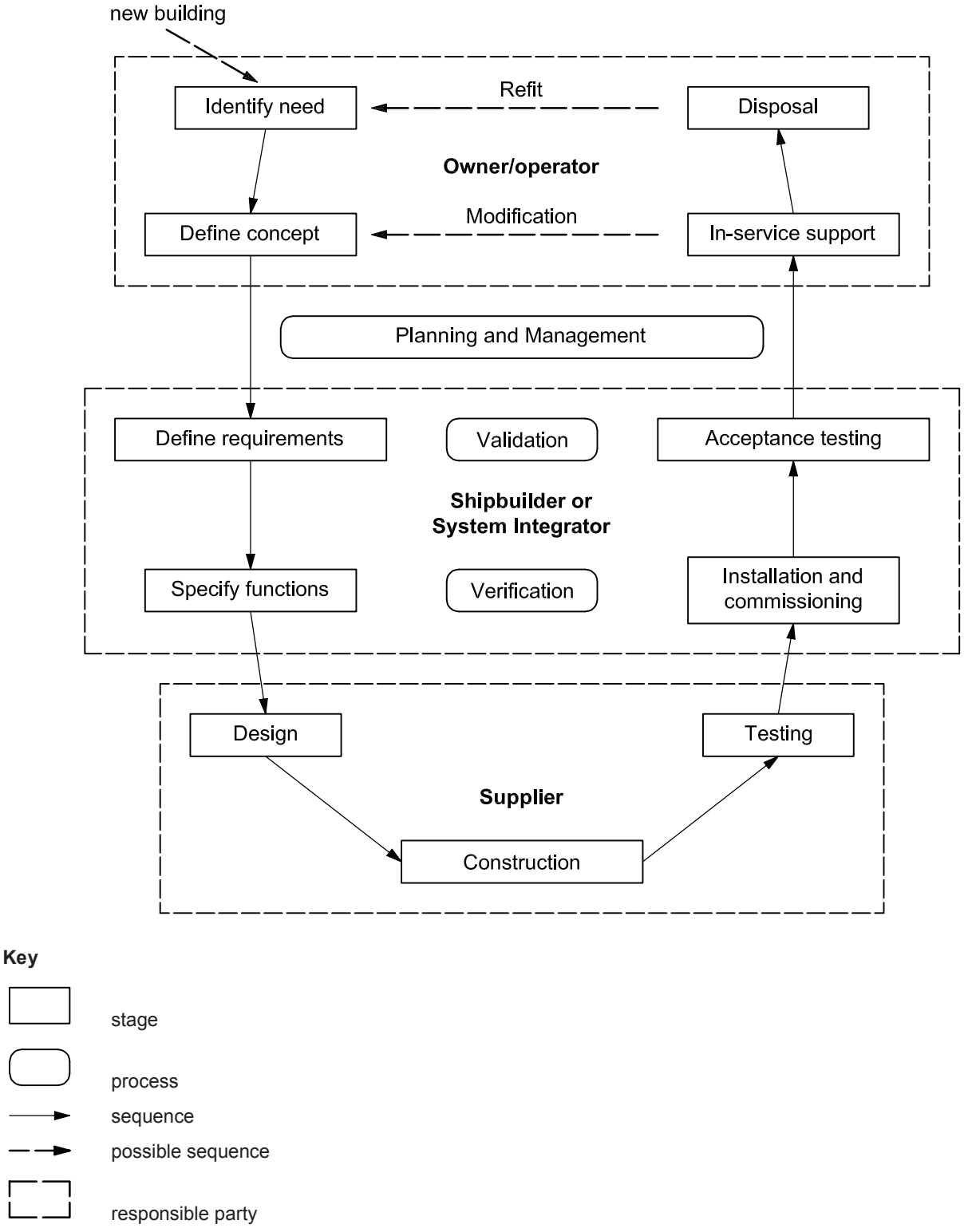

Figure C.1 — PES life cycle stages

Table C.1 — PES life cycle stages

The following stages are present in the definition, development and operation of a dependable PES.

Stage	Also known as and/includes	Objectives	Major Inputs	Major Outputs
Identify need	Initial requirement Needs analysis Concept formulation Change in use	For a potential purchaser of a PES to refine the need for a PES. This may be to: provide new systems; replace obsolete PES; investigate new technology; implement experience gained from existing systems. A focus is established on safety, security and crew issues relating to a new or replacement PES. This process is enacted by the owner/operator.	Company strategy Crew, market and technology forecasts Replacement request Legislative requirement	Business requirement Context(s) of use (predicted) System strategy (outline) Concept and scope description
Define concept	PES Concept PES Feasibility Pre-tender	The definition of concept precedes the commitment to select, purchase or develop new PES. It is performed to — identify the hazards and associated risks relating to the PES; — identify, clarify and record the characteristics of the stakeholders, their tasks and the organizational and physical environment in which the PES will operate; and — develop an understanding of the PES, its users, boundaries, environment and applicable requirements sufficient to enable satisfactory performance of following life cycle activities.	System strategy Project scope Legislation Competitor systems Other relevant information to meet the objectives	Concept and scope description Hazard and risk management description Context of use Invitation to tender
Define requirements	PES Requirements specification	Define a complete, correct and unambiguous set of functional and non-functional requirements for the PES. Establish the requirements of the organization which is acquiring or utilizing the PES and other interested parties (stakeholders) for the PES. This process takes full account of the needs, competencies and working environment of each relevant stakeholder in the system.	Concept and scope description Hazard and risk management description Project scope User representatives Industry, national and international standards Context of use	Requirements specification Context of use (revised)

Table C.1 (*continued*)

Stage	Also known as and/includes	Objectives	Major Inputs	Major Outputs
Design	PES Design and development Design study System design Functional design Produce design solutions Detailed specification for hardware and software	To design the PES to meet the specified requirements. Drawing on established state-of-the-art practice, the experience and knowledge of the supplier and other stakeholders and the results of the context of use analysis. To design the operation, maintenance, training, support and other procedures that ensure the PES performs as required in use. To develop integration testing approach and products.	Requirements specification Context of use Rules and regulations Standards and codes of practice Legislation Evaluation report	Design documentation Integration and test specification Training needs of crew Support plans
Construction	PES Design and development Program development Coding (COTS) selection Customization Paramete-rization	Production or acquisition of the components of the PES in hardware, software, training and procedures. The components of the PES include: hardware, software, operator's manuals, documentation, operational and maintenance procedures, training and support services.	Design documentation Operation and maintenance procedures	PES components Operation and maintenance procedures
Testing	PES integration and testing Assembly	To implement, integrate and test the PES components against their specified requirements. This stage includes activities associated with the rollout of the software.	PES components Design documentation Integration and test specification	Integrated PES Integration test report Integration test log
Installation and commis-sioning	PES installation and commissioning Implementation Cutover	To install and commission the validated PES. To establish the human-system aspects of the support and implementation of the system. NOTE As a result of crew turnover, the user component of the total system may require “re-commissioning” through training.	Validated PES Context of use Requirements specification Installation plan Stakeholder representatives Training materials Support plans	Installed PES Trained users
Acceptance testing	Sea trials Customer acceptance tests Software assessment	Assessment to demonstrate that the PES meets the stakeholder requirements This stage includes the handover of the system.	Installed PES Validation and acceptance test specification	Accepted PES Acceptance test report Acceptance test log

Table C.1 (*continued*)

Stage	Also known as and/includes	Objectives	Major Inputs	Major Outputs
In-service support	PES Operation and maintenance Post-design support	To operate and maintain the PES to keep the required dependability. NOTE The information gained at this stage may also be used as part of the definition of the concept for equivalent PES on similar ships.	Installed PES Operation and maintenance procedures PES manuals Support plans	Operation and maintenance log Monitoring log
Disposal	PES Decommis-sioning	To decommission the PES and remove it from service. NOTE The information gained at this stage may also be used in defining needs for equivalent PES on similar ships. NOTE Some components of the PES may be re-used as part of replacement systems. For example, communications cabling may be recommissioned as part of a faster or more extensive network.	Decommissioning request	Decommis-sioning report Decommis-sioning log

Table C.2 — PES life cycle processes

The following processes are performed as required during the definition, development and operation of a dependable PES.

Process	Also known as and/includes	Objectives	Major Inputs	Major Outputs
Planning and management	Plan and manage PES development PES validation planning Planning the human-centred process	To specify how the required technical, quality, safety and human-centred activities integrate and fit into the whole system life cycle. To develop a feasible PES validation plan that addresses all of the PES requirements.	Concept and scope description Terms and conditions of contract Requirements specification Context of use	Project plans Installation plan Validation plan
Validation	PES validation PES evaluation Evaluate designs against requirements	To validate that the PES meets the PES requirements specification and to ensure that it meets the requirements of the users, the tasks and the environment. This process may be used to collect feedback on the developing design. This feedback will be collected from end users and other representative sources.	Validation plan Requirements specification Project plan Context of use Standards legislation Users	Validated PES Validation report Validation log
Verification	PES verification	To test and evaluate the products of a given phase to ensure correctness and consistency with respect to the inputs to that phase.	Depends upon phase	Verification reports
Modification	PES modification Software maintenance	To correct, enhance or adapt the PES whilst maintaining the required dependability. The PES modification activity may lead to a return to any of the earlier life cycle phases, including possibly the concept phase if the enhancement or adaptation is a significant change.	Monitoring log Modification request Approval of modifications	Modification report Modification log Acceptance of modifications
Refit	Replacement	To dispose of a PES and install a replacement PES.	Monitoring Log	Replacement request

Annex D
(informative)

Checklist for marine PES life cycle outputs

D.1 Introduction

Life cycle stages and processes use and generate work products or **outputs**, many of which comprise information in the form of **documentation**. Table D.1 lists the likely contents of the main outputs produced by these stages or processes.

The approach to PES dependability presented in this International Standard is based on following a life cycle which considers quality, risk and user needs throughout the life of the PES. The production and maintenance of appropriate information is a significant factor in the control of the PES life cycle. These checklists may be used as a basis for evidence that a suitable life cycle is being followed.

Outputs relating to contractual, legal and commercial aspects of the PES life cycle are not described. Details of the documentation of these aspects may be found in BS 5515, IEE 1990 and ISO 15504.

Table D.1 — Requirements for PES life cycle outputs

Outputs	Requirements and contents	References
Installed PES	An installed and commissioned PES that is ready for operation.	
Integrated PES	A fully functioning PES that satisfies the requirement of the Design Documentation.	
Concept and scope description	Records the understanding of the PES and the environment in which it will be used. Definition of the equipment under control, its required control functions and its physical environment: — description of likely sources of hazards and information about the determined hazards; — information about current safety regulations; — identification of hazards due to interaction with other equipment under control; — specification of the external events to be taken into account during hazard and risk analysis; and — specification of subsystems associated with particular hazards. Analysis of the stakeholders in the system and their relevance. Human and organization impact assessment. Specification of the type of accident-initiating event to be considered.	[IEC 61508-1 §7.2.2.6, §7.3.2.5]
Context of use	Description of the components of the total system which are not part of the PES. The hardware and software infrastructure in which the PES is to operate. The systems with which the PES has to exchange data and commands. The physical environment in which the PES is to operate. The characteristics of the intended end users (their skills, training, physical abilities, level of responsibility etc.). The tasks the end users are to perform (including maintenance of the PES). The organizational and social environment in which the users are to use the PES.	[ISO 13407 §7.2]

Table D.1 (*continued*)

Outputs	Requirements and contents	References
Decommis-sioning report	Records the details of the process of decommissioning the PES. Chronological description of the details of decommissioning activities. Reference to the decommissioning plan. Reference to the decommissioning impact analysis.	[IEC 61508-1 §7.17.2.7]
Design document-ation	Defines and justifies the PES design to meet the **requirements specification** in terms of the overall architecture and the component details for both hardware and software elements. Design is derived from and traceable to the requirements specification. Design specifies how independence is achieved between safety and non-safety functions; safety functions at different SILs. Design documentation identifies the techniques and measures necessary to achieve the SIL. Design documentation justifies the techniques and measures chosen to form an integrated set which satisfies the required SIL. Architecture meets requirements for fault tolerance, diagnostic coverage and proof checks. Details of the allocation of functions between users and PES. Intended organization and operational structure. A task model for the use of the PES. Specification of the user system interaction. For SIL 4, the architecture is justified by a detailed quantitative reliability analysis of the hardware of the components. Design specifies features to control systematic faults. Design addresses testability and maintainability. Design decomposed into hierarchy of sub-systems/components with a design and test specification for each sub-system/component. Sub-systems/components clearly identified and fully documented. Design indicates where de-rating of components has been used. Significance of all hardware and software interactions identified, evaluated and detailed. Standards and other sources used, with an indication of how they have been incorporated (or why they have not been followed, if appropriate). Evidence that: — appropriate measures and techniques were used during design to help prevent the introduction of failures; — appropriate design methods were used; — maintenance control procedures are formalized in the design; — automatic testing tools and integrated development tools are used where appropriate; — software engineering procedures and techniques that help prevent introduction of failures were used during software design; — steps were taken to ensure that any prototyping activities covered key requirements and followed good practice; and — prototyping and user input were used to improved and refine the PES.	[IEC 61508-2 §7.4.2., §7.4.9.1] [BS EN 61069-2 §6] [ISO 9000-3 §7.3.3] [ISO 13407] §7.4] [IEC 61508-3 §7.4.2, §7.4.3, §7.4.5]

Table D.1 (*continued*)

Outputs	Requirements and contents	References
Hazard and risk management description	Records the information and results of the hazard and risk analysis activities. Definition of each identified hazardous event and the components that contribute to it. Definition of the consequences and likelihood of the event sequences with which each hazardous event is associated. Definition of the estimated risk for each hazardous event. Definition of the measures taken to reduce or remove hazards and risks. Record of the assumptions made during risk analysis including estimated demand rates and equipment failure rates. Definition of any credit taken for operational constraints or human intervention. References to key documentation which relate to the PES at each life cycle stage.	[IEC 61508-1 §7.4.2.10]
Installation and commission-ing report	Reports the results of installing and commissioning the PES. Record of installation activities. Record of commissioning activities. References to failure reports. Documenting the resolution of failures and incompatibilities.	[IEC 61508-1 §7.13] [ISO 9000-3 §7.5.1, §8.2.4]
Integration and test specification	Defines the steps for integrating the components of the PES and identifies the tests that will demonstrate that the integrated PES satisfies its design documentation. Identifies the integration tests to be performed. The tests demonstrate the conformance of the PES with the design documentation. Tests show all modules interact correctly to perform their intended function and do not perform unintended functions. Identifies procedures to be followed. Identifies test environment. Identifies tools. Identifies configuration to be tested. Addresses coverage of the tests. Merging of software onto hardware identified. Integration of modules/sensors/actuators identified.	[IEC 61508-2 §7.4.7.5] [ISO 9000-3 §8.1 §7.6]
Integration test report	Reports the conditions and results of all levels (component and overall) integration testing. States whether the objectives and criteria decided during the design phase have been met. Reasons for failure are stated. Report is auditable. Specifies the version of Integration and test specification used. Specifies the version of PES tested. Specifies the tools and equipment used, with calibration data. Species the results of each test. Identifies any discrepancy between expected and actual results. Describes the analysis made and decisions taken when discrepancies occur. Addresses impact studies for modification.	[IEC 61508-2 §7.5.7.6] [ISO 9000-3 §8.2.4 §8.3, §8.4] [ISO 13407 §7.5.7]

Table D.1 (*continued*)

Outputs	Requirements and contents	References
Logs: **Operation and maintenance** **Monitoring** **Modification**	Provide a chronological record of the associated development activities with the sources of information used at each stage. Record of the activities providing information on events in a chronological sequence. The **operation and maintenance log** contains: — results of safety audits and tests; — record of the times and causes of demands on safety-related PES in actual operation; — record of the performance of safety-related PES when subject to those demands; — record of faults found during routine maintenance; and — record of the modifications made to the PES and the equipment under control. The **monitoring log** reports the performance of the system in use: — monitoring criteria, programme, process followed, period reported; — deviations from stated processes and reasons for deviations; — deviations from legislative requirements and reasons; and — information for future development projects. The **modification log** contains: — record of all modifications and retrofits; — references to the modification request; — references to the impact analysis; — references to the re-verification and re-validation of the PES and the results; and — references to all documents affected by the modification activity.	[IEC 61508-1 Tables A1 and A2 and A3, §7.15.2.3, §7.16.2.7] [ISO 13407 §7.5.6]
Modification report	Records all modification requests and monitoring surveys for the PES and their subsequent analysis and progress. Specification of the modification or change. Impact analysis of the modification on the PES, the user and the environment. Approval for changes. Progress of changes. Test cases for components. PES configuration management history. Record of any deviations from normal operations and conditions. Changes to system procedures. Changes to other documents.	[IEC 61508-2 §7.8.7.1] [ISO 9000-3 §7.5.1, §7.5.3] [ISO 13407 §7.5.7]

Table D.1 (*continued*)

Outputs	Requirements and contents	References
Operation and maintenance procedures	Defines the procedures that ensure the PES performs as required during operation and maintenance. Specifies the routine actions needed to maintain the 'as designed' functional safety of the PES, including condition and availability of supporting documentation or other advice to users. Specifies the actions and constraints during different operating situations to prevent unsafe state and/or reduce the consequences of a hazardous event. Specifies the operational procedures to be followed by users in day-to-day operation of the PES. Specifies the operational procedures to be followed by users adapting or customizing the operation of the PES, e.g. in varying set points or limits. Specifies the maintenance procedures to the followed when faults are discovered or when failures occur in the PES. Describes the jobs of the users using the PES. Operating instructions and user manuals. Specifies the required competence (skill, training and experience) of each type of user. Specifies training plans and training material. Specifies user support plans and service description. Specifies the monitoring activities required to assure continued dependable operation of the PES. Monitoring plan: Workplace audit plan, scope and criteria, programme, process, tools. Specifies the records to be kept on system failures and on demand rates on the PES. Specifies the documentation to be kept on the results of audits and tests on the PES. Specifies the procedures for monitoring on the effectiveness of maintenance in terms of failure reporting and failure analysis. Specifies the tools needed for maintenance and testing. Specifies the maintenance of the tools needed for maintenance and testing.	[IEC 61508-2 §7.6.2.1] [ISO 9000-3 §, §7.5.1]
Project plans:	Project plans are produced to show how the PES is to be engineered, how the desired level of quality is to be achieved, and how the project is to be resourced so that it is delivered on time and to budget.	

Table D.1 (*continued*)

Outputs	Requirements and contents	References
Technical plan **Quality plan** **Management plan**	The **technical plan** details the strategy that will be adopted to ensure that dependability is engineered into the PES. The strategy should take into consideration any risks and uncertainties in the project as well as the characteristics of the system to be developed so that the chance of producing a system that is not fit for purpose is minimized. The main characteristics and uses of the system to be produced. Expectations or requirements that the client has with respect to how the system should be engineered and the resulting implications. Uncertainties that contribute to a technical risk to the successful completion of the project.. Organization and responsibilities of personnel performing all activities within the project. Roles and purposes of teams within the project and degrees of integration and independence between them. Details of the overall development strategy, and approaches to specification, design, coding, integration and testing, and the relationship between the two. Integration strategy for specialist activities (e.g. safety, human factors and security), including procedures for establishing feedback and communication on these activities as they affect other design activities. Details of the process model to be adopted by the project including, for each activity, the inputs to, outputs from, entry and exit conditions, reviews and role responsibilities. The rationale for and choice of methods, techniques, languages and tools for specification, design, coding, and verification and validation. The target, development, test and maintenance environments. The deliverables to be produced and their nature. A technical log which provides evidence of a sound technical approach is being followed in accordance with the technical plan. The standards, procedures, practices and conventions to be adopted during the development with references. The particular mix of skills and experience that the project requires, including those that will be required for verification and validation. The plans for release, support and modification.	[LRGDS] §5 [ISO 13407 §5 and 6]

Table D.1 (*continued*)

Outputs	Requirements and contents	References
Quality plan	The **quality plan** defines how an organization's quality management system is applied to the project. The quality plan defines the quality features in the deliverables to be produced and the means by which they will be checked. It also details the controls and procedures that will be adopted for the project to ensure that quality is achieved in all deliverables produced. Specification of the items within the scope of the quality plan and the intended use of the PES. Identification of the definitive requirements specification against which acceptance is to be made. Organization of personnel performing quality control and assurance activities on the project, including all verification work, indication of, relation to and interaction with other teams on the project. For each project deliverable define the — format and content; — way in which quality features will be defined and verified; — personnel responsible for origination, verification, maintenance and control; — method for identifying and tracing requirements through the deliverable; — reference to the technical, verification and validation plans; — the deliverables that will be produced and the filing system to be used for these items; — personnel responsible; — scheme for unique identification of item, issue and its status; — meaning of item status; — issue and storage of initial and updated versions of items including how, when and to whom the items will be issued; — specification of how changes to items are to be marked and recorded, and the change history maintained; and — methods and facilities to be used to protect items from unauthorized access or inadvertent damage or degradation, covering items in use or archived and stored on- and off- site and items in transit. Specification of all standards, procedures, practices and conventions to be used on the project, the way in which compliance will be monitored, and how divergence is described and justified. Specification of methods, techniques and tools for verification and validation activities. Specification of procedures for assuring that software purchased or developed under sub-contract meets its requirements. Project metrics and their use.	[LRGDS] §6

Table D.1 (*continued*)

Outputs	Requirements and contents	References
Quality procedures	Specification of reviews: — point in development process; — material to be reviewed; — criteria for assessing material; — roles of participants; — how review is conducted; — how results will be recorded; and — how and when follow-up actions will be performed. Configuration management: — personnel responsible; — procedures for identification of configuration items and baselines; — define how different versions of configuration items will be identified; — define procedures for configuration control; — identify the configuration management tools to be used; — define how the status of a configuration item can be determined from a given baseline; — detail the mechanism for storage of archival and retrieval of different configuration items and baselines; — detail the mechanism for building baselines of the PES; and — define what records will be kept of the deliveries or installations of the different baselines. Detail of change control process: — personnel responsible; — procedure for requesting changes; — procedure for evaluation of changes and their impact; — procedure for responding to and implementing a change request; — procedure for testing the effect and monitoring the progress of a change; and — how and where change control records will be stored. Corrective action procedures: — personnel responsible; — procedure for reporting faults; — procedure for evaluation of faults; — procedure for responding to a fault report; — procedure for fixing a fault; — procedure for monitoring faults and fixes; and — format and location of fault log. Details of audits that will be undertaken during the project to check that the quality measures specified in the quality plan are being adhered to and are appropriate to the project quality objectives.	[LRGDS] §6

Table D.1 (*continued*)

Outputs	Requirements and contents	References
Management plan	The **management plan** is the top-level planning document for a project. It details the purpose of the project, the deliverables to be produced and the associated timescales, the strategy to be adopted, the costing and resourcing, and the way in which the project will be managed. It is produced when the technical and quality plans have been produced. It will evolve over the life of the project. Detail should always be given for the immediate future and an outline for the rest of the project. NOTE The technical and management plans may be combined. The purpose of the project, why the project is being undertaken, what it will achieve and who it is for. The organization of the project and responsibilities of those involved. The approach to be taken in order to achieve a successful completion to the project. A full list of deliverable items and their contracted delivery dates. The scheduling and duration of all activities to be performed, including suitable timescales to allow feedback to be incorporated into the design schedule (including early stage feedback). Details of each project activity, including responsibility, and start and end dates. Details of the project staff and equipment. Financial information related to the project, including resources and potential costs. Any factors which present a risk to the successful completion of the project. Details of training requirements for project staff. Controls to be exercised during the life of the project to ensure that the plan and quality standards are maintained. Criteria and collecting methods for measuring the progress of the project and to aid the planning of future projects. Evidence that the project is being managed well and in accordance with the management plan.	[LRGDS] §4

Table D.1 (*continued*)

Outputs	Requirements and contents	References
Requirements specification	Identifies the functional requirements for the PES. Identifies the non-functional requirements, including the performance, dependability, operability, and safety requirements for the PES. Identifies the statutory and legislative requirements for the PES. Traceable to the overall system requirements and the context of use. Traceable to requirements arising from planning. Defines feasible requirements. Expresses requirements in a clear, precise, unequivocal manner. Defines requirements that are verifiable and testable. Uses terminology and description that is understandable by those who need to use the specification. Provides details of user representatives and their involvement. Gives evidence of confirmation of the requirements by all relevant stakeholders. Describes the functions required of the PES, including behaviour under failure, start-up and restart conditions. Defines throughput and response time performance. Defines user and external system interfaces. Describes the range and relevance of users and other personnel in the design. Defines training needs. Defines modes of operation of the equipment under control. Identifies any constraints arising from software/hardware interaction. Identifies the extremes of environmental conditions likely to be encountered at any stage in the life cycle. Specifies the electromagnetic environment that will be encountered in terms of electromagnetic compatibility levels. Specifies the requirements for proof testing the PES hardware. Gives evidence that the requirements have been used in the design process.	[IEC 61508-2 §7.2.3] [ISO 9000-3 §7.3.2] [BS EN 61069-2 §5] [ISO 13407 §7.3]

Table D.1 (*continued*)

Outputs	Requirements and contents	References
Validation plan	Defines the technical and procedural steps to be used to validate the PES against the **requirements specification**. Specification of the relevant modes of operation of the equipment under control. References the **requirements specification** and cites the goals against which the PES is to be validated. Defines the technical strategy for the validation. Defines the measures and techniques to be used for the validation . Defines the procedures to validate the correct implementation of each safety function. Defines the procedures to validate the achieved safety integrity of each safety function. Identifies required input data, expected outputs and other acceptance criteria. Specifies the required competencies of the validation staff. Specifies the test environment, including all calibrated tools and equipment. Defines the test evaluation procedures (with justifications). Defines the test procedures and criteria to validate electromagnetic immunity levels. Defines the policy and procedures for resolving failures during validation. Defines the schedule and resources for the validation. Identifies the safety related software to be validated for each mode of operation. For usability evaluation: — definition of the context of use which was used as a basis for the evaluation; and — description of the users, methods and measures and the rationale for their use.	[IEC 61508-2 §7.3.2.2] [ISO 9000-3 §7.3.6 §7.4.3 §8.1] [ISO 13407 §7.5.2]
Verification plan	Identifies the component (software, hardware, data, training, document, etc.) to be verified. Defines the technical and procedural steps to be used to verify the component against the **design documentation**. References the **design documentation** and cites the criteria against which the component is to be verified. Defines the technical strategy for the verification. Defines the measures and techniques to be used for the verification . Identifies required input data, expected outputs and other acceptance criteria. Specifies the required competencies of the verification staff. Specifies the test environment, including all calibrated tools and equipment. Defines the test evaluation procedures (with justifications). Defines the policy and procedures for resolving failures during verification. Defines the schedule and resources for the verification. Identifies the safety-related software to be verified for each mode of operation.	[IEC 61508-2 §7.5.2, §7.9] [ISO 9000-3 §7.3.5 §7.4.3 §8.1]

Table D.1 (*continued*)

Outputs	Requirements and contents	References
Validation report	Reports the results of all the validation activities for the PES. Pass/fail decision in relation to the **requirements specification** and the **validation plan.** References the version of the **validation plan** being used. Specifies the safety function under test (or analysis). References the specific validation requirement in the validation plan. Records who performed the evaluation. Records the tools and equipment used. Records the calibration data used. Records the result of each test. Describes any discrepancies between expected and actual results. Describes the analysis and actions arising from any discrepancies found during validation. Evidence of the appropriateness of test procedures. For tests against standards: — list of standards used and rationale for their use; — evidence that sufficient parts of the system have been assessed to give meaningful results for the system as a whole; — report of all major and minor non-compliances and observations and an overall assessment; and — report on how non-conformities were dealt with in the design. Justification of deviations from standards to meet particular user requirements. In the case of usability evaluations or routine monitoring, a relevant statistical analysis should be provided.	[IEC 61508-2 §7.7.2.4] [IACS §7.1] [ISO 9000-3 §7.3.6 §7.3.7, §8.2.4, §7.5.3] [ISO 13407 §7.5.7]
Verification report	Reports the results of the verification activities associated with a life cycle phase. Contains or references results of verification. Addresses non-conformances in respect to the PES life cycle, design standards and safety management requirements. Describes how the relevant requirements have been met in the current phase. Addresses the specific conformities identified for the corresponding verification plan. States whether the PES has passed the verification activity or the reasons for failures.	[IEC 61508-1 §7.18.2.4] [IEC 61508-2 §7.9.2.7] [ISO 9000-3 §7.3.3 §7.3.5, §7.3.7, §7.5.3 §7.4.3] [ISO 13407 §7.5.7]

Annex E
(informative)

Application of the principles in the life cycle

E.1 Introduction

This International Standard presents a set of principles whereby the development and use of dependable PES can be assured. All principles are applicable to the whole system and its components throughout its life. The principles are the generic set of dependability requirements for the PES, and the criteria are significant attributes of these requirements. In any particular application and at any point in the life cycle of a particular PES, the meaning and relative importance of each principle may change. When the standard is used, this interpretation has to be made and shared with relevant parties. This annex illustrates the issues, actions and responsibilities associated with use of the standard, and provides examples of the use of the principles in the life cycle.

E.2 Life cycle

A system's design, development and use can be considered as a series of distinct stages, which represent the life cycle from “cradle to grave”. The life cycle is initiated by a need to perform one or more tasks and the decision to employ PES to this end. The life cycle ends when the system in use no longer fulfils this need or the need itself has changed. The system is then either modified for further use, initiating a new life cycle, or disposed of. Between these two points, the system can exist in a number of states: an idea, on paper, and eventually an assembly of component parts, either bought or manufactured for this purpose.

Figure E.1 presents a simplified version of the “Vee” model of the system life cycle. This model is detailed for the marine community in Annex C. As in Annex C, stakeholders have been assigned responsibility for one or more processes: the operator for concept and service, the systems engineer for specification and technical risk management, the system integrator for commissioning, and suppliers for design and build. Iteration is implicit in the model with cycles back to each previous process in the succession of processes and back across the V for evaluation. Two broad life cycle phases are displayed in the model. The planning phase (from concept to detailed design) broadly concerns documentation, while the delivery phase (from component build to operation) concerns technology. The former is characterized by dissemination of the need, the latter by integration of the component parts. The planning phase also serves to establish interfaces between products, people and organizations, which must be managed throughout the life cycle if proper integration is to be achieved.

The planning and delivery phases have symmetry. The delivered system reflects the operational concept. Commissioning reflects the specification process. Technology build reflects its design. Failings of the planning phase often become evident later in the life cycle. For example, the need for *in situ* modification of equipment resulting in delay, cost and potential operational risk.

Failures during the delivery phase, in the broad sense of deviations from expected behaviour, tend to be a legacy of the planning phase. (Software does not, by nature, fail randomly, and reliability of PES hardware continues to improve, making random failures relatively infrequent.) Most failures are systematic, arising from intrinsic faults and occurring in specific circumstances, originating in the documentation (product) or its through-life use (process). The natural inclination of most engineers to focus on technological solutions rather than dwelling on the planning phase is a source of project risk.

The cost and/or risk of change increases as a failure becomes more removed from its cause. For example, to change the concept before the specification process begins takes little effort, but changes to the specification during delivery would usually require extensive re-engineering. It is easier to change documentation than to change technology. Consistency, completeness and clarity of documentation at the proper stage of the

planning phase increase the probability of delivering a dependable integrated system and better management of through-life costs.

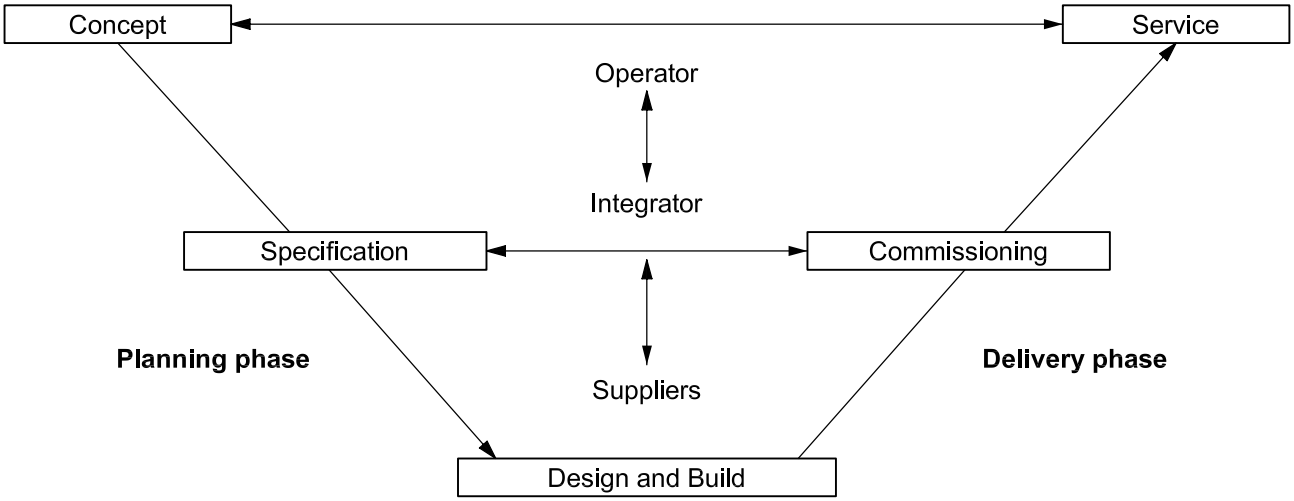

Figure E.1 — Simplified life cycle model

E.3 Planning phase

The planning phase produces the documentation required to facilitate the delivery and use of the technology. This phase should be characterized by a clear understanding of the owner's operational concept such that it can be traced through the specification to the detailed design. Omission and ambiguity in the documentation give rise to assumption and interpretation, which leads to the interfaces between components of the PES becoming ill-defined. The more complex a system is, the more interfaces it contains, and the greater the threat to dependability from poor definition.

The specification stage comprises a number of individual processes that typically includes: the identification of stakeholders, establishing their needs, consolidating these as a set of consistent requirements, and establishing criteria by which compliance will be assessed during the delivery phase. The principles in this International Standard provide a generic set of PES dependability requirements. A programme of assessments against the principles can also be defined.

There will be a number of stakeholders influencing the process, either directly (owner) or indirectly (technology suppliers) by virtue of their demands and constraints. However, the end user, though often overlooked, should be regarded as the primary stakeholder. Neglecting the user and other key stakeholders will lead to expensive changes in the PES during the delivery phase. Stakeholder requirements should be collated and rationalized, then used to facilitate the specification process.

Before detailed design can be undertaken, it is usually necessary to consider the allocation of requirements. Some functions of the total system are best performed by the user, others by the technology. The technology itself will typically involve multiple suppliers, each with particular skills and experience. A system architecture apportioning individual tasks and requirements amongst people and technologies should be defined. This apportionment introduces complex interfaces that need to be managed. Omission and ambiguity should be minimized in order to avoid the introduction of systematic faults that will propagate through the design and into the delivery phase.

A common failing of specifications is the lack of defined acceptance criteria. These may be either quantitative or qualitative, but regardless they should be specific, measurable, agreed, realistic and timed. Acceptance criteria enable the technology to be verified and validated objectively.

At the early stages of a project, there is no system to which the principles can be applied. During this time, process capability determination using an appropriate process reference model, such as ISO/IEC 12207 for

software processes and the process assessment framework provided by ISO/IEC 15504, may be used as a basis for contract award and/or the definition of a process improvement programme. As soon as a concept is defined for a system or its components, then the product principles can be applied. A team review of the dependability requirements of the system and its components against the product principles is a convenient way of focusing attention on dependability issues in the design.

E.4 Delivery phase

The delivery phase is concerned with the integration of parts, either bespoke or commercial off-the-shelf (COTS) components, to provide the enabling technology for the required tasks. This integration is in the context of the use of the system in its organization and physical environment. The cost and effort of integrating COTS products is difficult to predict, more so than for bespoke products, and represents a challenge to project management.

To test even relatively simple software exhaustively very quickly becomes an impracticable proposition. The prevailing marine practice of factory acceptance testing, harbour and sea trials does not in any substantive way serve to indicate that a complex technology is free from faults. The most practical solution lies in modular, hierarchical design and a systematic program of verification and validation testing throughout the development process, and the careful use of COTS products. Functional testing should serve to confirm rather than mandate. Type-testing of products might seem to be a solution, but the inflexibility of type-tested technology places an increased burden on the human element insofar as the user, organization and environment have to accommodate their limitations. There is a cost/benefits balance to be struck and this must be based on sound judgement and understanding.

During design, build and delivery, the principles may be applied in three ways. Firstly, in reviews of component development activities against the product and (relevant) life cycle principles in order to ensure that design intent is achieved. Secondly, in evaluation of components against the product principles in order to ensure that verification is relevant, sufficient and timely. Thirdly, in the review of the total system against the product principles to ensure that validation is relevant and adequate.

E.5 Management

The management of the project will determine the extent of success in applying the principles in this International Standard. The key to effective project management lies in open communication and fostering a partnership. The transition from one life cycle stage or project process to another involves communication and possibly changes in assigned roles and responsibilities. Individual processes will typically involve product iteration and thereby on-going communication between the participating stakeholders.

Once the operational concept for the system is well defined, the next step is to develop a specification that fulfils the operational concept and delivers an enabling technology, taking account of any imposed constraints. It is necessary to plan, organize, monitor and control the various processes that constitute this task. This requires a clear and agreed understanding of roles and responsibilities for each partner. The life cycle principles in this International Standard provide a general set of process requirements for dependable systems.

The process of specification transfers the primary responsibility from the operator to the systems engineer. Traditionally, the role of systems engineer has fallen to the shipyard. The shipyard may need to acquire the capability to fully discharge this responsibility. It will not be achieved if the yard devolves responsibility to its various suppliers unless they have the authority and disposition to ensuring that the total system satisfies the concept. The suppliers' role is principally one of delivering COTS product. This can only be achieved if the specification and allocation processes are adequate.

The role of systems engineer is highly involved, both in management and technology terms. It requires an understanding of both the operational concept (upstream) and the enabling technology (downstream). If the systems engineer fails to properly manage interfaces, then extensive re-engineering may be required. This usually involves unforeseen delay and cost, and introduces risk insofar as each modification raises the possibility of further systematic faults.

Verification and validation are important tools for project management. Given that verification is a matter of ensuring the “correctness” of a product rather than its suitability for the task, this aspect could in principle be left primarily to the assigned stakeholder, e.g. technology supplier. Part of the management process is ensuring that appropriate checks are in place, e.g. third-party audit or review of test records and associated documentation. Proper verification establishes confidence in the technology's reliability and allows factory acceptance testing, harbour and sea trials, etc. to focus on verification of interfaces and validation of the total system. If dependability is to be established, then validation too must be a planned and managed process.

The principles provide a tool for management. They can initially be employed in conjunction with relevant process reference standards (e.g. ISO/IEC 15288, ISO 13407 and IEC 61508) as a checklist of the project activities that will be required to ensure that threats to the dependability of the PES are analysed, monitored and mitigated. From that time onward, they provide the basic set of questions for suitably-timed reviews of partner/project activities against the life cycle principles. These reviews should take account of the process risks arising from the capability of the partners as identified in the planning phase and also those emerging during delivery.

Annex F
(informative)

Principles for marine PES

F.1 Intention for marine PES

The PE*S* 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 will be achieved if the following principles are fulfilled by the PES and its associated elements throughout its life.

F.2 Product principles for marine PES

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

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

c) The PES shall provide functions which meet user needs.

d) Functions shall be appropriately allocated between users and PES.

e) The PES shall be tolerant of faults and input errors.

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

g) Unauthorized access to the PES shall be prevented.

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

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

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

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

F.3 Life cycle principles for marine PES

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 7.3 are described below.

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

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

c) Human-centred activities shall be employed throughout the life cycle.

d) Verification and validation activities shall be employed throughout the life cycle.

e) All parties involved in life cycle activities shall have and use a quality management system.

f) Existing requirements for marine systems shall be taken into account throughout the life cycle.

g) Suitable documentation shall be produced to ensure that all PES life cycle activities can be performed effectively.

h) Persons who have responsibilities for any life cycle activities shall be competent to discharge those responsibilities.

i) The PES configuration shall be identified and controlled throughout the life cycle.

Bibliography

The following standards and guides were used to inform the principles and criteria of this document. The identity and scope of application of the primary standards is outlined at the end of this clause. In order to preserve traceability the cited version is the one used in preparing this revision of ISO 17894. Readers are encouraged to use the most recent version of these documents. In order to assist readers, recent changes in reference or title of the cited standards are indicated.

The referencing system employed in this International Standard uses an abbreviation of the standard's title e.g. [ISO 9000]. This is done to make the document easier to use when tracing detailed requirements in the standard.

EN 292-1 *Safety of machinery — Basic concepts, general principles for design — Basic terminology Methodology* [BS 292-1]

EN 292-2 *Safety of machinery — Technical principles and specifications* [BS 292-2]

IEC 61069-2:1993 *Industrial-process measurement and control — Evaluation of system properties for the purpose of system assessment — Assessment methodology* [IEC 61069-2]

IEC EN 61069-5:1994 *Industrial-process measurement and control — Evaluation of system properties for the purpose of system assessment — Assessment of system dependability* [IEC 61069-5]

Research In Waterborne Transport Area 6.33/26(2nd Call): Demonstration of ISC - DISC Final Report, D101.00.01.047.003, 1997.04.21, DISC Consortium www.atomos.org [DISC]

Generalised Assessment Method Part 1: Rules, CAS/LR/WP2.T3/SM/D2.3.1, Issue 0.C DRAFT, 20 September 1996, ESPRIT 9032 CASCADE project. Lloyd's Register of Shipping, 71 Fenchurch Street, London EC3M 4BS [GAM1]

MSC/Circular 891, 21st December 1998, *Guidelines for the on-board use and application of computers* [MSC/Circ. 891]

IEC 61162 *Maritime navigation and Radiocommunication equipment and systems — Digital interfaces* (all parts) [IEC 61162]

IEC 61209, Ed. 1.0 *Maritime navigation and Radiocommunications equipment and systems — Integrated Bridge Systems (IBS), Operational and performance requirements, methods of testing and required test results* [IEC 1209]

IEC 61508-2:2000 *Functional Safety — Safety related systems — Requirements for E/E/PES* [IEC 61508-2]

IEC 61508-3:1998 *Functional Safety — Safety related systems — Software requirements* [IEC 61508-3]

IEC 61508-4:1998 *Functional Safety — Safety related systems — Definitions and Abbreviations of Terms* [IEC 61508-4]

IEC 61508-7:2000 *Functional Safety — Safety related systems — Bibliography of techniques and measures* [IEC 61508-7]

ISO/IEC Guide 51:1999 *Safety aspects — Guidelines for their inclusion in standards* [IEC 51]

IEC 60092-504 third edition 2001, *Electrical installations in ships — Special features — Control and instrumentation* [IEC 92504]

International Management Code For The Safe Operation Of Ships And For Pollution Prevention (International Safety Management [ISM] Code), IMO [ISM]

ISO 9000-3 A*pplication of ISO 9001 to software*. (ISO 9000-3 has been revised by ISO/IEC JTC 1/SC 7 and will be published as ISO 900003) [ISO 9000-3]

ISO 9001:2000 *Quality management systems — Requirements.* [ISO 9001]

prEN 894-1:1996 *Safety of Machinery — Ergonomic requirements for the design of displays and control actuators — Part 1: General principles for human interactions with displays and control actuators.* (now ISO 9355) [EN 894-1]

Classification Of Ships Rules And Regulations Part 6: Control, Electrical, Refrigeration and Fire, Lloyd's Register [RULES PT6]

BS 5515:1984 *Documentation of computer-based systems,* British Standard Code of practice [BS 5515]

Guidelines for the documentation of computer software for real time and interactive systems, IEE, 1990, second edition [IEE 1990]

Lloyd's Register Guidelines for the development of Dependable Software, V5 Lloyd's Register, 1992. Lloyd's Register of Shipping, 71 Fenchurch Street, London EC3M 4BS [LRGDS]

ISO/IEC TR 15504:1999 *Software process assessment — Part 5: exemplar assessment model* (this standard is currently under revision to ISO 15504 *Process assessment*) [ISO 15504]

International Maritime Organization, 1995, *Standards of Training, Certification and Watchkeeping for Seafarers* [STCW95]

IEC 60945:2002, *Maritime Navigation and Radiocommunication Equipment and Systems — General requirements — methods of testing and required test results*, Fourth Edition [IEC 60945]

ISO/IEC 15288:2002 *Systems engineering — System life cycle processes* [ISO 15288]

Stevens, R., Brook, P., Jackson, K., Arnold, S., 1889, *Systems Engineering — coping with complexity*, Prentice Hall Europe, ISBN 0-13-095085-8, 374 pp.

Messer A.C., 2002, *Systems integration and complexity: managing dependability*, Proceedings IMarEST sixth international naval engineering conference and exhibition, Glasgow 2002, p. 175-181 [INEC]

Earthy J.V., 1999, *A new approach to marine programmable systems assessment*, Scandinavian yearbook of maritime technology, 1999, Scandinavian Shipping Gazette [SSG]

Scope of application of primary references

[IEC 61069-1] for product principles relevant to industrial process measurement and control systems.

[IEC 61209] for product principles relevant to both marine sector requirements and to integrated PES.

[IEC 61508-1], [IEC 61508-2], [IEC 61508-3] for both product and life cycle principles relevant to safety related measurement, control and safety systems. Includes the risk-based approach and the concept of safety life cycle.

[ISO 13407] for life cycle principles relevant to the process of human centred design for interactive PES.

[ISO/IEC 9000-3], [ISO 9000] for life cycle principles relating to the requirements of a quality system to develop, supply and maintain programmable systems. [ISO 9241-10] for product principles relevant to human centred requirements of user interfaces.

ICS 35.240.60; 47.020.99

Price based on 64 pages

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email bsmusales@bsigroup.com.

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

Useful Contacts:

Customer Services
Tel: +44 845 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 845 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

bsi.

...making excellence a habit.™