



IEEE

IEC/IEEE 60880

Edition 1.0 2026-10

INTERNATIONAL STANDARD

**Nuclear power plants - Instrumentation and control systems important to safety -
Software aspects for computer-based systems performing category A functions**

Sample Document

get full document from standards.iteh.ai



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2026 IEC, Geneva, Switzerland

Copyright © 2026 IEEE

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing being secured. Requests for permission to reproduce should be addressed to either IEC at the address below or IEC's member National Committee in the country of the requester or from IEEE.

IEC Secretariat
3, rue de Varembe
CH-1211 Geneva 20
Switzerland
Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue
New York, NY 10016-5997
United States of America
stds.ipr@ieee.org
www.ieee.org

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About the IEEE

IEEE is the world's largest professional association dedicated to advancing technological innovation and excellence for the benefit of humanity. IEEE and its members inspire a global community through its highly cited publications, conferences, technology standards, and professional and educational activities.

About IEC/IEEE publications

The technical content of IEC/IEEE publications is kept under constant review by the IEC and IEEE. Please make sure that you have the latest edition, a corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform

The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee, ...). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

IEC Customer Service Centre - webstore.iec.ch/csc

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

IEC Products & Services Portal - products.iec.ch

Discover our powerful search engine and read freely all the publications previews, graphical symbols and the glossary. With a subscription you will always have access to up to date content tailored to your needs.

Electropedia - www.electropedia.org

The world's leading online dictionary on electrotechnology, containing more than 22 500 terminological entries in English and French, with equivalent terms in 25 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

Warning! Make sure that you obtained this publication from an authorized distributor.

CONTENTS

FOREWORD	5
INTRODUCTION	7
1 Scope	9
2 Normative references	9
3 Terms, definitions, symbols and abbreviations	10
3.1 Terms and definitions	10
3.2 Symbols and abbreviations	16
4 General requirements for software projects	17
4.1 General	17
4.2 Software types	18
4.3 Software development approach	19
4.4 Software project management	20
4.5 Software quality assurance plan	22
4.6 Software configuration management	22
5 Software requirements definition	23
5.1 Specification of software requirements	23
5.2 Self-supervision	24
5.3 Periodic testing	25
5.4 Documentation	25
6 Software design and implementation	26
6.1 Principles for design and implementation	26
6.1.1 Language independent design and implementation principles	26
6.1.2 Design and implementation of software in general-purpose languages	27
6.1.3 Design and implementation of software in application-oriented languages	27
6.1.4 Configuration of pre-developed software	28
6.1.5 Management of configuration data	29
6.2 Selection of languages	30
6.2.1 Language independent	30
6.2.2 General-purpose languages	30
6.2.3 Application-oriented languages and associated automated code generation	31
6.3 Detailed requirements and recommendations	31
6.4 Documentation	32
7 Software verification	33
7.1 Software verification process	33
7.2 Software verification activities	34
7.2.1 Software verification plan	34
7.2.2 Design verification	36
7.2.3 Implementation verification	36
8 Software aspects of system integration	39
8.1 General	39
8.2 Software integration plan	39
8.3 System integration	40
8.4 Integrated system verification	41
8.5 Fault resolution procedures	41

8.6	Software integration report	41
9	Software aspects of system validation testing	41
9.1	Software validation plan	41
9.2	System validation testing	41
9.3	Fault resolution procedures	41
9.4	Software validation report	41
10	Software aspects of system installation	41
11	Software modification	42
11.1	Software modification definition and control procedure	42
11.2	Software modification request	42
11.3	Procedure for executing a software modification	44
11.4	Anomaly reporting	45
12	Defences against common cause failure due to software	45
13	Acceptance of software tools for the development of software	46
13.1	General	46
13.2	Selection of software tools	46
13.3	Requirements for software tools	47
13.3.1	Software engineering environment	47
13.3.2	Tool qualification	48
13.3.3	Tool configuration management	49
13.3.4	Translators/compilers	49
13.3.5	Automation of testing	51
14	Qualification of pre-developed software	51
14.1	General	51
14.2	PDS qualification process	54
14.2.1	Evaluation of the functional and performance features	54
14.2.2	Quality evaluation	55
14.2.3	Evaluation of operating experience	56
14.2.4	Comprehensive assessment	59
14.2.5	Maintenance	59
Annex A (normative)	Detailed requirements and recommendations for design and implementation	60
Annex B (informative)	Example of application-oriented software engineering	71
B.1	General	71
B.2	Principle of application of requirements	71
B.3	Application of requirements for software lifecycle	71
B.4	Application of requirements for automated code generation	72
B.4.1	General	72
B.4.2	Tools for design and project management	72
B.4.3	Tools for automated generation	73
Annex C (informative)	Software verification and testing	75
C.1	Software verification and testing activities	75
C.2	Systematic approaches	75
C.3	Statistical approaches	76
C.4	Verification and testing methods	77
C.4.1	Selected verification methods	77
C.4.2	Testing methods	79
Annex D (informative)	Typical list of software documentation	81

Annex E (informative) Tools for production and checking of specification, design and implementation	82
E.1 General.....	82
E.2 Constructive tools	82
E.2.1 Text editor	82
E.2.2 Graphical interface	82
E.2.3 Automated code generator.....	82
E.2.4 Proof obligation generator	82
E.3 Analytical tools	83
E.3.1 Syntax checker.....	83
E.3.2 Semantic checker	83
E.3.3 Formal proof generator	83
E.3.4 Animator.....	83
E.3.5 Compliance analyser	83
Annex F (informative) Correspondence between IEC 61513 and this document	84
Annex G (informative) Relationship with IEC 61508	85
G.1 General.....	85
G.2 Comparison of scope and concepts.....	85
G.3 Correspondence between this document and IEC 61508-3:2010	86
Bibliography.....	87
Figure 1 – Activities of the system safety lifecycle (as defined by IEC 61513)	17
Figure 2 – Software related activities in the system safety lifecycle.....	18
Figure 3 – Development activities of the IEC/IEEE 60880 software safety lifecycle	20
Figure 4 – Outline of the qualification process of PDS.....	53
Figure B.1 – Lifecycle for application-oriented software engineering	74
Table 1 – Process and product aspects of design and implementation	32
Table A.1 – Design process: modifiability.....	60
Table A.2 – Design process: top-down approach	60
Table A.3 – Design process: verification of intermediate design products	61
Table A.4 – Design process: modification control during the development.....	61
Table A.5 – Software structure: control and access structures	62
Table A.6 – Software structure: modules.....	62
Table A.7 – Software structure: operational system software	63
Table A.8 – Software structure: execution time	63
Table A.9 – Software structure: interrupts	64
Table A.10 – Software structure: arithmetic expressions	64
Table A.11 – Self-supervision: plausibility checks	64
Table A.12 – Self-supervision: safe output.....	65
Table A.13 – Self-supervision: memory contents.....	65
Table A.14 – Self-supervision: error checking	65
Table A.15 – Detailed design and coding: branches and loops.....	66
Table A.16 – Detailed design and coding: subroutines	66
Table A.17 – Detailed design and coding: nested structures	66

Table A.18 – Detailed design and coding: addressing and arrays.....	67
Table A.19 – Detailed design and coding: data structures	67
Table A.20 – Detailed design and coding: dynamic changes	67
Table A.21 – Detailed design and coding: unit and integration tests	68
Table A.22 – Language dependent: sequences and arrangements	68
Table A.23 – Language dependent: comments.....	68
Table A.24 – Language dependent: assembler	69
Table A.25 – Language dependent: coding rules.....	69
Table A.26 – Language dependent: application-oriented languages	69
Table A.27 – Language dependent: automated code generation	70
Table D.1 – Typical list of software documentation	81
Table F.1 – Correspondence between subclauses of IEC 61513:2026 and this document.....	84
Table G.1 – Correspondence between this document and IEC 61508-3:2010.....	86

Sample Document

get full document from standards.iteh.ai

Nuclear power plants - Instrumentation and control systems important to safety - Software aspects for computer-based systems performing category a functions

FOREWORD

- 1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC document(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation.

IEEE Standards documents are developed within IEEE Societies and Standards Coordinating Committees of the IEEE Standards Association (IEEE SA) Standards Board. IEEE develops its standards through a consensus development process, approved by the American National Standards Institute, which brings together volunteers representing varied viewpoints and interests to achieve the final product. Volunteers are not necessarily members of IEEE and serve without compensation. While IEEE administers the process and establishes rules to promote fairness in the consensus development process, IEEE does not independently evaluate, test, or verify the accuracy of any of the information contained in its standards. Use of IEEE Standards documents is wholly voluntary. *IEEE documents are made available for use subject to important notices and legal disclaimers (see <https://standards.ieee.org/ipr/disclaimers.html> for more information).*

IEC collaborates closely with IEEE in accordance with conditions determined by agreement between the two organizations. This Dual Logo International Standard was jointly developed by the IEC and IEEE under the terms of that agreement.

- 2) The formal decisions of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees. The formal decisions of IEEE on technical matters, once consensus within IEEE Societies and Standards Coordinating Committees has been reached, is determined by a balanced ballot of materially interested parties who indicate interest in reviewing the proposed standard. Final approval of the IEEE standards document is given by the IEEE Standards Association (IEEE SA) Standards Board.
- 3) IEC/IEEE Publications have the form of recommendations for international use and are accepted by IEC National Committees/IEEE Societies in that sense. While all reasonable efforts are made to ensure that the technical content of IEC/IEEE Publications is accurate, IEC or IEEE cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
- 4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications (including IEC/IEEE Publications) transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC/IEEE Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
- 5) IEC and IEEE do not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC and IEEE are not responsible for any services carried out by independent certification bodies.
- 6) All users should ensure that they have the latest edition of this publication.
- 7) No liability shall attach to IEC or IEEE or their directors, employees, servants or agents including individual experts and members of technical committees and IEC National Committees, or volunteers of IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE SA) Standards Board, for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC/IEEE Publication or any other IEC or IEEE Publications.
- 8) Attention is drawn to the normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
- 9) Attention is drawn to the possibility that implementation of this IEC/IEEE Publication may require use of material covered by patent rights. By publication of this standard, no position is taken with respect to the existence or validity of any patent rights in connection therewith. IEC or IEEE shall not be held responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patent Claims or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility.

IEC/IEEE 60880 has been prepared by subcommittee 45A: Instrumentation, control and electrical power systems of nuclear facilities, of IEC technical committee 45: Nuclear instrumentation in cooperation with Nuclear Power Engineering Committee of the IEEE, under the IEC/IEEE Dual Logo Agreement between IEC and IEEE. It is an International Standard.

This is the first edition developed according to the IEC/IEEE Dual Logo Agreement. This edition cancels and replaces the second edition IEC 60880 published in 2006. It constitutes a technical revision.

The revision of the standard is intended to accomplish the following:

- a) To take into account the fact that software engineering techniques advanced significantly in the intervening years.
- b) To align the standard with the new IAEA document SSG-39.
- c) To align as far as possible the definitions in the standard with the International Atomic Energy Agency, IAEA Nuclear Safety and Security Glossary, 2022 (Interim) Edition, IAEA, Vienna (2022).
- d) To adapt the requirements associated with standards published or revised since the second edition of IEC 60880, especially IEC 61513, IEC 61226, IEC 62138, IEC 60987, IEC 62340, IEC 62645 and IEC 62671.
- e) To review the existing requirements.

The text of this International Standard is based on the following IEC documents:

Draft	Report on voting
45A/1661/FDIS	45A/1668/RVD

Full information on the voting for its approval can be found in the report on voting indicated in the above table.

The language used for the development of this International Standard is English.

This document was drafted in accordance with the rules given in the ISO/IEC Directives, Part 2, available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/publications/.

The IEC Technical Committee and IEEE Technical Committee have decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under webstore.iec.ch in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn, or
- revised.

INTRODUCTION

a) Technical background and main issues

Engineering of computer-based instrumentation and control (I&C) systems to be used for nuclear safety purposes is a challenge due to the safety requirements to be fulfilled. The safety software used in nuclear power plants (NPP) which is often required only in emergency cases, is fully validated and qualified before use in operation. In order to achieve the high dependability required, special care is taken throughout the entire lifecycle, including the basic requirements, the various design phases, the verification and validation testing procedures for operation and maintenance. This document addresses the related safety aspects and provides requirements for achieving the high software quality necessary.

b) Situation of the current standard in the structure of the SC 45A standard series

This document is directly referenced by IEC 61513 which deals with the system aspects of I&C systems and equipment that are used to perform functions important to safety in NPPs.

This document is the second level SC 45A document tackling the issue of software aspects for I&C systems performing category A functions.

Software for categories B and C functions is dealt with in IEC 62138.

This document and IEC 62138 together cover the domain of the software aspects of computer-based systems used in nuclear power plants to perform functions important to safety.

IEC 62566 and IEC 62566-2 together cover the domain of the programmable logic used in nuclear power plants to perform functions important to safety.

IEC 62340 covers the domain of requirements for coping with common cause failure (CCF).

This document is to be read in conjunction with IEC 61513, the appropriate SC 45A standard on system aspects of I&C systems and equipment that are used to perform functions important to safety.

For more details on the structure of the SC 45A standard series see item d) of this introduction.

c) Recommendation and limitation regarding the application of this document

This document establishes no additional functional requirements for systems important to safety.

Aspects for which special requirements and recommendations have been produced, are:

- a) a general approach to software development to assure the production of the highly reliable software required including hardware and software interdependencies;
- b) a general approach to software verification and to the software aspects of the computer-based system validation;
- c) procedures for software modification and configuration control;
- d) requirements for use of tools;
- e) procedures for qualification of pre-developed software.

It is recognised that software technology is continuing to develop at a rapid pace and that it is not possible for this document to include references to all modern design technologies and techniques.

To ensure that this document continues to be relevant in future years the emphasis has been placed on issues of principle, rather than specific software technologies.

If new techniques are developed then it is deemed possible to assess the suitability of such techniques by applying the safety principles contained within this document.

d) Description of the structure of the SC 45A standard series and relationships with other IEC documents and other bodies documents (IAEA, ISO)

The IEC SC 45A standard series comprises a consistent set of documents organised in a hierarchy of four levels. The top-level documents of the IEC SC 45A standard series are IEC 61513 and IEC 63046, covering respectively general requirements for I&C systems and general requirements for electrical power systems of NPPs. IEC 61513 and IEC 63046 adopt an overall system lifecycle framework and constitute, along with the relevant second-level standards, the nuclear implementation of the basic safety series IEC 61508. IEC 61513 and IEC 63046 refer to ISO 9001 as well as to IAEA GSR part 2 and IAEA GS-G-3.1 and IAEA GS-G-3.5 for topics related to quality assurance (QA).

IEC 61513 and IEC 63046 refer directly to second-level IEC SC 45A standards for general requirements for specific topics, such as categorization of functions and classification of systems (IEC 61226), qualification (IEC/IEEE 60780-323), separation (IEC 60709), control room design (IEC 60964), electromagnetic compatibility (IEC 62003), human factors engineering (IEC 63351), programmable digital item and hardware aspects for programmable digital systems (in particular this document and IEC 62566) and management of ageing (IEC 62342). For cybersecurity, IEC 62645 builds upon the valid high-level principles and main concepts of the generic security standards, in particular ISO/IEC 27001 and ISO/IEC 27002; it adapts them and completes them to fit the nuclear context and coordinates with the IEC 62443 series.

At a third level, standards relate to specific requirements for specific equipment, technical methods, or activities. Usually, these documents refer to second-level documents for general requirements and can be used on their own.

A fourth level extending the IEC SC 45A standard series, corresponds to Technical Reports which are not normative.

The IEC SC 45A standards series consistently implements the safety and cybersecurity principles and terminology of relevant IAEA safety standards and documents of the IAEA Nuclear Security Series (NSS). In particular, this includes IAEA Safety Requirements SSR-2/1, establishing safety requirements related to the design of NPPs; IAEA Safety Guide SSG-30, addressing the safety classification of structures, systems and components in NPPs; IAEA Safety Guide SSG-39, addressing the design of I&C systems for NPPs; IAEA Safety Guide SSG-34, addressing the design of electrical power systems for NPPs; IAEA Safety Guide SSG-51, addressing human factors engineering in the design of NPPs; and Nuclear Security Series Implementing Guide NSS 42-G and Technical Guidance NSS 17-T for computer security at nuclear facilities.

NOTE IEC TR 63400 provides a more comprehensive description of the overall structure of the IEC SC 45A standards series and of its relationship with other standards bodies and standards.

1 Scope

This document provides requirements for the software of computer-based systems of nuclear power plants performing functions of safety category A as defined by IEC 61226. As an IEC/IEEE standard developed according to the Dual Logo Agreement, when used within the context of IEEE, this document is considered to provide an acceptable set of requirements for achieving the quality and dependability objectives for the software used in IEEE Class 1E safety systems, subsystems and components.

According to the definition in IEC 61513, I&C systems of safety class 1 are intended to support category A functions, but can also support functions of lower categories. However the system requirements are always determined by the functions of the highest category implemented.

For software of I&C system performing only category B and C functions in NPP as defined by IEC 61226, the requirements and guidance of IEC 62138 are applicable.

This document provides requirements for the purpose of achieving highly dependable software. It addresses each stage of software generation and documentation, including requirements specification, design, implementation, verification and validation testing.

The principles applied in developing these requirements include:

- best available practices;
- top-down design methods;
- modularity;
- verification of each phase;
- clear documentation;
- auditable documents;
- validation testing.

Annex A provides detailed requirements and recommendations for design and implementation of software.

Additional informative guidance is given in Annex B to Annex G.

This document does not explicitly address the protection of software against threats arising from malicious attacks, that is, cybersecurity, for computer-based systems. IEC 62645 provides cybersecurity requirements.

IEC 62671 can be used as an alternative to this document for digital devices of limited functionality. IEC 62671 contains precise criteria to determine if it is applicable to a particular device.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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.

IEC 61513:2026, *Nuclear power plants - Instrumentation and control important to safety - General requirements for systems*

3 Terms, definitions, symbols and abbreviations

3.1 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO, IEC, and IEEE maintain terminology databases for use in standardization at the following addresses:

- IEC Electropedia: available at <https://www.electropedia.org/>
- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEEE Standards Dictionary Online: available at <http://dictionary.ieee.org>

3.1.1

animation

process by which the behaviour defined by a specification is displayed with actual values derived from the stated behaviour expressions and from some input values

3.1.2

application function

function of an I&C system that performs a task related to the process being controlled rather than to the functioning of the system itself

[SOURCE: IEC 61513:2026, 3.1, modified – notes removed.]

3.1.3

application-oriented language

computer language specifically designed to address a certain type of application and to be used by persons who are specialists of this type of application

Note 1 to entry: Application-oriented languages may be used to specify the functional requirements of an I&C system, or to specify or design application software. They may be based on texts, on graphics, or on both.

Note 2 to entry: Examples: Instruction List (IL), Structured Text (ST), Ladder Diagram (LD), Function Block Diagram (FBD).

Note 3 to entry: See 3.1.18.

3.1.4

application software

software part of an I&C system which is distinct from the operational system software

Note 1 to entry: The distinction between system software (generic, re-usable) and application software (typically plant-specific) is generally made to minimize re-development of code and to optimize the allocation of the qualification activities. It is an especially useful distinction when using an I&C platform.

Note 2 to entry: See 3.1.2, 3.1.28, and 3.1.37.

[SOURCE: IEC 61513:2026, 3.2]

3.1.5

automated code generation

function of automated tools allowing transformation of the application-oriented language into a form suitable for compilation or execution

3.1.6

code compaction

purposeful reduction in memory size required for a program by the elimination of redundant or extraneous instructions

3.1.7**common cause failure****CCF**

failures of two or more structures, systems or components due to a single specific event or cause

Note 1 to entry: For example consider software dependent on calendar date or similar time counters used in several systems and comprising a design fault leading to its failure on a specific date. The single initiator leads to the simultaneous common cause failure of several components (all components containing the offending software).

[SOURCE: IAEA Nuclear Safety and Security Glossary, 2022 (Interim) Edition, modified – note added]

3.1.8**computer-based item**

item that relies on software instructions running on microprocessors or microcontrollers

Note 1 to entry: In this term and its definition, the term item can be replaced by the terms: system or equipment or device.

Note 2 to entry: Computer-based item is a kind of programmable digital item.

Note 3 to entry: This term is equivalent to software-based item.

Note 4 to entry: The IEC definition differs from the IAEA definition for “computer-based systems” because it is more specific regarding the kind of digital technology covered.

[SOURCE: IEC 62138:2018, 3.8, modified – Note 4 has been added.]

3.1.9**data**

representation of information or instructions in a manner suitable for communication, interpretation, or processing by digital equipment

Note 1 to entry: Data which are required to define parameters and to instantiate application and service functions in the system are called “configuration data”.

[SOURCE: IEC 61513:2026, 3.15, modified – note added]

3.1.10**defence in depth**

hierarchical deployment of different levels of diverse equipment and procedures to prevent the escalation of anticipated operational occurrences and to maintain the effectiveness of physical barriers placed between a radiation source or radioactive material and workers, members of the public or the environment, in operational states and, for some barriers, in accident conditions

[SOURCE: IAEA Nuclear Safety and Security Glossary, 2022 (Interim) Edition]

3.1.11**dependability**

overall trustworthiness of a system; that is, the extent to which reliance can justifiably be placed on this system. Reliability, availability and safety are attributes of dependability

[SOURCE: IAEA Nuclear Safety and Security Glossary, 2022 (Interim) Edition]

3.1.12**deterministic software**

software that allows to know, the execution path for each situation envisaged for the software, the corresponding expected outputs of the software and the use of the resources for each of these paths

3.1.13**diversity**

presence of two or more independent (redundant) systems or components to perform an identified function, where the different systems or components have different attributes so as to reduce the possibility of common cause failure, including common mode failure

Note 1 to entry: When the term “diversity” is used with an additional attribute, the term diversity indicates the general meaning “existence of two or more different ways or means of achieving a specified objective”, while the attribute indicates the characteristics of the different ways applied, for example, functional diversity, equipment diversity, signal diversity.

[SOURCE: IAEA Nuclear Safety and Security Glossary, 2022 (Interim) Edition]

3.1.14**dynamic analysis**

process of evaluating a system or component based on its behaviour during execution

Note 1 to entry: In contrast to static analysis (see 3.1.36).

3.1.15**failure**

loss of the ability of a structure, system or component to function within acceptance criteria

Note 1 to entry: The structure, system or component is considered to fail when it becomes incapable of functioning, whether or not this is necessary at that time.

Note 2 to entry: A failure in, for example, a backup system is not necessarily manifest until the system is called upon to function, either during testing or on failure of the system it is backing up.

Note 3 to entry: A failure can be the result of, for example, a hardware fault, a software fault, a system fault, an operator error or a maintenance error.

Note 4 to entry: See 3.1.16.

[SOURCE: IAEA Nuclear Safety and Security Glossary, 2022 (Interim) Edition]

3.1.16**fault**

defect in a hardware, software or system component

Note 1 to entry: A fault in a system can be due to a random failure of a system component, that results, for example, from hardware degradation due to ageing. It can also be a systematic fault, for example, software fault, which results from design errors.

Note 2 to entry: A fault (notably a design fault) can remain undetected in a system until specific conditions are such that the result produced does not conform to the intended function, that is, a failure of the system occurs.

[SOURCE: IEC 61513:2026, 3.24]

3.1.17**firmware**

software which is closely coupled to the hardware characteristics on which it is installed

[SOURCE: IAEA Nuclear Safety and Security Glossary, 2022 (Interim) Edition]

3.1.18**general-purpose language**

computer language designed to address all types of usage

Note 1 to entry: The operational system software is usually implemented using general-purpose languages.

Note 2 to entry: Examples: Ada, C.

Note 3 to entry: See 3.1.3.

3.1.19**human error**

discrepancy between the human action taken or omitted, and that intended or required

[SOURCE: IEC 61513:2026, 3.31]

3.1.20**integration tests**

tests performed during the integration of several verified software modules, or during the hardware and software integration process, prior to computer-based system validation testing to verify compatibility of the software and the computer hardware

3.1.21**library**

collection of related software elements that are grouped together, but which are individually selected for inclusion in the final software product

3.1.22**operational system software**

part of the system software running on the target processor during system operation

EXAMPLE Operating system, input and output drivers, exception handler, communication software, application software libraries, self-supervision, redundancy and graceful degradation management.

Note 1 to entry: See 3.1.37.

3.1.23**pre-developed software**

software that already exists, is available as a commercial or proprietary product or as open-source software, and is being considered for use in an instrumentation and control system

Note 1 to entry: The IEC definition differs from the IAEA definition of "predeveloped item" because open-source software has been explicitly added as candidate pre-developed software.

[SOURCE: IAEA Nuclear Safety and Security Glossary, 2022 (Interim) Edition, adapted from "predeveloped item".]

3.1.24**programmable digital item**

item that relies on software instructions or programmable logic to accomplish a function

Note 1 to entry: In this term and its definition, the term item can be replaced by the terms: system or equipment or device.

Note 2 to entry: The main kinds of programmable digital items are computer-based items and programmable logic items.

Note 3 to entry: This term used by IEC SC 45A is equivalent to programmable electronic item (PE item) defined according to IEC 61508.

[SOURCE: IEC 62138:2018, 3.34]