BS IEC 61513:2011

BSI Standards Publication

Nuclear power plants — Instrumentation and control important to Safety — General requirement for systems

bsi.

...making excellence a habit.™

Document Sharing Hub

Full document details: BS IEC 61513:2011

National foreword

This British Standard is the UK implementation of IEC 61513:2011. It supersedes BS IEC 61513:2001 which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee NCE/8, Reactor instrumentation.

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.

© BSI 2011

ISBN 978 0 580 61774 4

ICS 27.120.20

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 October 2011.

Amendments issued since publication

Amd. No.	Date	Text affected

Documents
Document Sharing Hub

Full document details: BS IEC 61513:2011

IEC 61513

Edition 2.0 2011-08

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Nuclear power plants – Instrumentation and control important to safety – General requirements for systems

Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Exigences générales pour les systèmes

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

PRICE CODE
CODE PRIX XD

ICS 27.120.20

ISBN 978-2-88912-663-7

® Registered trademark of the International Electrotechnical Commission
Marque déposée de la Commission Electrotechnique Internationale

Documents
Document Sharing Hub

Full document details: BS IEC 61513:2011

CONTENTS

FOREWORD 5
INTRODUCTION 7
1 Scope 9
1.1 General 9
1.2 Application: new and pre-existing plants 9
1.3 Framework 9
2 Normative references 12
3 Terms and definitions 13
4 Symbols and abbreviations 26
5 Overall I&C safety life cycle 26
5.1 General 26
5.2 Deriving the I&C requirements from the plant safety design base 29
5.2.1 General 29
5.2.2 Review of the functional, performance and independence requirements 29
5.2.3 Review of the categorisation requirements 30
5.2.4 Review of plant constraints 31
5.3 Output documentation 32
5.4 Design of the overall I&C architecture and assignment of the I&C functions 32
5.4.1 General 32
5.4.2 Design of the I&C architecture 33
5.4.3 Assignment of functions to systems 36
5.4.4 Required analysis 37
5.5 Overall planning 38
5.5.1 General 38
5.5.2 Overall quality assurance programs 38
5.5.3 Overall security plan 38
5.5.4 Overall I&C integration and commissioning 39
5.5.5 Overall operation plan 41
5.5.6 Overall maintenance plan 42
5.5.7 Planning of training 42
5.6 Output documentation 43
5.6.1 General 43
5.6.2 Architectural design documentation 43
5.6.3 Functional assignment documentation 43
6 System safety life cycle 44
6.1 General 44
6.2 Requirements 46
6.2.1 General 46
6.2.2 System requirements specification 47
6.2.3 System specification 52
6.2.4 System detailed design and implementation 55
6.2.5 System integration 57
6.2.6 System validation 58
6.2.7 System installation 59
6.2.8 System design modification 59

AVA Documents
Document Sharing Hub
Full document details: BS IEC 61513:2011

6.3 System planning ... 59
6.3.1 General ... 59
6.3.2 System quality assurance plan ... 60
6.3.3 System security plan ... 62
6.3.4 System integration plan ... 62
6.3.5 System validation plan ... 63
6.3.6 System installation plan ... 63
6.3.7 System operation plan ... 64
6.3.8 System maintenance plan ... 64
6.4 Output documentation ... 65
6.4.1 General ... 65
6.4.2 System requirements specification documentation ... 65
6.4.3 System specification documentation ... 66
6.4.4 System detailed design documentation ... 67
6.4.5 System integration documentation ... 68
6.4.6 System validation documentation ... 69
6.4.7 System modification documentation ... 69
6.5 System qualification ... 70
6.5.1 General ... 70
6.5.2 Generic and application-specific qualification ... 70
6.5.3 Qualification plan ... 71
6.5.4 Additional qualification of interconnected systems ... 72
6.5.5 Maintaining qualification ... 73
6.5.6 Documentation ... 73
7 Overall integration and commissioning ... 74
7.1 General ... 74
7.2 Requirements on the objectives to be achieved ... 75
7.3 Output documentation ... 75
8 Overall operation and maintenance ... 75
8.1 General ... 75
8.2 Requirements on the objectives to be achieved ... 75
8.3 Output documentation ... 76
Annex A (informative) Basic safety issues in the NPP ... 77
Annex B (informative) Categorisation of functions and classification of systems ... 80
Annex C (informative) Qualitative defence approach against CCF ... 85
Annex D (informative) Relations of IEC 61508 with IEC 61513 and standards of the nuclear application sector ... 89
Annex E (informative) Changes to be performed in later revisions of SC 45A standards to adapt to this version of IEC 61513 ... 96
Bibliography ... 98

Figure 1 – Overall framework of this standard ... 11
Figure 2 – Typical relations of hardware and software in a computer-based system ... 25
Figure 3 – Relations between system failure, random failure and systematic fault ... 25
Figure 4 – Connections between the overall I&C safety life cycle and the safety life cycles of the individual I&C systems ... 29
Figure 5 – System safety life cycle ... 46

AVA Documents
Document Sharing Hub
Full document details: BS IEC 61513:2011

Figure 6 – Product- and plant-application-specific topics to be addressed in the system qualification plan 74
Figure B.1 – Relations between I&C functions and I&C systems 81
Figure C.1 – Examples of assignment of functions of a safety group to I&C systems 85

Table 1 – Overview of the overall I&C safety life cycle 27
Table 2 – Correlation between classes of I&C systems and categories of I&C functions 33
Table 3 – Overview of the system safety life cycle 44
Table B.1 – Typical classification of I&C systems 84
Table C.1 – Examples of CCF sensitive in safety groups 86

Documents
Document Sharing Hub
Full document details: BS IEC 61513:2011

INTERNATIONAL ELECTROTECHNICAL COMMISSION

NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL IMPORTANT TO SAFETY – GENERAL REQUIREMENTS FOR SYSTEMS

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 Publication(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. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements 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.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC 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 transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is 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 its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees 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 Publication or any other IEC 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 some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 61513 has been prepared by subcommittee 45A: Instrumentation and control of nuclear facilities, of IEC technical committee 45: Nuclear instrumentation.

This second edition cancels and replaces the first edition, published in 2001, and constitutes a technical revision.

The main technical changes with regard to the previous edition are as follows:

- to align the standard with the new revisions of IAEA NS-R-1 and NS-G-1.3, to review the existing requirements and to update the terminology and definitions;
- to take account of, as far as possible, requirements associated with standards published since the first edition, especially IEC 60880, IEC 61226, IEC 62138, IEC 62340 and IEC 60987;
- to take into account the fact that software engineering techniques have advanced significantly in the intervening years;

AVA Documents
Document Sharing Hub

- to integrate requirements for staff training.

The text of this standard is based on the following documents:

FDIS	Report on voting
45A/838/FDIS	45A/848/RVD

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

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

Documents
Document Sharing Hub
Full document details: BS IEC 61513:2011

INTRODUCTION

a) Technical background, main issues and organisation of the standard

This International Standard sets out requirements applicable to instrumentation and control systems and equipment (I&C systems) that are used to perform functions important to safety in nuclear power plants (NPPs).

This standard highlights the relations between

- the safety objectives of the NPP and the requirements for the overall architecture of the I&C systems important to safety;
- the overall architecture of the I&C systems and the requirements of the individual systems important to safety.

It is intended that the standard be used by designers, operators of NPPs (utilities), systems evaluators and by licensors.

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

IEC 61513 is the first level IEC SC 45A document tackling the issue of general requirements for systems. It is the entry point of the IEC SC 45A standard series.

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

c) Recommendations and limitations regarding the application of this standard

It is important to note that this standard establishes no additional functional requirements for safety systems.

To ensure that the standard will continue to be relevant in future years, the emphasis has been placed on issues of principle, rather than specific technologies.

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

The top-level document of the IEC SC 45A standard series is IEC 61513. It provides general requirements for I&C systems and equipment that are used to perform functions important to safety in NPPs. IEC 61513 structures the IEC SC 45A standard series.

IEC 61513 refers directly to other IEC SC 45A standards for general topics related to categorisation of functions and classification of systems, qualification, separation of systems, defence against common cause failure, software aspects of computer-based systems, hardware aspects of computer-based systems, and control room design. The standards referenced directly at this second level should be considered together with IEC 61513 as a consistent document set.

At a third level, IEC SC 45A standards not directly referenced by IEC 61513 are standards related to specific equipment, technical methods, or specific activities. Usually these documents, which make reference to second-level documents for general topics, can be used on their own.

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

Documents
Document Sharing Hub
Full document details: BS IEC 61513:2011

IEC 61513 has adopted a presentation format similar to the basic safety publication IEC 61508, with an overall safety life-cycle framework and a system life-cycle framework. Regarding nuclear safety, it provides the interpretation of the general requirements of IEC 61508-1 [1][1], IEC 61508-2 and IEC 61508-4, for the nuclear application sector. In this framework, IEC 60880 and IEC 62138 correspond to IEC 61508-3 [2] for the nuclear application sector.

IEC 61513 refers to ISO as well as to IAEA GS-R-3 and IAEA GS-G-3.1 for topics related to quality assurance (QA).

The IEC SC 45A standards series consistently implements and details the principles and basic safety aspects provided in the IAEA code on the safety of NPPs and in the IAEA safety series, in particular the requirements document NS-R-1, establishing safety requirements related to the design of nuclear power plants, and the safety guide NS-G-1.3 dealing with instrumentation and control systems important to safety in nuclear power plants. The terminology and definitions used by SC 45A standards are consistent with those used by the IAEA.

NOTE It is assumed that for the design of I&C systems in NPPs that implement conventional safety functions (e.g. to address worker safety, asset protection, protection from chemical hazards and process energy hazards), international or national standards would be applied, that are based on the requirements of such a standard as the IEC 61508 series.

[1] References in square brackets refer to the bibliography.

Documents
Document Sharing Hub
Full document details: BS IEC 61513:2011

NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL IMPORTANT TO SAFETY – GENERAL REQUIREMENTS FOR SYSTEMS

1 Scope

1.1 General

I&C systems important to safety may be implemented using conventional hard-wired equipment, computer-based (CB) equipment or by using a combination of both types of equipment (see Note 1). This International Standard provides requirements and recommendations (see Note 2) for the overall I&C architecture which may contain either or both technologies.

This standard highlights also the need for complete and precise requirements, derived from the plant safety goals, as a pre-requisite for generating the comprehensive requirements for the overall I&C architecture, and hence for the individual I&C systems important to safety.

This standard introduces the concept of a safety life cycle for the overall I&C architecture, and a safety life cycle for the individual systems. By this, it highlights the relations between the safety objectives of the NPP and the requirements for the overall architecture of the I&C systems important to safety, and the relations between the overall I&C architecture and the requirements of the individual systems important to safety.

The life cycles illustrated in, and followed by, this standard are not the only ones possible; other life cycles may be followed, provided that the objectives stated in this standard are satisfied.

NOTE 1 I&C systems may also use electronic modules based on complex electronic components such as ASICs or FPGA. Depending on the scope and functionality of these components, they may be treated according to the guidance for conventional electronic equipment, or similar to CB equipment. A significant part of the guidance for CB equipment is also applicable to the design of equipment with complex electronic components, including e.g. the concepts of re-using pre-existing designs, and the evaluation of design errors in software or complex hardware designs.

NOTE 2 In the following, “requirement” is used as a comprehensive term for both requirements and recommendations. The distinction appears at the level of the specific provisions where requirements are expressed by “shall” and recommendations by “should”.

1.2 Application: new and pre-existing plants

This standard applies to the I&C of new nuclear power plants as well as to I&C up-grading or back-fitting of existing plants.

For existing plants, only a subset of requirements is applicable and this subset should be identified at the beginning of any project.

1.3 Framework

The standard comprises four normative clauses (an overview is provided in Figure 1):

- Clause 5 addresses the overall architecture of the I&C systems important to safety:
  - defining requirements for the I&C functions, and associated systems and equipment derived from the safety analysis of the NPP, the categorisation of I&C functions, and the plant lay-out and operational context;
  - structuring the overall I&C architecture, dividing it into a number of systems and assigning the I&C functions to systems. Design criteria are identified, including those to give defence in depth and to minimize the potential for common cause failure (CCF);

AVA Documents
Document Sharing Hub

– planning the overall architecture of the I&C systems.

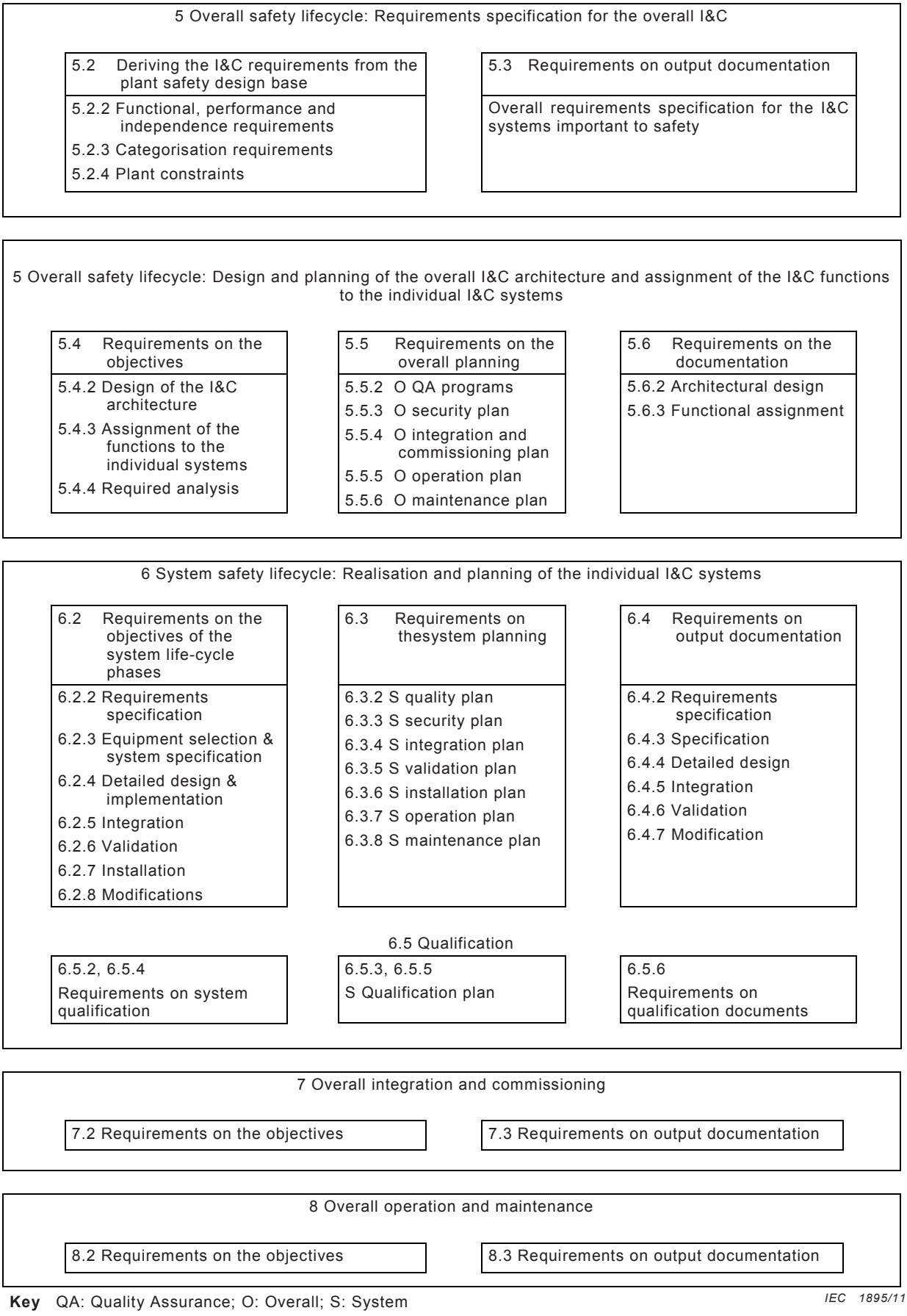
- Clause 6 addresses the requirements for the individual I&C systems important to safety, particularly the requirements for computer-based systems. This includes differentiation of requirements according to the safety category of the I&C functions which are implemented;
- Clauses 7 and 8 address the overall integration, commissioning, operation and maintenance of the I&C systems.

NOTE Figure 1 outlines the structure of the standard. It does not necessarily present the timely order of activities which may be in reality partially executed in parallel, or include iterations.

Additionally, the standard provides informative annexes:

- Annex A highlights the relations between IAEA and basic safety concepts that are used throughout this standard;
- Annex B provides information on the categorisation/classification principles;
- Annex C gives examples of I&C sensitivity to CCF;
- Annex D provides guidance to support comparison of this standard with parts 1, 2 and 4 of IEC 61508. This annex surveys the main requirements of IEC 61508 to verify that the issues relevant to safety are adequately addressed, considers the use of common terms and explains the reason for adopting different or complementary techniques or terms;
- Annex E indicates modifications to be made in future revisions of daughter standards of IEC 61513 to make them consistent and to minimize overlapping contents.

Documents
Document Sharing Hub
Full document details: BS IEC 61513:2011



Key QA: Quality Assurance; O: Overall; S: System

Figure 1 – Overall framework of this standard

Documents
Document Sharing Hub
Full document details: BS IEC 61513:2011

2 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.

IEC 60671, *Nuclear power plants – Instrumentation and control systems important to safety – Surveillance testing*

IEC 60709, *Nuclear power plants – Instrumentation and control systems important to safety – Separation*

IEC 60780, *Nuclear power plants – Electrical equipment of the safety system – Qualification*

IEC 60880:2006, *Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions*

IEC 60964:2009, *Nuclear power plants – Control rooms – Design*

IEC 60965, *Nuclear power plants – Control rooms – Supplementary control points for reactor shutdown without access to the main control room*

IEC 60980, *Recommended practices for seismic qualification of electrical equipment of the safety system for nuclear generating stations*

IEC 60987:2007, *Nuclear power plants – Instrumentation and control important to safety – Hardware design requirements for computer-based systems*

IEC 61000-4-1, *Electromagnetic compatibility (EMC) – Part 4-1: Testing and measurement techniques – Overview of IEC 61000-4 series*

IEC 61000-4-2, *Electromagnetic compatibility (EMC) – Part 4-2: Testing and measurement techniques – Electrostatic discharge immunity test*

IEC 61000-4-3, *Electromagnetic compatibility (EMC) – Part 4-3: Testing and measurement techniques – Radiated, radio-frequency, electromagnetic field immunity test*

IEC 61000-4-4, *Electromagnetic compatibility (EMC) – Part 4-4: Testing and measurement techniques – Electrical fast transient/burst immunity test*

IEC 61000-4-5, *Electromagnetic compatibility (EMC) – Part 4-5: Testing and measurement techniques – Surge immunity test*

IEC 61000-4-6, *Electromagnetic compatibility (EMC) – Part 4-6: Testing and measurement techniques – Immunity to conducted disturbances, induced by radio-frequency fields*

IEC 61226:2009, *Nuclear power plants – Instrumentation and control systems important to safety – Classification of instrumentation and control functions*

IEC 61500, *Nuclear power plants – Instrumentation and control important to safety – Data communication in systems performing category A functions*

IEC 61508-2:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

Documents
Document Sharing Hub
Full document details: BS IEC 61513:2011

IEC 61508-4:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations*

IEC 62138:2004, *Nuclear power plants – Instrumentation and control important for safety – Software aspects for computer-based systems performing category B or C functions*

IEC 62340, *Nuclear power plants – Instrumentation and control systems important to safety – Requirements for coping with common cause failure (CCF)*

ISO 9001:2008, *Quality management systems – Requirements*

IAEA INSAG-10:1996, *Defence in Depth in Nuclear Safety*

IAEA NS-R-1:2000, *Safety of Nuclear Power Plants: Design*

IAEA GS-R-3:2006, *The Management System for Facilities and Activities Safety – Requirements*

IAEA GS-G-3.1:2006, *Application of the Management System for Facilities and Activities – Safety Guide*

IAEA NS-G-1.3:2002, *Instrumentation and Control Systems Important to Safety in Nuclear Power Plants*

IAEA 75-INSAG-3 Rev. 1 – INSAG 12:1999, *Basic Safety Principles for Nuclear Power Plants*

3 Terms and definitions

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

3.1
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

NOTE 1 See also “I&C function”, “I&C system”, “application software”.

NOTE 2 An application function is normally a subfunction of an I&C function.

3.2
application software
part of the software of an I&C system that implements the application functions

NOTE 1 See also “application function”, “application software library”, “system software”.

NOTE 2 Application software contrasts with system software.

NOTE 3 See also Figure 2.

NOTE 4 In the context of complex electronic components, the term “application logic” may be inferred instead of “application software” where appropriate throughout this standard.

3.3
application software library
collection of software modules implementing typical application functions

NOTE 1 When using pre-existing equipment, such a library is considered to be part of the system software and qualified as such.

Documents
Document Sharing Hub
Full document details: BS IEC 61513:2011

NOTE 2 See also Figure 2.

3.4
category of an I&C function
one of three possible safety assignments (A, B, C) of I&C functions resulting from considerations of the safety relevance of the function to be performed. An unclassified assignment may be made if the function has no importance to safety

NOTE 1 See also “class of an I&C system”, “I&C function”.

NOTE 2 IEC 61226 defines categories of I&C functions. To each category there corresponds a set of requirements applicable on both the I&C function (concerning its specification, design, implementation, verification and validation) and the whole chain of items which are necessary to implement the function (concerning the properties and the related qualification) regardless of how these items are distributed in a number of interconnected I&C systems. For more clarity, this standard defines categories of I&C functions and classes of I&C systems and establishes a relation between the category of the function and the minimal required class for the associated systems and equipment.

3.5
channel
an arrangement of interconnected components within a system that initiates a single output. A channel loses its identity where the single-output signals are combined with signals from another channel (e.g., from a monitoring channel or a safety actuation channel).

[IAEA Safety Glossary, 2007 Edition] [3]

3.6
class of an I&C system
one of three possible assignments (1, 2, 3) of I&C systems important to safety resulting from consideration of their requirement to implement I&C functions of different safety importance. An unclassified assignment is made if the I&C system does not implement functions important to safety

NOTE See also “category of an I&C function”, “items important to safety”, “safety systems”.

3.7
commissioning
the process by means of which systems and components of facilities and activities, having been constructed, are made operational and verified to be in accordance with the design and to have met the required performance criteria

NOTE Commissioning may include both non-nuclear/non-radioactive and nuclear/radioactive testing.

[IAEA Safety Glossary, 2007 Edition]

3.8
common cause failure
CCF
failure of two or more structures, systems or components due to a single event or cause

[IAEA Safety Glossary 2007 Edition, Modified]

NOTE 1 Common causes may be internal or external to an I&C system.

NOTE 2 The IEC definition differs from the IAEA definition in two points:

1) The term “specific” was deleted because otherwise the definition of CCF is not consistent with the definition of CMF “Common mode failure”. Furthermore, this additional word is not necessary in order to understand the definition.

2) The word “and” was replaced by “or” because IEC/SC 45A experts thought it was a typing fault. In the online IAEA dictionary (NUSAFE) this correction was already done.

Documents
Document Sharing Hub
Full document details: BS IEC 61513:2011

3.9
complexity
degree to which a system or component has a design, implementation or behaviour that is difficult to understand and verify

[IEEE 610, modified] [4]

3.10
component
one of the parts that make up a system. A component may be hardware or software and may be subdivided into other components

[IEEE 610]

NOTE 1 See also “I&C system”, “equipment”.

NOTE 2 The terms “equipment”, “component”, and “module” are often used interchangeably. The relationship of these terms is not yet standardised.

NOTE 3 This IEC/SC 45A definition is in principle compatible with the sub-definition of “Component” given in the frame of the 2007 edition of the IAEA Safety Glossary definition of “Structures Systems and Components (SCC)”. Nevertheless as only examples of hardware components are given, this can mislead the reader and IEC/SC 45A prefer to use a definition which explicitly covers software components.

3.11
computer-based system
I&C system whose functions are mostly dependent on, or completely performed by microprocessors, programmed electronic equipment or computers

NOTE Equivalent to digital system, software-based system, programmed system.

3.12
configuration management
the process of identifying and documenting the characteristics of a facility’s structures, systems and components (including computer systems and software), and of ensuring that changes to these characteristics are properly developed, assessed, approved, issued, implemented, verified, recorded and incorporated into the facility documentation

[IAEA Safety Glossary, 2007 Edition]

3.13
data
representation of information or instructions in a manner suitable for communication, interpretation, or processing by computers

[IEEE 610, modified]

NOTE See Figure 2.

3.14
defence-in-depth
the application of more than one protective measure for a given safety objective, such that the objective is achieved even if one of the protective measures fails

[IAEA Safety Glossary, 2007 Edition]

NOTE See also Clause A.4.

3.15
diversity
presence of two or more 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

AVA Documents
Document Sharing Hub

Full document details: BS IEC 61513:2011

[IAEA Safety Glossary edition 2007, modified]

NOTE 1 When “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”, where the attribute indicates the characteristics of the different ways applied, e.g. functional diversity, equipment diversity, signal diversity.

NOTE 2 See also “functional diversity”

3.16
equipment
one or more parts of a system. An item of equipment is a single definable (and usually removable) element or part of a system

NOTE 1 See also “component”, “I&C system”.

NOTE 2 Equipment may include software.

NOTE 3 The terms “equipment”, “component”, and “module” are often used interchangeably. The relationship of these terms is not yet standardised.

NOTE 4 This definition deviates from that provided in IEC 60780. The deviation is justified by the fact that IEC 61513 considers "equipment" as part of a system whereas IEC 60780 considers equipment as the object of qualification.

3.17
equipment family
set of hardware and software components that may work co-operatively in one or more defined architectures (configurations). The development of plant specific configurations and of the related application software may be supported by software tools. An equipment family usually provides a number of standard functionalities (e.g. application functions library) that may be combined to generate specific application software

NOTE 1 See also “functionality”, “application software”, “application software library”.

NOTE 2 An equipment family may be a product of a defined manufacturer or a set of products interconnected and adapted by a supplier.

NOTE 3 The term “equipment platform” is sometimes used as a synonym of “equipment family”.

3.18
error
discrepancy between a computed, observed or measured value or condition and the true, specified or theoretical value or condition

NOTE See Figure 3.

3.19
evaluation (of a system property)
attribution of a qualitative or quantitative value to that system property

[IEC 61069-1:1991, 2.2.2] [5]

3.20
failure
loss of the ability of a structure, system or component to function within acceptance criteria

[IAEA Safety Glossary edition 2007, modified]

NOTE 1 Equipment is considered to fail when it becomes incapable of functioning, whether or not it is needed at that time. A failure in, for example, a backup system may not be manifest until the system is called upon to function, either during testing or on failure of the system it is backing up.

NOTE 2 A failure is the result of a hardware fault, software fault, system fault, or operator or maintenance error, and the associated signal trajectory which results in the failure.

NOTE 3 See also “fault”, “software failure”.

Documents
Document Sharing Hub
Full document details: BS IEC 61513:2011

NOTE 4 IEC/SC 45A experts consider that the IAEA definition lacks the concept that a failure is an event and not a state. IEC/SC 45A experts proposed that the IAEA definition should be modified to take this point into account.

3.21
fault
defect in a hardware, software or system component

NOTE 1 See also Figure 3.

NOTE 2 Faults may be originated from random failures, that result e.g. from hardware degradation due to ageing, and may be systematic faults, e.g. software faults, which result from design errors.

NOTE 3 A fault (notably a design fault) may remain undetected in a system until specific conditions are such that the result produced does not conform to the intended function, i.e. a failure occurs.

NOTE 4 See also “software fault”.

3.22
functional diversity
application of diversity at the level of process engineering application functions (for example, to have trip activation on both pressure and temperature limit)

[IEC 60880:2006, 3.19, modified]

NOTE IAEA Safety Glossary, edition 2007, does not give a definition for functional diversity but gives examples of means to achieve it. This IEC/SC 45A definition is compatible with the means indicated in the IAEA safety glossary to achieve functional diversity.

3.23
functional validation
verification of the correctness of the application functions specifications against the top level plant functional and performance requirements. It is complementary to the system validation that verifies the compliance of the system with the functions specification

3.24
functionality
attribute of a function which defines the operations which transform input information into output information

NOTE Functionality of application functions generally affect the plant operation. Input may be obtained from sensors, operators, other equipment, or from other software. Outputs may be directed to actuators, operators, other equipment, or other software (see IEC 61508-2).

3.25
hazard
event having the potential to cause injury to plant personnel or damage to components, equipment or structures. Hazards are divided into internal hazards and external hazards

NOTE 1 Internal hazards are, for example, fire and flooding. Internal hazards may be also a consequence of a PIE (for example, loss of coolant accident, steam-line break).

NOTE 2 External hazards are, for example, earthquake and lightning.

3.26
human error (or mistake)
human action that produces an unintended result

[IEC 60880:2006, 3.21]

3.27
I&C architecture
organisational structure of the I&C systems of the plant which are important to safety

NOTE 1 See also “I&C system architecture”, “I&C system”.

Documents
Document Sharing Hub
Full document details: BS IEC 61513:2011

NOTE 2 The organisational structure defines notably the main functions, class and boundaries of each system, the interconnections and independence between systems, the priority and voting between concurrently acting signals, the HMI.

NOTE 3 In this standard the term designates only a subset of the whole I&C architecture of the plant. The latter includes also the unclassified systems and equipment.

NOTE 4 For simplicity reasons, the term "overall I&C architecture" is used as short form for "overall architecture of the I&C systems important to safety".

3.28
I&C function
function to control, operate and/or monitor a defined part of the process

NOTE 1 The term "I&C function" is used by process engineers to structure the functional requirements for the I&C. An I&C function is defined in such a way that it

– gives a complete representation of a functional objective,
– can be categorised according to its degree of importance to safety,
– comprises the smallest entity, from sensor to actuator, to achieve its functional objective.

NOTE 2 An I&C function may be subdivided into a number of subfunctions (for example, measuring function, control function, actuation function) for the purpose of allocation to I&C systems.

3.29
I&C system
system, based on electrical and/or electronic and/or programmable electronic technology, performing I&C functions as well as service and monitoring functions related to the operation of the system itself

The term is used as a general term which encompasses all elements of the system such as internal power supplies, sensors and other input devices, data highways and other communication paths, interfaces to actuators and other output devices (see Note 2). The different functions within a system may use dedicated or shared resources.

NOTE 1 See also "system" and "I&C function".

NOTE 2 The elements included in a specific I&C system are defined in the specification of the boundaries of the system.

NOTE 3 According to their typical functionality, IAEA distinguishes between automation / control systems, HMI systems, interlock systems and protection systems (see Clause B.4).

3.30
I&C system architecture
organisational structure of an I&C system

NOTE See also "I&C architecture".

3.31
independent equipment
equipment that possesses both of the following characteristics:

1) the ability to perform its required function is unaffected by the operation or failure of other equipment;
2) the ability to perform its function is unaffected by the occurrence of the effects resulting from the postulated initiating event for which it is required to function

[IAEA Safety Glossary, 2007 Edition]

NOTE Means to achieve independence in the design are electrical isolation (also called functional isolation in IAEA documents), physical separation and communications independence.

Documents
Document Sharing Hub
Full document details: BS IEC 61513:2011

3.32
interrupt
suspension of a process such as the execution of a computer program, caused by an event external to that process

[IEEE 610] [1]

3.33
item important to safety
item that is part of a safety group and/or whose malfunction or failure could lead to radiation exposure of the site personnel or members of the public

Items important to safety include:

a) those structures, systems and components whose malfunction or failure could lead to undue radiation exposure of the site personnel or members of the public;
b) those structures, systems and components that prevent anticipated operational occurrences from leading to accident conditions;
c) those features which are provided to mitigate the consequences of malfunction or failure of structures, systems or components

[IAEA Safety Glossary, 2007 Edition]

NOTE 1 This definition is intended to encompass all aspects of nuclear safety.

NOTE 2 In this standard, the items considered will be mainly I&C systems or I&C functions.

NOTE 3 See also “I&C function”.

3.34
overall I&C safety life cycle
necessary activities involved in the implementation of the systems and equipment important to safety of the overall I&C architecture, occurring during a period of time that starts with deriving I&C requirements from the plant safety design base and finishes when none of the I&C systems are available for use

[IEC 61508-4:2010, 3.7.1, modified] [6]

NOTE 1 The overall safety lifecycle of the I&C induces requirements for the individual system safety life cycles.

NOTE 2 See also “system safety lifecycle”.

3.35
postulated initiating event
PIE
event identified during design as capable of leading to anticipated operational occurrences or accident conditions

[IAEA Safety Glossary, 2007 Edition]

3.36
pre-existing items
hard- or software or software-based equipment that already exists, is available as a commercial or proprietary product, and is being considered for use

NOTE This definition includes that of pre-developed software, see IEC 60880:2006, 3.28.

3.37
project organisation
organisation(s) or individuals that have responsibility during the phases of the overall I&C safety life cycle and/or during the phases of the safety life cycles of the I&C systems, to

AVA Documents
Document Sharing Hub
Full document details: BS IEC 61513:2011

define and perform all management and technical activities concerning the I&C functions, systems and equipment important to safety

NOTE This term is to be contrasted with “operating organisation”.

3.38
qualification
process of determining whether a system or component is suitable for operational use. The qualification is performed in the context of a specific class of the I&C system and a specific set of qualification requirements

NOTE 1 The qualification requirements are derived from the specific class of the I&C system and a specific application context.

NOTE 2 I&C systems are typically implemented on the basis of interacting sets of equipment. Such equipment may be developed as part of the project, or it may be pre-existing equipment (i.e. developed in the framework of a previous project, or being a commercial off-the-shelf product). Typically, qualification of an “I&C system” is accomplished in stages: first by the qualification of individual pre-existing equipment (usually early in the system realization process); in a second step by the qualification of the integrated I&C system (i.e. the final realized design).

NOTE 3 Qualification of I&C systems is always a plant- and application-specific activity. However, it may rely to a large degree on qualification activities performed outside the framework of a specific plant design (these are called “generic qualification” or “pre-qualification”). Pre-qualification may reduce the plant-specific qualification effort significantly, however, the application-specific qualification requirements should still be shown to be met.

3.39
quality
degree to which a set of inherent characteristics fulfils requirements

[ISO 9000:2005] [6]

3.40
quality assurance
function of a management system that provides confidence that specific requirements will be fulfilled

[IAEA Safety Glossary, 2007 Edition]

NOTE This definition is compatible with that of ISO 8402:1994, 3.5 [7].

3.41
quality plan
document setting out the specific quality practices, resources and sequence of activities relevant to a particular product, project or contract

3.42
redundancy
provision of alternative (identical or diverse) structures, systems or components, so that any one can perform the required function regardless of the state of operation or failure of any other

[IAEA Safety Glossary, 2007 Edition]

3.43
reliability
probability that a device, system or facility will meet its minimum performance requirements when called upon to do so for a specified time under stated operating conditions

[IAEA Safety Glossary, 2007 Edition, modified]

NOTE 1 The reliability of a computer-based system includes the reliability of its hardware which is usually quantified and the reliability of its software which is usually a qualitative measure because there are no generally recognised means to quantify the reliability of software.

AVA Documents
Document Sharing Hub
Full document details: BS IEC 61513:2011

NOTE 2 This definition differs from 2007 edition of the IAEA Safety Glossary one which is "The probability that a system or component will meet its minimum performance requirements when called upon to do so." IEC/SC 45A experts indicated that this IAEA definition is not consistent with general practice in that it does not include the concept of mission time.

3.44
requirement
expression in the content of a document conveying criteria to be fulfilled if compliance with the document is to be claimed and from which no deviation is permitted

[ISO/IEC Directives, Part 2, 2004, 3.12.1] [8]

NOTE 1 In IEC/SC 45A documents the following types of requirements are distinguished:

Safety requirements – Requirements imposed by authorities (legal, regulatory or standards bodies) and design organizations on the safety of the NPP in terms of impact on individuals, society and environment during the NPP lifecycle.

Functional and performance requirements – Functional requirements state the actions to be taken by the system in response to specific signals or conditions, and performance requirements define features such as response times and accuracy.

Operational requirements – Requirements on the operational capacity and ability of the plant imposed by the owner.

Plant design requirements – Technical requirements on plant general design for the fulfilment of the safety requirements and operational requirements on the plant.

System design requirements – Design requirements on individual systems to give a design of the complete plant fulfilling the plant design requirements.

Equipment requirements – Requirements on individual equipment for its fulfilment of the demands of the system design.

NOTE 2 The IAEA Safety Glossary, Edition 2007 contains the following definition:

Required, requirement – Required by (national or international) law or regulations, or by IAEA Safety Fundamentals or Safety requirements.

This IAEA definition is useful in the framework of IAEA publications, but too narrow for use in a technical standard. It corresponds to the IEC/SC 45A definition "Safety requirement" as provided in Note 1.

NOTE 3 It is understood that any deviations from the requirements will be justified.

3.45
reusable software
software module that can be used in more than one computer program or software system

[IEEE 610, modified]

3.46
safety group
assembly of equipment designated to perform all actions required for a particular postulated initiating event to ensure that the limits specified in the design basis for anticipated operational occurrences and design basis accidents are not exceeded

[IAEA Safety Glossary, 2007 Edition]

3.47
safety system
system important to safety, provided to ensure the safe shutdown of the reactor and the residual heat removal from the core, or to limit the consequences of anticipated operational occurrences and design basis accidents

[IAEA Safety Glossary, 2007 Edition]

Documents
Document Sharing Hub
Full document details: BS IEC 61513:2011

3.48
security
capability of the CB system to protect information and data so that unauthorized persons or systems cannot read or modify relevant data or perform or inhibit control actions, and authorized persons or systems are not denied access

[ISO/IEC 12207:2008, 4.39, modified] [9]

3.49
single failure
loss of capability of a component to perform its intended safety function(s), and any consequential failure(s) which result from it

[IAEA Safety Glossary, 2007 Edition, modified]

NOTE This definition differs from the 2007 edition of the IAEA Safety Glossary one which is "A failure which results in the loss of capability of a system or component to perform its intended safety function(s), and any consequential failure(s) which result from it". The term "system" was suppressed because the original IAEA definition for single failure was deemed inadequate by IEC/SC 45A experts in that it must result in the loss of system function. Systems that meet the single failure criterion would therefore have no single failures. It seems that this could lead to circular arguments regarding compliance with the single failure criteria. Furthermore, this modified IAEA definition is aligned with the "failure" IEC/SC 45A definition.

3.50
single failure criterion
criterion (or a requirement) applied to a system such that it must be capable of performing its safety task in the presence of any single failure

[IAEA Safety Glossary, 2007 Edition]

NOTE See e.g. IAEA NS-R-1:2000, 5.37, for guidance how the single failure criterion is achieved and how it is applied to a safety group.

3.51
software
programs (i.e. sets of ordered instructions), data, rules and any associated documentation pertaining to the operation of a computer-based I&C system

3.52
software failure
system failure due to the activation of a design fault in a software component

NOTE 1 All software failures are due to design faults, since software consists solely of design and does not wear out or suffer from physical failure. Since the triggers which activate software faults are encountered at random during system operation, software failures also occur randomly.

NOTE 2 See also "failure", "fault", "software fault".

3.53
software fault
design fault located in a software component

NOTE See also "fault".

3.54
software reliability
component of the system reliability related to software failures

3.55
specification
document that specifies, in a complete, precise, verifiable manner, the requirements, design, behaviour or other characteristics of a system or component and, often, the procedures for determining whether these provisions have been satisfied

AVA Documents
Document Sharing Hub
Full document details: BS IEC 61513:2011

[IEC 60880:2006, 3.39]

3.56
system
set of components which interact according to a design, where an element of a system can be another system, called a subsystem

[IEC 61508-4:2010, 3.3.1, modified]

NOTE 1 See also “I&C system”.

NOTE 2 I&C systems are distinguished from mechanical systems and electrical systems of the NPP.

NOTE 3 This IEC/SC 45A definition is totally compatible with the sub-definition of “system” given in the frame of the 2007 edition of the IAEA Safety Glossary definition of “Structures Systems and Components (SCC)”.

3.57
system safety life cycle
necessary activities involved in the implementation of an I&C system important to safety occurring during a period of time that starts at a concept phase with the system requirements specification and finishes when the I&C system is no longer available for use

NOTE 1 The system safety life cycle refers to the activities of the overall I&C safety life cycle.

NOTE 2 See also “overall I&C safety life cycle”.

3.58
system software
software designed for a specific computer system or family of computer systems to facilitate the operation and maintenance of the computer system and associated programs, for example, operating systems, computers, utilities. System software is usually composed of operational system software and support software

NOTE 1 Operational system software: software running on the target processor during system operation, such as: operating system, input/output drivers, exception handler, communication software, application-software libraries, on-line diagnostic, redundancy and graceful degradation management.

NOTE 2 Support software: software that aids in the development, test, or maintenance of other software and of the system such as compilers, code generators, graphic editor, off-line diagnostic, verification and validation tools, etc.

NOTE 3 See also “application software”.

NOTE 4 See also Figure 2.

3.59
system validation
confirmation by examination and provision of other evidence that a system fulfils in its entirety the requirement specification as intended (functionality, response time, fault tolerance, robustness)

[IEC 60880:2006, 3.42]

NOTE The 2007 edition of the IAEA Safety Glossary gives the two following definitions:

> *Validation*: The process of determining whether a product or service is adequate to perform its intended function satisfactorily. Validation is broader in scope, and may involve a greater element of judgment than verification.
>
> *Computer system validation*: The process of testing and evaluating the integrated computer system (hardware and software) to ensure compliance with the functional, performance and interface requirements.

Firstly, the definition “system validation” is a specific case of validation. It refers to a specific product, namely to the validation of an I&C system. This is consistent with the IAEA definition. Secondly, the IEC definition specifies the reference of validation, namely the requirement specification whereas the IAEA definition only refers to the “intended function”.

AVA Documents
Document Sharing Hub
Full document details: BS IEC 61513:2011

3.60
systematic fault
fault related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors

[IEC 61508-4:2010, 3.6.6, modified]

3.61
type test(s)
conformity test made on one or more items representative of the production

[IEC 60050-394:2007, 40-02] [10]

3.62
verification
confirmation by examination and by provision of objective evidence that the results of an activity meet the objectives and requirements defined for this activity

[IEC 62138:2004, 3.35]

NOTE The 2007 edition of the IAEA Safety Glossary gives the two following definitions:

Validation: The process of determining whether a product or service is adequate to perform its intended function satisfactorily. Validation is broader in scope, and may involve a greater element of judgment than verification.

Verification: The process of determining whether the quality or performance of a product or service is as stated, as intended or as required.

The IAEA definition of “verification” is very similar to the IAEA one of « validation », as both address the final product or service.

In IEC SC 45A standards, the terms “verification” and “validation” refer to the result of the life cycle of specific products, namely I&C equipment and systems, but not to services in general.

Furthermore, “verification” and “validation” are used to identify two different and complementary types of assessments:

“*Verification*” indicates the assessment of the results of an individual activity against its inputs.

“*Validation*” indicates the assessment of the final product against its documented objectives and requirements.

Documents
Document Sharing Hub
Full document details: BS IEC 61513:2011

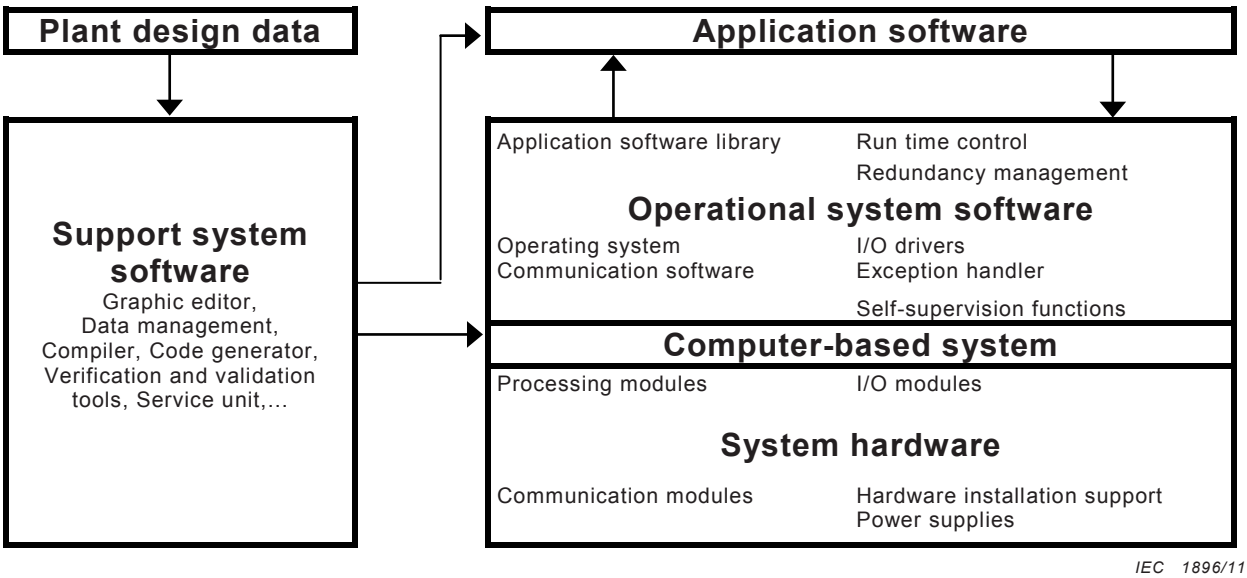


Figure 2 – Typical relations of hardware and software in a computer-based system

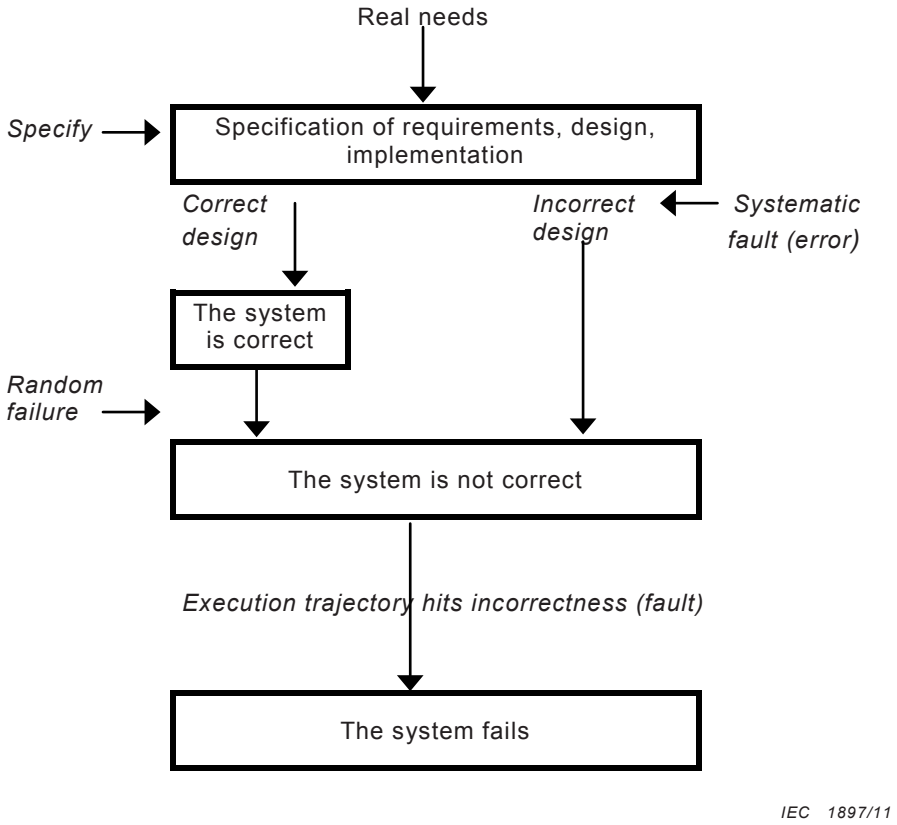


Figure 3 – Relations between system failure, random failure and systematic fault

Documents
Document Sharing Hub
Full document details: BS IEC 61513:2011

4 Symbols and abbreviations

ASIC	Application-specific integrated circuit
CB	Computer-based
CCF	Common-cause failure
CM	Configuration management
COTS	Commercial off-the-shelf
EMI	Electromagnetic interference
FPGA	Field-programmable gate array
HMI	Human machine interface
I&C	Instrumentation and control
I/O	Input/output
NPP	Nuclear power plant
PDS	Pre-developed software
PIE	Postulated initiating events
QA	Quality assurance

5 Overall I&C safety life cycle

5.1 General

The objective of this clause is to define how to

- derive the requirements for the architecture of the I&C systems important to safety from the safety design base of the NPP (see Clauses A.2 and A.3), and
- derive the requirements for the individual I&C systems important to safety from these overall requirements.

To ensure that all the plant safety requirements to be met by the I&C are captured, implemented, and maintained, a systematic approach is required. This is achieved by placing the activities associated with development, implementation and operation of I&C in the framework of a safety life cycle of the overall I&C. This life cycle refers in turn to the safety life cycles of the individual I&C systems (see Clause 6).

The phases of a typical overall I&C safety life cycle include

a) review of the plant safety design base including (see 5.2):
   - functional, performance and independence requirements;
   - functional categorisation;
   - constraints from the plant design framework;

b) definition of the overall requirements specification of the I&C functions, systems and equipment important to safety (see 5.3);

c) design of the overall I&C architecture and assignment of the I&C functions to individual systems and equipment (see 5.4);

d) definition of the overall planning (see 5.5);

e) realisation of the individual systems (see Clause 6);

f) overall integration and commissioning of the systems (see Clause 7);

g) overall operation and maintenance (see Clause 8);

Documents
Document Sharing Hub
Full document details: BS IEC 61513:2011

Numbers in brackets identify the clause and subclause of this standard where the relevant phase is addressed, while the objective, inputs to, outputs from, and scope of each phase are developed in Table 1.

The connections between this life cycle and the safety life cycles of the individual I&C systems are shown in simplified form in Figure 4.

a) the overall I&C safety life cycle is an iterative process where the outputs of each phase shall be verified as being consistent with the inputs from the preceding activities. A phase may start even if the activities of the preceding phase are not finished providing that adequate configuration controls have been applied which ensure that the overall consistency of the development process is maintained;

b) phase shall only be finished if the preceding phases have been completed.

Table 1 – Overview of the overall I&C safety life cycle

Clause or subclause	Inputs	Objectives of the activity	Scope	Outputs
5 Requirements placed upon the overall I&C safety life cycle and its relationship to the systems' life cycles				
5.2 Deriving the I&C requirements from the plant safety design base				
5.2.2 Review of the functional, performance and independence requirements	Plant safety design base documents Principles of plant operation	To identify – the overall functional and performance requirements of the I&C systems important to safety, – the defence in-depth concept of the plant and the independence requirements placed upon the I&C functions, – the automatic functions and operator task	Plant systems and related I&C systems important to safety	Identification of input requirements for 5.3
5.2.3 Review of the categorisation requirements	Plant safety categorisation	To identify the categorisation of I&C functions To verify for completeness To verify for feasibility of complex requirements	I&C functions important to safety	Identification of input requirements for 5.3
5.2.4 Review of plant constraints	Plant lay-out documents and design data base	To identify – plant/I&C systems boundaries, – constraints from support systems and plant layout, environmental conditions, – sources of potential internal and external hazards, – principles of plant operation and maintenance	Plant layout Plant systems I&C systems	Identification of constraints for the architectural design (see 5.4) and for the requirements specification of the individual I&C systems (see 6.2)
5.3 Output documentation	Outputs of 5.2	To develop the overall requirements specification of the I&C systems important to safety in terms of functional, performance, independence and categorisation requirements	I&C systems	Overall I&C requirements specification for 5.4
5.4 Design of the overall I&C architecture and assignment of the I&C functions				
5.4.2 Design of the I&C architecture	Output of 5.3	To design the overall I&C architecture suitable to implement the overall requirements specifications of the I&C systems important to safety To provide adequate measures against CCF potential	I&C functions and I&C systems	Detailed design of the safety I&C architecture in terms of automation systems, HMI and interconnections, tools (see 5.6.2)
5.4.3	Output of 5.4.2	To assign the I&C functions to the	I&C functions	Requirements for the

AVA Documents
Document Sharing Hub
Full document details: BS IEC 61513:2011

Clause or subclause	Inputs	Objectives of the activity	Scope	Outputs
Functional assignment	and 5.5 (Iteration with output of 6.4)	individual I&C systems and equipment To provide requirements (boundaries, classification, functionality, reliability and other required properties) for the individual I&C systems	and I&C systems	application functions of systems and HMI, the design of the I&C systems and the tools (see 5.6.3)
5.4.4 Required analysis	Outputs of 5.4.2 and 5.4.3	To assess reliability and defence against CCF To assess human factors	I&C functions and I&C systems	Assessment of reliability and defence against CCF (5.4.4.2) Assessment of human factors (5.4.4.3)
5.5 Overall planning	Output of 5.4	To develop plans for QA, security, integration, commissioning, operation and maintenance of systems	I&C systems working co-operatively	Plans for the designated activities
6 System safety life cycle	Output of 5.6	To specify and create I&C systems conforming to the I&C architecture specification (see Clause 6)	Individual I&C systems	Outputs are described in Table 3
7 Overall integration and commissioning	Output of 5.5.4 and 6.3.6	To test and commission the interconnected systems of the I&C architecture	I&C systems of the I&C architecture	Fully integrated and commissioned systems Report of the overall commissioning (see 7.3)
8 Overall operation and maintenance	Output of 5.5.5, 5.5.6 and 7.2	To operate maintain and repair the systems in order that the safety is maintained	I&C systems of the I&C architecture	Continuing achievement of functions. Records of operation and maintenance (see 8.3)
NOTE For a comparison of this definition of phases with that of IEC 61508-1, see Annex D.				

Documents
Document Sharing Hub
Full document details: BS IEC 61513:2011

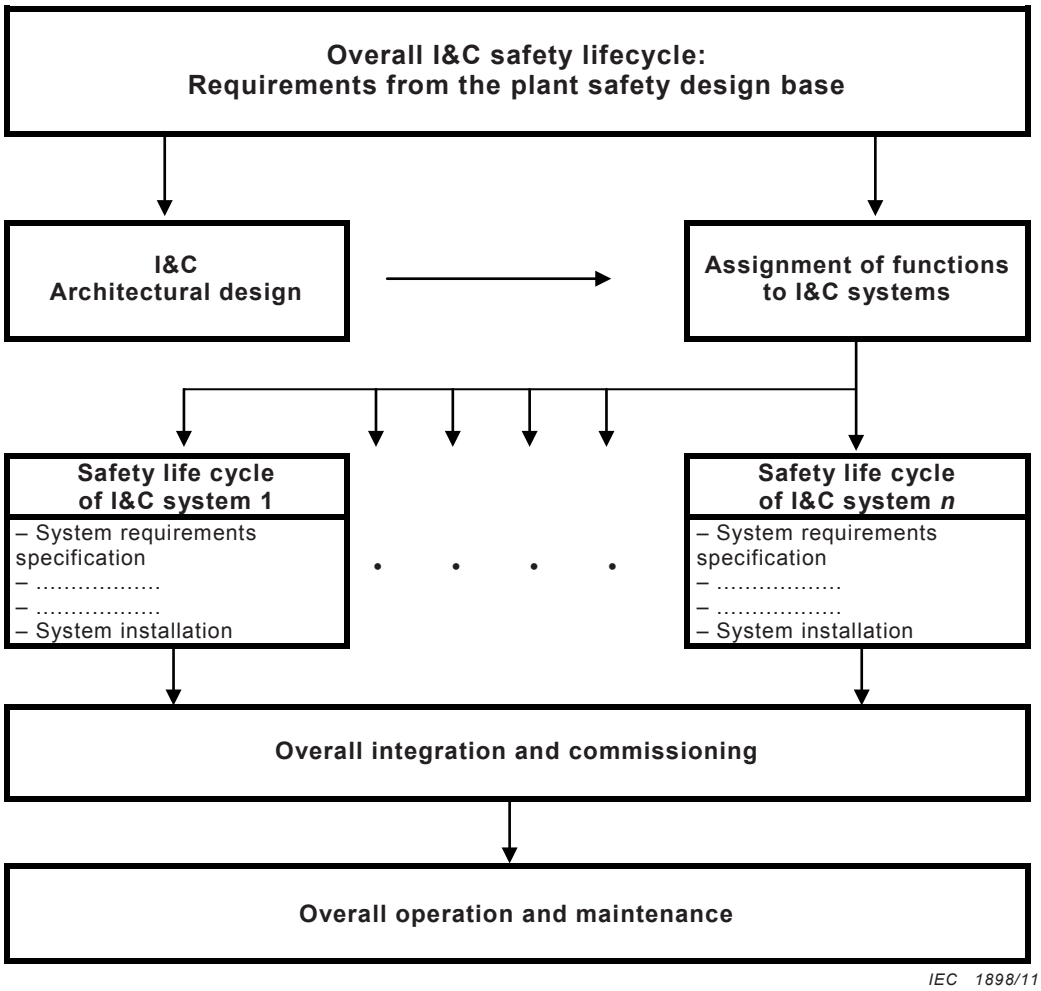


Figure 4 – Connections between the overall I&C safety life cycle and the safety life cycles of the individual I&C systems

5.2 Deriving the I&C requirements from the plant safety design base

5.2.1 General

The objective of the requirements of this subclause is to derive input requirements for the specification of the I&C systems and input constraints for the I&C architectural design, resulting from the plant safety design base and the plant design framework.

75-INSAG-3 defines a number of individual “safety principles” that together make up an “integrated overall safety approach” ensuring the safety of a NPP. These principles will be used in the design (IAEA NS-R-1) by considering all relevant “postulated initiating events” (PIEs) and successive physical barriers to keep radiation exposure to workers, public and the environment within limits (see Clauses A.2, A.3 and A.4). Following this approach, the plant design base specifies an appropriate quality level for the plant functions and systems necessary to maintain the plant in a normal operating state, to ensure the correct response to all PIEs, and to facilitate the long-term management of the plant following an accident.

5.2.2 Review of the functional, performance and independence requirements

The functional, performance and independence requirements for the I&C functions important to safety and the principles of operation of the plant are defined in the plant safety design base which is an inherent element of the overall I&C design project. The requirements

AVA Documents
Document Sharing Hub
Full document details: BS IEC 61513:2011