BS EN 61513:2013

BSI Standards Publication

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

National foreword

This British Standard is the UK implementation of EN 61513:2013. It is identical to IEC 61513:2011. It supersedes BS IEC 61513:2011 which is withdrawn.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.

Published by BSI Standards Limited 2013

ISBN 978 0 580 76695 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 March 2013.

Amendments issued since publication

Date	Text affected

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 61513

February 2013

ICS 27.120.20

English version

Nuclear power plants - Instrumentation and control important to safety - General requirements for systems (IEC 61513:2011)

Centrales nucléaires de puissance - Instrumentation et contrôle-commande importants pour la sûreté - Exigences générales pour les systèmes (CEI 61513:2011)

Kernkraftwerke - Leittechnik für Systeme mit sicherheitstechnischer Bedeutung - Allgemeine Systemanforderungen (IEC 61513:2011)

This European Standard was approved by CENELEC on 2013-01-14. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

CENELEC

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

Management Centre: Avenue Marnix 17, B - 1000 Brussels

Foreword

This document (EN 61513:2013) consists of the text of IEC 61513:2011 prepared by SC 45A "Instrumentation and control of nuclear facilities" of IEC/TC 45 "Nuclear instrumentation".

The following dates are fixed:

• latest date by which this document has to be implemented at national level by publication of an identical national standard or by endorsement	(dop)	2014-01-14
• latest date by which the national standards conflicting with this document have to be withdrawn	(dow)	2016-01-14

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

As stated in the nuclear safety directive 2009/71/EURATOM, Chapter 1, Article 2, item 2, Member States are not prevented from taking more stringent safety measures in the subject-matter covered by the Directive, in compliance with Community law. In a similar manner, this European Standard does not prevent Member States from taking more stringent nuclear safety measures in the subject-matter covered by this standard.

Endorsement notice

The text of the International Standard IEC 61513:2011 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following notes have to be added for the standards indicated:

IEC 61508-1:2010	NOTE	Harmonized as EN 61508-1:2010 (not modified).
IEC 61508-3:2010	NOTE	Harmonized as EN 61508-3:2010 (not modified).
IEC 61069-1:1991	NOTE	Harmonized as EN 61069-1:1993 (not modified).
IEC 62381	NOTE	Harmonized as EN 62381.
IEC 61000-6-2	NOTE	Harmonized as EN 61000-6-2.
IEC 61000-6-4	NOTE	Harmonized as EN 61000-6-4.
ISO 9000:2005	NOTE	Harmonized as EN ISO 9000:2005 (not modified).
ISO 8402:1994	NOTE	Harmonized as EN ISO 8402:1995 (not modified).

Annex ZA
(normative)

Normative references to international publications with their corresponding European publications

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

NOTE When an international publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

Publication	Year	Title	EN/HD	Year
IEC 60671	-	Nuclear power plants - Instrumentation and control systems important to safety - Surveillance testing	EN 60671	-
IEC 60709	-	Nuclear power plants - Instrumentation and control systems important to safety - Separation	EN 60709	-
IEC 60780	-	Nuclear power plants - Electrical equipment of the safety system - Qualification	EN 60780	-
IEC 60880	2006	Nuclear power plants - Instrumentation and control systems important to safety - Software aspects for computer-based systems performing category A functions	EN 60880	2009
IEC 60964	2009	Nuclear power plants - Control rooms - Design	EN 60964	2010
IEC 60965	-	Nuclear power plants - Control rooms - Supplementary control points for reactor shutdown without access to the main control room	EN 60965	-
IEC 60980	-	Recommended practices for seismic qualification of electrical equipment of the safety system for nuclear generating stations	-	-
IEC 60987 (mod)	2007	Nuclear power plants - Instrumentation and control important to safety - Hardware design requirements for computer-based systems	EN 60987	2009
IEC 61000-4-1	-	Electromagnetic compatibility (EMC) - Part 4-1: Testing and measurement techniques - Overview of IEC 61000-4 series	EN 61000-4-1	-
IEC 61000-4-2	-	Electromagnetic compatibility (EMC) - Part 4-2: Testing and measurement techniques - Electrostatic discharge immunity test	EN 61000-4-2	-
IEC 61000-4-3	-	Electromagnetic compatibility (EMC) - Part 4-3: Testing and measurement techniques - Radiated, radio-frequency, electromagnetic field immunity test	EN 61000-4-3	-
IEC 61000-4-4	-	Electromagnetic compatibility (EMC) - Part 4-4: Testing and measurement techniques - Electrical fast transient/burst immunity test	EN 61000-4-4	-

Publication	Year	Title	EN/HD	Year
IEC 61000-4-5	-	Electromagnetic compatibility (EMC) - Part 4-5: Testing and measurement techniques - Surge immunity test	EN 61000-4-5	-
IEC 61000-4-6	-	Electromagnetic compatibility (EMC) - Part 4-6: Testing and measurement techniques - Immunity to conducted disturbances, induced by radio-frequency fields	EN 61000-4-6	-
IEC 61226	2009	Nuclear power plants - Instrumentation and control important to safety - Classification of instrumentation and control functions	EN 61226	2010
IEC 61500	-	Nuclear power plants - Instrumentation and control important to safety - Data communication in systems performing category A functions	EN 61500	-
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	EN 61508-2	2010
IEC 61508-4	2010	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 4: Definitions and abbreviations	EN 61508-4	2010
IEC 62138	2004	Nuclear power plants - Instrumentation and control important for safety - Software aspects for computer-based systems performing category B or C functions	EN 62138	2009
IEC 62340	-	Nuclear power plants - Instrumentation and control systems important to safety - Requirements for coping with common cause failure (CCF)	EN 62340	-
ISO 9001	2008	Quality management systems - Requirements	EN ISO 9001	2008
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 for 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	-	-

CONTENTS

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.

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.

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);

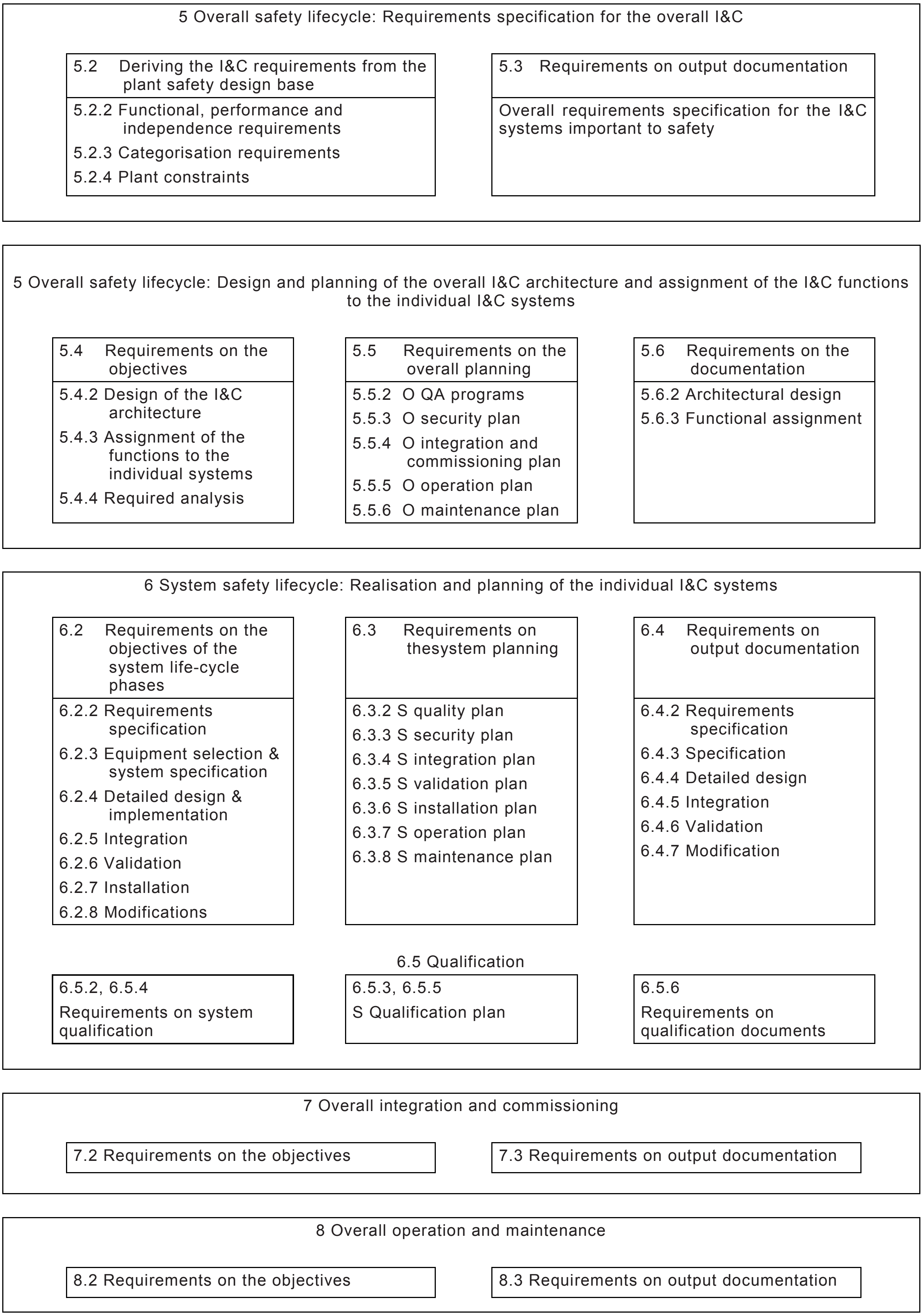
  – planning the overall architecture of the I&C systems.

- 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.



5 Overall safety lifecycle: Requirements specification for the overall I&C

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

5.2.2 Functional, performance and independence requirements

5.2.3 Categorisation requirements

5.2.4 Plant constraints

5.3 Requirements on output documentation

Overall requirements specification for the I&C systems important to safety

5 Overall safety lifecycle: Design and planning of the overall I&C architecture and assignment of the I&C functions to the individual I&C systems

5.4 Requirements on the objectives

5.4.2 Design of the I&C architecture

5.4.3 Assignment of the functions to the individual systems

5.4.4 Required analysis

5.5 Requirements on the overall planning

5.5.2 O QA programs

5.5.3 O security plan

5.5.4 O integration and commissioning plan

5.5.5 O operation plan

5.5.6 O maintenance plan

5.6 Requirements on the documentation

5.6.2 Architectural design

5.6.3 Functional assignment

6 System safety lifecycle: Realisation and planning of the individual I&C systems

6.2 Requirements on the objectives of the system life-cycle phases

6.2.2 Requirements specification

6.2.3 Equipment selection & system specification

6.2.4 Detailed design & implementation

6.2.5 Integration

6.2.6 Validation

6.2.7 Installation

6.2.8 Modifications

6.3 Requirements on thesystem planning

6.3.2 S quality plan

6.3.3 S security plan

6.3.4 S integration plan

6.3.5 S validation plan

6.3.6 S installation plan

6.3.7 S operation plan

6.3.8 S maintenance plan

6.4 Requirements on output documentation

6.4.2 Requirements specification

6.4.3 Specification

6.4.4 Detailed design

6.4.5 Integration

6.4.6 Validation

6.4.7 Modification

6.5 Qualification

6.5.2, 6.5.4

Requirements on system qualification

6.5.3, 6.5.5

S Qualification plan

6.5.6

Requirements on qualification documents

7 Overall integration and commissioning

7.2 Requirements on the objectives

7.3 Requirements on output documentation

8 Overall operation and maintenance

8.2 Requirements on the objectives

8.3 Requirements on output documentation

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

IEC 1895/11

Figure 1 – Overall framework of this standard

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*

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.

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.

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

[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”.

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”.

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.

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

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.

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]

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

[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”.

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:

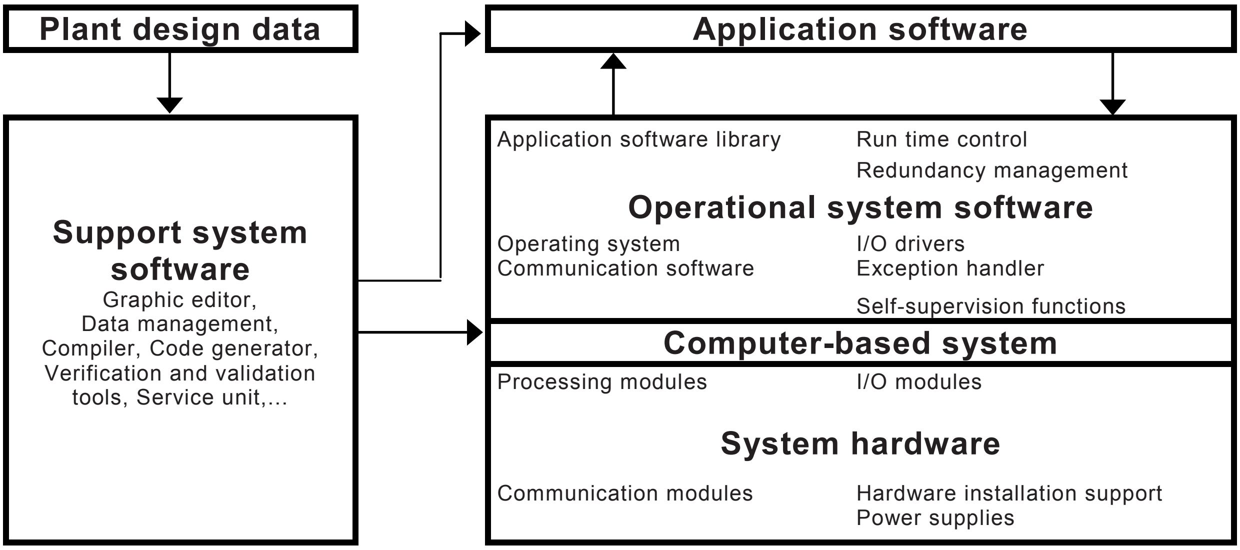
> *Validation*: The process of determining whether a product or service is adequate to perform its intended function satisfactorily. Validation is broader in scope, and may involve a greater element of judgment than verification.
>
> *Verification:* The process of determining whether the quality or performance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

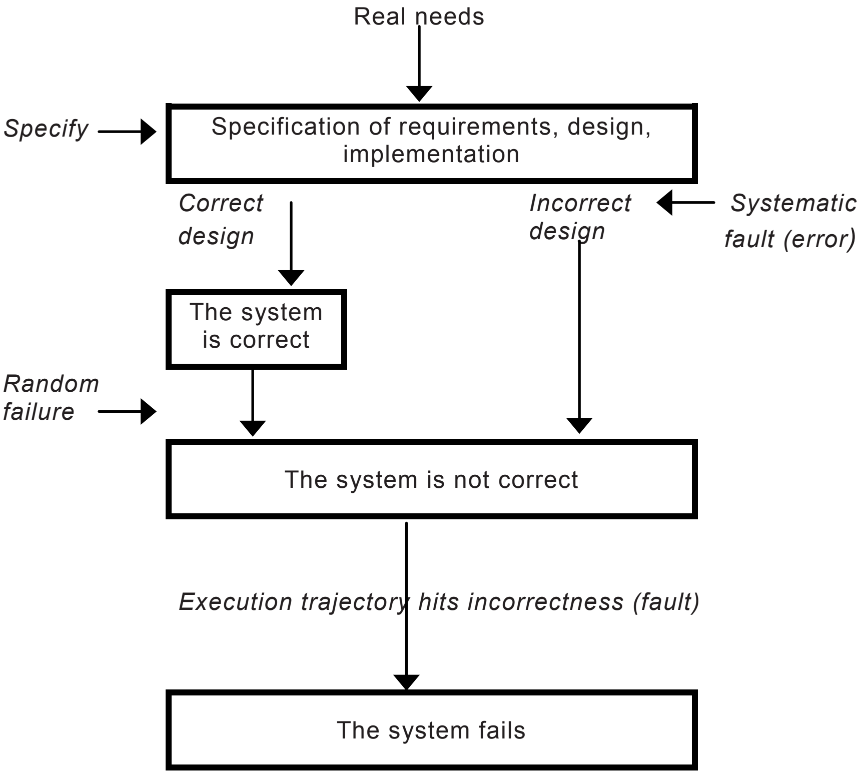
Furthermore, “verification” and “validation” are used to identify two different and complementary types of assessments:

> “*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.



IEC 1896/11

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


Real needs
Specify
Specification of requirements, design, implementation
Correct design
Incorrect design
Systematic fault (error)
The system is correct
Random failure
The system is not correct
Execution trajectory hits incorrectness (fault)
The system fails

IEC 1897/11

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

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);

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

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.				

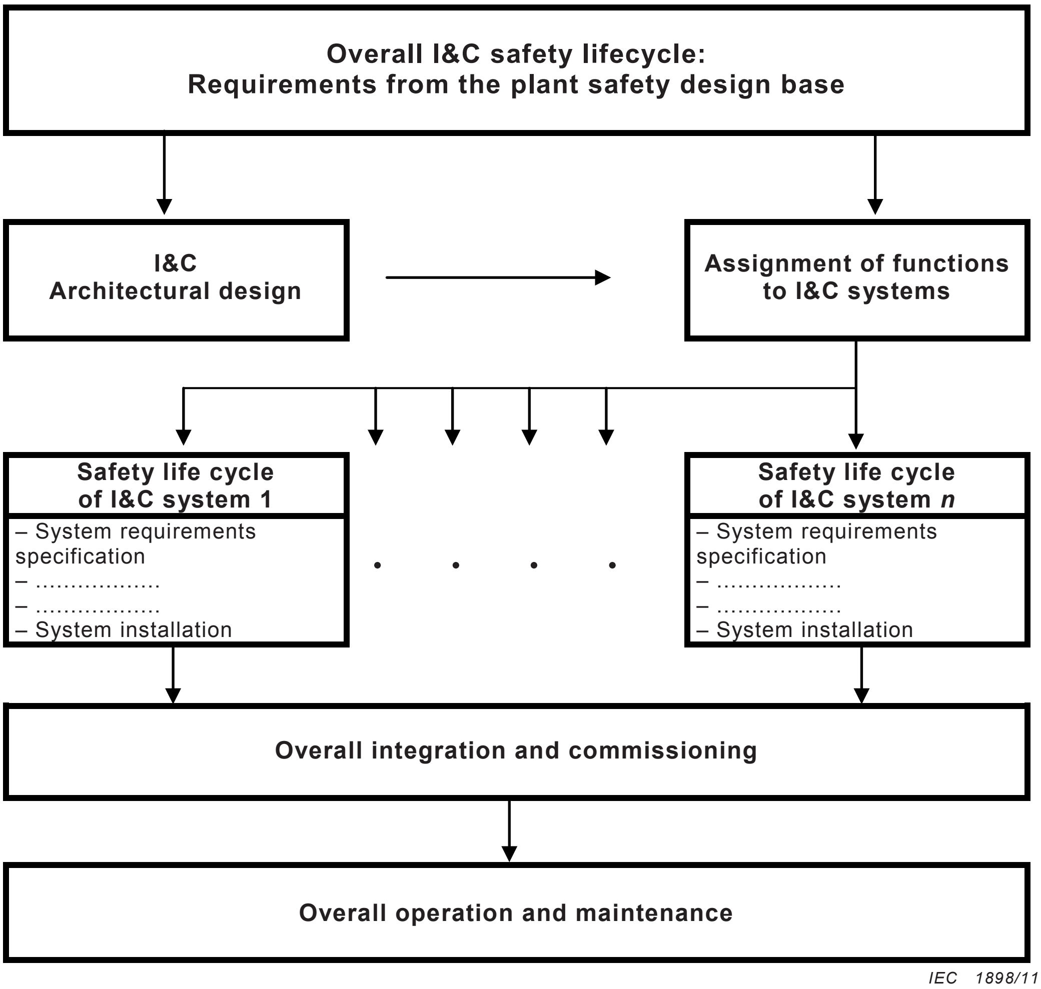


Figure 4 – Connections between the overall I&C safety life cycle and the safety life cycles of the individual I&C systems

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 concerning human-machine interactions consider the principles of operation together with ergonomic considerations in order to minimize failures due to human factors.

The I&C design process requires the following inputs from the plant safety design base:

- the defence in-depth concept of the plant (see Clause A.4), and the groups of functions provided to address PIEs sequences in order to fulfil the safety objectives (see Clause A.3);

  NOTE 1 In cases where the reliability of a function is required to be very high, the requirements specification for the plant and the I&C stipulate different lines of defence for the same PIE, for example, two or more independent and functionally diverse physical initiation criteria and, if appropriate, a second, functionally diverse, independent, redundant mechanical system for accident control.

  NOTE 2 The defence in-depth echelons may include functions important to safety and may include other functions. The requirements of this standard address only those functions that are important to safety.

- the functional and performance requirements of the functions of the plant important to safety needed to meet the general safety requirements (see Clause A.4);

  NOTE 3 Where functional validation is required (see 6.2.4.2), the design base provides the initial conditions, allowable limits and allowable rate of change of the plant variables to be controlled by the I&C systems important to safety.

- the role of automation and prescribed operator actions in the management of anticipated operational occurrences and accident conditions (see Clause A.4);
- a task analysis in accordance with 6.3 of IEC 60964:2009 defining which functions should be assigned to operators and which functions should be assigned to machines;
- the variables to be displayed for the operator to use in taking manual control actions;
- the priority principles between automatic and manually initiated actions, taking into account functional categories, operator rooms or locations.

5.2.3 Review of the categorisation requirements

5.2.3.1 Assumptions of this standard concerning categorisation of functions and classification of systems

Functions, systems and equipment in the NPPs are classified according to their importance to safety. This standard distinguishes between categorisation of I&C functions and classification of I&C systems, in accordance with IEC 61226.

NOTE 1 The terms "categorisation" and "classification" are sometimes synonymously used, even in IEC 61226. For the purpose of clarity in this standard, the term "categorisation" is reserved for the functions and the term "classification" for the systems.

The categorisation process places each I&C function into a category according to its importance to safety.

These categories are characterised by sets of requirements on the specification, design, implementation, verification and validation of the I&C function, as well as by requirement on the properties of the systems suitable for the categories, their qualification, the application functions, the service functions, and the system software functions of the system as appropriate. Consistent requirements apply to the whole chain of items which are necessary to implement a function of a given category, regardless of how it is distributed in a number of interconnected I&C systems. Therefore, it is practical to define classes of I&C systems which are suitable to implement I&C functions up to a defined category.

The categorisation of the I&C functions is part of the plant safety design base and is outside the scope of this standard. This standard assumes that the plant safety design base has assigned the individual I&C functions important to safety into one of three categories A, B or C and that the main design requirements for the systems and equipment associated with these categories are consistent with those of Clause 7 of IEC 61226:2009. Furthermore, the requirements for category A are consistent with the requirements for safety systems of the IAEA.

NOTE 2 The normative references for categorisation of functions may vary between countries and deviate from the reference of this standard (IEC 61226). A specific situation may also arise when applying this standard to existing plants where new categorization requirements are valid only for the parts in the scope of a modernization project. In such cases, a specific analysis may be required to identify the minimum requirements per system class.

The classification of the I&C systems is defined by the I&C project organisation in the design phase of the I&C architecture before the functional assignment of the I&C functions to the systems (see 5.4.2 and 5.4.3).

5.2.3.2 Requirements

a) The categorisation of the I&C functions shall be provided in the plant safety design base and shall constitute a reference input to the overall I&C requirements specification (see 5.3).

b) The I&C project organisation shall review the categorisation and verify it for completeness and feasibility. In the case of non-feasibility (for example, assignment of the highest category to a function which cannot meet the single failure criterion due to the plant design), the definition and categorisation of I&C functions shall be reviewed against the plant I&C functional requirements. The functional requirements and their associated categorisation shall be iterated until a feasible solution is achieved.

5.2.4 Review of plant constraints

The I&C architectural design (see 5.4) is subject to constraints imposed from the plant design framework.

a) The I&C project organisation shall identify the constraints placed on I&C equipment by the plant layout, the interfaces with plant equipment, and the events outside the I&C, including
   - the boundaries between the I&C systems and equipment and the plant systems, including the interfaces to the electrical/mechanical actuation systems and the auxiliary systems, such as power supplies and air conditioning systems;
   - the range of transient and steady-state environmental conditions in normal, abnormal and accident conditions under which the I&C systems are required to operate;
   - the range of transient and steady-state conditions of motive and control power in normal, abnormal and accident conditions under which the I&C systems are required to operate;
   - the general constraints on installation and cable routing;
   - the specific constraints on installation and cable routing to centres of convergence such as the control room and cable spreading rooms;
   - the constraints on grounding and power supply distribution;
   - the internal and external hazards to be considered according to the plant hazard assumptions. These include fire, flooding, icing, lightning, overvoltage, electromagnetic interference, earthquake, explosion and chemical influences.

b) The I&C project organisation shall identify the constraints placed on I&C equipment by the utility’s principles of operation, i.e. constraints from
   - security;
   - operation and maintenance (see 5.6 of IEC 60964:2009);
   - "in-service maintenance" of the I&C systems.

   Typically, this will lead to additional requirements guiding the subdivision of the I&C architecture in separate sub-systems. Areas to be considered include:
   - the plant is typically subdivided in distinct plant systems, which are grouped in lots so as to organize engineering, installation, start-up and testing activities. The subdivision of the I&C systems should take into account this boundary condition;

- optimal scheduling of maintenance work, periodic testing and modification activities should be possible for selected plant and I&C subsystems whereas other subsystems have to stay fully operational;
- the impact of the distribution and sharing of operating staff responsibilities should be analysed and taken into account in the subdivision of the I&C systems;
- requirements should be identified regarding tools and service work stations for maintenance and diagnostics, including the interface to the engineering systems. This may include requirements concerning the human-machine interfaces to the maintenance staff, interfaces with central plant management facilities etc.

5.3 Output documentation

The output documents of the activity described in 5.2 are the requirements specifications for the individual I&C systems important to safety.

NOTE 1 The requirements specifications encompass the whole of the I&C function from its inputs (sensors, operators, other equipment) to its outputs (directed to actuators, operators or other equipment). Further splitting of these requirements specifications will provide the requirements specifications of the subfunctions at the level of the individual I&C systems. This will depend upon the selected I&C architecture (see 5.4) and how the functions are implemented through distributed equipment (instrumentation, processing and actuators).

a) A requirements specification shall be established for each I&C function. It shall include:
   1) a functionality requirements specification defining the way the function transforms input information to output information in order to operate or monitor the plant;
   2) a performance requirements specification defining the range, accuracy and dynamic performance of the function;

   NOTE 2 This comprises requirements on timely behaviour which may have been omitted for hardware systems in the past.

   3) specification of the category of the function.

   NOTE 3 The category implicitly defines the minimal classification requirements of the I&C systems required for the implementation of the function (see Table 2).

b) The overall requirements specification shall define any dependency between functions which generate constraints on the assignment of functions to the I&C systems. This includes:
   1) the combinations of functions to be monitored to control protective actions;
   2) the combination of functions ensuring defence in depth;
   3) the combination of functions which constitute a safety group.
c) The requirements specifications of all the I&C functions shall be verified to ensure that a complete and consistent set of functions and constraints are defined for the purpose of assignment of functions to systems and the production of the specification of those systems (see 6.2).

   NOTE 4 When starting to prepare the requirement specification for an I&C function, it may happen that the complete set of sensors or actuators linked to that function has not yet been fully determined. It will then be necessary to successively complete the specification so that all sensors and actuators are included. Also the control of any additional actuator, possibly initially not considered, needs to be assessed and properly categorized. This is possibly performed in iterations of the requirement specification.

5.4 Design of the overall I&C architecture and assignment of the I&C functions

5.4.1 General

This subclause describes how the

- constraints from 5.2.4 and requirements from 5.3 apply to the design of the overall architecture of the I&C systems important to safety (in short “I&C architecture”);
- I&C functions are assigned to the individual I&C systems.

5.4.2 Design of the I&C architecture

5.4.2.1 General

The design of the I&C architecture provides a top-level definition of the I&C systems of the NPP, of the communication between these systems, and of the tools necessary to ensure a consistent interface between these systems.

5.4.2.2 General requirements

a) The design of the I&C architecture shall encompass the entire I&C necessary to implement the I&C functions important to safety specified in 5.3.

b) The design of the I&C architecture shall decompose the entire I&C into sufficient systems and equipment to meet the requirements on

- independence of the functions in different lines of defence,
- adequate separation of the systems of different classes,
- fulfilment of the constraints on the physical separation and electrical isolation arising from the environmental and layout constraints, hazard analysis, and constraints from start-up activities, testing, maintenance and operation (see 5.2.4).

c) The design of the I&C architecture shall provide sufficient systems and sub-systems so that the single failure criterion is met for category A functions, for all permitted configurations of the systems and the plant (see 4.17 – 4.21 of IAEA NS-G-1.3:2002).

d) Each I&C system shall be classified according to its suitability to implement I&C functions up to a defined category.

Table 2 – Correlation between classes of I&C systems and categories of I&C functions

Categories of I&C functions important to safety			Corresponding classes of I&C systems important to safety
A	(B)	(C)	1
	B	(C)	2
		C	3
NOTE A special case is discussed in 7.3.2.1 of IEC 61226:2009.			

e) The interfaces with the plant and interconnections between the I&C systems shall be defined as part of the architectural design in order to identify

- sharing of (measurement) signals by different functions important to safety,
- the voting of, and priority between, actuation signals from different systems,
- signal paths and equipment that are common to automatic or manual actuation functions in different lines of defence.

f) The description of the systems, equipment and their interconnections in the design of the I&C architecture shall be sufficiently detailed to allow the analysis of the I&C safety issues.

5.4.2.3 Human machine interfaces

a) The design of the I&C architecture shall structure the HMI systems of the different plant control and monitoring areas including the main control room, supplementary control points, local control panels and emergency control centre, with the degree of redundancy and user friendliness necessary to accommodate the constraints from plant operation and maintenance (see 5.2.4).

b) The design of the I&C architecture shall comply with the principles for plant operation established in the plant design base (see 5.2.2) including:

- the priority principles between automatic signals and manually initiated control signals;

- the priority principles between the different HMI systems during normal, accident, and post-accident operation;
- the priority principles between normal and back-up HMI systems;
- the principles of switchover conditions between normal and back-up HMI systems.

c) The architectural design shall define how faults or failures detected by diagnostic facilities of the individual systems are announced to the plant operator. The form of annunciation shall be such that the operator can:

- recognise immediately the indication of a failure and distinguish it from other operational indications;
- decide whether to take manual control actions to bring the plant into a safe state;
- identify the systems in question to the appropriate maintenance personnel.

NOTE 1 Manual control actions are understood to use controls and displays for feedback information. Direct intervention in the I&C equipment e.g. by insertion of simulation pins or disconnecting leads is not considered.

d) The design of the I&C architecture shall be demonstrated to be consistent with the main decisions concerning the technology of the HMI systems (e.g. computerised or conventional). More complex systems should be used for the presentation of information to the plant operators if this reduces the human factor contribution to a failure on demand and if this effect can be reduced by having better information. The potential for CCF of a CB information system should be considered in comparison with the potential for failures due to human factors.

e) The design of the I&C architecture shall

- assign the functions to human control or to automatic control in accordance with the plant design base task analysis (see 5.2.2),
- determine I&C system processing capability necessary to process the information and capability to complete the tasks defined for operator interaction (see 6.3.3 of IEC 60964:2009);
- ensure that information, characteristics of the HMI and time available to the operator for manual control action is consistent with the requirements of the plant design base (see 5.2.2).

f) Human factor techniques based on IEC 60964 and IEC 60965 shall be used for ensuring the effectiveness of the HMI in the design of the main control room and other control areas of the plant.

NOTE 2 Starting point for human-factor oriented analyses are the related operator tasks and their performance requirements, leading to a proper integration of displays and controls, especially for tasks to be executed frequently, under time pressure or with increased risk in case of human error.

g) The tasks of the operator and the optimisation of HMI requirements, of both tasks, important to safety and not important to safety, shall be taken into account in the design analysis.

5.4.2.4 Data communication

Data communication between systems making up the I&C architecture includes all the links provided to transmit one or more signals or messages over one or more paths using serial data communication.

a) Communication links shall be capable of meeting the overall performance requirements specifications (see 5.3) under all plant demand conditions.

b) Communication links architecture and technology shall ensure that the independence requirements between systems are met. In addition to physical separation and electrical isolation, the design should include provisions to ensure that faults and disturbances of communication links do not cause processing modules to deliver unsafe results.

c) Communication links shall include provision for checking the operation of the communication equipment and the integrity of transmitted data.

d) Redundancy of the communication links should be provided to accommodate failures.

e) Communication links shall be designed in such a way that data communication and operation of the higher safety category function cannot be jeopardised by data communication with lower classified systems.

See IEC 61500 and 60709 for details.

5.4.2.5 Tools

a) The I&C architectural design shall include the definition of the tools, usually computer based (see Clause 14 of IEC 60880:2006 and 5.1.4 and 6.1.4 of IEC 62138:2004), that are to be used to assure consistency of data exchanged between I&C systems working co-operatively and to ensure consistency of data with the plant data base.

   NOTE Tools specific to the individual systems are defined in the system specification phase (see 6.2.3.2).

b) Tools should be used in all the phases of the overall I&C safety life cycle where benefits to the assurance of quality and to the reliability of the functions important to safety can be obtained, e.g. to support

   - all aspects related to the design of interfaces between I&C systems,
   - the overall integration and commissioning of distributed functions.

c) Tools shall be selected and methods to obtain adequate quality of output shall be defined in accordance with the requirements of IEC 60880 (for class 1 systems) respectively IEC 62138 (for class 2/3 systems).

5.4.2.6 Defence against CCF

I&C systems with redundant architecture can fail if two or more redundant channels fail concurrently (CCF) (i.e. the voting majority of the redundant channels fails on demand). Such an occurrence can happen if one or more latent faults are systematically incorporated in some or all redundant channels and if a mechanism exists which can trigger such a systematic latent fault of two or more redundant channels so that they fail in a timely correlated manner (see IEC 62340).

The origin for systematic latent faults is mostly related to human errors. They may be introduced in any phase of the life cycle of an I&C system. The use of computers allows more complex algorithms and processes to be used than is possible with hardware alone. Furthermore the design effort of computer based I&C, including the activities related to the design of the underlying I&C platform, is higher than for hardware I&C, and the design may be more complex.

Design choices should be evaluated with the objective to minimize the introduction of avoidable complexity.

The defence against the CCF of I&C systems includes the following levels:

a) A functional validation of the application functions requirements specification should be performed for class 1 systems (see 6.2.4.2.1) to reduce the likelihood of latent faults in the requirements specification.

b) A clearly structured engineering process shall be performed with highest attention to all verification and validation activities, so as to reduce the likelihood of latent faults in the design. The effort should be graded for class 1, class 2 and class 3 systems.

c) I&C systems of class 1 and their support systems should be designed in a way that they operate independent from influencing factors from the plant process, so as to minimize the possibility that potential latent faults can be triggered (e.g. hardware components performing PIE mitigations should not be subject to adverse environmental conditions arising from that PIE; the scheduling of software execution should not depend on the plant signals).

   NOTE 1 This recommendation corresponds to the requirement of IEC 62340 that I&C systems should operate independently from the “plant demand profile”.

d) For class 1 systems, an analysis shall be performed to identify possible sources of CCF and mechanisms which could trigger postulated latent faults to cause a failure. Within this analysis special care should be given to communication links and data transmission arrangements and to components whose loading is demand dependent. The possible failure modes and the failure sequences of such components should be assessed with regard to possible sources and effects of CCF. The analysis should also include those systems of the concerned safety group which are credited to mitigate the effects of postulated CCF of class 1 systems.

A design for coping with CCF is required if the postulated failure of functions important to safety would lead to unacceptable consequences. This is in general the case for category A functions, and for a subset of category B functions (see 5.3.2 and 5.3.3 in IEC 61226:2009).

e) The I&C architectural design should use the principle of diversity where high reliability is required for a safety group, and hence sources and effects of CCF are to be considered. Functional, signal and equipment diversity should be considered. If diversity is used to support defence against CCF, the design shall include an analysis of the effectiveness of diverse features claimed to minimize the potential for CCF.

f) Where Class 1 and lower class I&C systems are claimed in the deterministic safety case as different lines of defence effective for design basis accidents, these systems shall be independent. I&C systems perform their safety functions independently if a postulated failure of one of these I&C systems does not prevent the other systems from performing their functions as intended. Independent I&C systems shall be operated at different signal trajectories. This can be assured by diversity (e. g. by equipment diversity or functional diversity).

Further requirements concerning measures to cope with CCF in systems performing category A functions are provided in IEC 62340.

NOTE 2 An activity should be performed on plant safety analysis level to verify that the design measures taken to handle/meet I&C failures will be managed by the category A/B/C functions specified. This will be an activity not only on I&C but safety analysis level and is therefore out of the scope of this standard.

5.4.3 Assignment of functions to systems

The functional assignment process assigns the overall requirements of the I&C functions important to safety, established in 5.3, to the individual systems of the I&C architecture. Where necessary, functions may be decomposed into a number of subfunctions distributed over a number of systems. All the functions or subfunctions are called the application functions of the I&C systems (see 6.2.2.2).

a) The functional and performance requirements specification of the application functions shall address the overall requirements of the I&C functions. If a function is distributed over more than one I&C system, these interconnected systems shall be arranged in such a way that the overall requirements defined in 5.3 are met.

   NOTE 1 This includes an evaluation of the fulfilment of the probabilistic targets defined.

b) The functional and performance requirements specification of the application functions shall include all the ancillary validation, interlock, and monitoring functions which were identified during the design of the I&C architecture, for example, status and operating mode of the interconnected systems, validation of signals received from other systems.

c) The assignment of application functions to systems shall conform to the principles relating to the system class and category of function defined in Table 2.

d) Category A functions shall be assigned to systems in such a way that the single failure criterion is complied with.

   NOTE 2 To align with NS-R-1, it is the “safety group” that has to meet the single failure criterion, not the individual systems per se.

e) The assignment of category A functions of the same safety group to systems shall take into account the measures for defence against CCF stated in 5.4.2.6. Examples of assignment of functions of different categories are given in Figure C.1.

f) The assignment of the application functions to the systems shall attempt to minimize the complexity of class 1 systems.

NOTE 3 This is valid especially for new plants. In cases of replacements of hard-wired systems by CB systems, the same requirements are normally assigned to the CB system for the application functions as for the previous hard-wired system.

NOTE 4 System complexity may be reduced by considering design approaches such as

- avoiding complex algorithms and processing that cannot be clearly defined and validated,
- reducing the number of different functions that are implemented in a system,
- using simple design features to limit the impact of potential complex fault conditions.

However, any reduction in complexity should not result in excessive negative design impacts, such as increased complexity in the overall I&C architecture or reductions in safety related functionality such as the extent of self test coverage.

g) The reliability required of each application function implemented in the systems shall be compatible with limits, including CCF, estimated as being achievable.

NOTE 5 The evaluation of limits may depend on recommendations from standards, preliminary analyses performed and evaluation of previous licensing experience and licensing risk evaluations.

h) The records produced from the process of assigning functions to systems shall clearly identify which systems are performing what functions, i.e. traceability shall be provided.

5.4.4 Required analysis

5.4.4.1 General

Analysis is required to verify the design of the I&C architecture and the assignment of functions to the I&C systems. Such analysis is an iterative process to be performed together with the design process (see Clause 6).

5.4.4.2 Assessment of reliability and defences against CCF

a) An evaluation of the reliability of the I&C systems important to safety should be performed. The evaluation should include dependencies on common services, such as electrical and pneumatic power supplies and heating and ventilation facilities.

b) This may be based initially on the estimated reliability achievable for the functions of the different systems and should be verified following completion of the design process based on the reliability assessment of the individual systems (see 6.2.4.2.2).

c) An evaluation of the vulnerability to CCF of safety groups performing category A functions shall be performed, to evaluate the effectiveness of measures against CCF and to identify potentially weak points of the overall architecture.

d) The design documentation of the systems (see 6.4.4) shall be analysed to identify common or identical hardware or software components supporting different functions of a safety group including category A functions. If common or identical items are found in different lines of defence, a justification shall be provided to show that the CCF potential is sufficiently low, in line with the safety role of the safety group.

e) There is no commonly recognised method available for quantitative assessment of CCF potential, so methods used for the estimation are essentially qualitative (see Annex C). The methods to be used should be defined at the beginning of the design.

NOTE 1 One aim of the above recommendations and requirements is to rule out the need to make late changes to the planning and design of a system in response to changes in requirements, with subsequent potential causes for CCFs from errors made in response to these.

NOTE 2 The level of detail of the CCF analysis may depend on the category of the functions supported by the systems and will be justified.

NOTE 3 Requirements for the analysis of CCF in class 1 systems due to software are given in 13.3 of IEC 60880:2006.

5.4.4.3 Human factors assessment

The verification of the architectural design should include an analysis of human factors requirements to allow optimisation of the design of HMI systems.

5.5 Overall planning

5.5.1 General

This subclause places requirements upon the development of overall plans which ensure the consideration of common requirements from the overall I&C lifecycle for all individual I&C systems, and which ensure that the requirements of the I&C functions important to safety distributed over the I&C systems will be achieved and maintained throughout the life of the systems.

The requirements of this clause co-ordinate and complement the plans established in 6.3 for the individual I&C systems.

NOTE The following requirements on plans do not preclude that the plans may be organised in a different number of documents.

The overall plans shall be established before the activities they address are initiated.

5.5.2 Overall quality assurance programs

This standard assumes that a quality assurance program or preferably an integrated management system consistent with the requirements of IAEA GS-R-3 and IAEA GS-G-3.1 exists as an integral part of the NPP project and that it provides control of the constituent activities.

a) Quality assurance programmes shall be established and implemented for each activity related to the overall I&C safety life cycle.

b) The quality assurance programs shall include all activities that are necessary to achieve quality and the activities which verify that the required quality has been achieved.

c) The verification activities shall be defined in verification plans. The verification plans include the resources, process and outputs of the phases of the overall I&C safety life cycle and define

   - procedures and tools for verification activities;
   - the records to be kept and verified;
   - the safety relevant aspects to be verified;
   - procedures for the resolution of failures and incompatibilities;
   - the criteria for declaring each phase complete;
   - the final reports to be produced showing the compliance of the outputs of the phase with the inputs requirements and the resolution of anomalies.

d) The quality assurance programs shall be planned and included within the general quality assurance program of the NPP project, and its activities shall be included within the general schedule of the activities of the NPP project.

5.5.3 Overall security plan

Security measures are required to protect the information processed within systems important to safety against unauthorised modification including unauthorised control actions (integrity), disruption of access (availability) and unauthorised disclosure (confidentiality).

NOTE 1 For I&C systems in nuclear power plants, integrity and availability requirements predominate over confidentiality.

Software (programme code as well as parameters and data) may be especially vulnerable during the design and maintenance processes. Threats that need to be considered include deliberate malicious modifications that cause erroneous behaviour of the software either in general or triggered by certain time or data constraints.

NOTE 2 Threats arising from unintended modifications are addressed in the system requirements specification (see 6.2.2.5).

The overall security plan specifies the procedural and technical measures to be taken to protect the architecture of I&C systems from deliberate and intelligent attacks that may jeopardise functions important to safety. The provisions of the overall security plan may differentiate between requirements for systems of class 1, 2 and 3.

a) The security requirements of functions and systems important to safety shall be identified in the system security plan (see 6.3.3).
b) The risk arising from unauthorised access and modification shall be managed in a systematic manner during all phases of the life cycle from inception to disposal. This includes the development and engineering systems as well as the I&C systems to be installed in the plant. Physical access as well as remote access shall be considered.
c) The security provisions for a system shall be such that they do not have a significant impact on its reliability or availability.
d) To maintain security of systems at a continuously high level a site-specific security policy shall be established. It shall contain procedures related to the interface between administrative and technical security, access to systems, security aspects of data handling, security aspects of modification and maintenance, security auditing and reporting, and security training.
e) Systems performing functions important to safety shall be physically protected against unauthorised access (see 4.51 of IAEA NS-G-1.3:2002). Access control shall include identification and authentication of personnel for systems performing category A functions and reliable identification of personnel for systems performing category B and C functions.
f) Features for remote (external to the plant) access shall not be implemented for systems performing category A and B functions, and should not be implemented for systems performing category C functions. If access features via data links (internal or external to the plant) are provided, they shall be analysed and it shall be demonstrated that they do not introduce unacceptable risk of unauthorised system access or unacceptable risk of system failure.

   NOTE 3 Preventing access does not preclude sending data out from a system.

g) Access to systems (including attempts to access) should be logged. This comprises recording the personnel, the type of access, the time, and the actions carried out.
h) Security logs shall be formally inspected at defined intervals for systems performing category A functions and should be checked periodically for systems performing category B and C functions.

5.5.4 Overall I&C integration and commissioning

5.5.4.1 General

Overall I&C integration is the combination of all on-site technical and administrative actions enabling the I&C systems to be installed on site, interconnected, tested, calibrated and set ready for full operational use.

Overall commissioning is the combination of all on-site technical and administrative actions necessary to give assurance that the installed systems and plant are satisfactory for service before they become operational (see 4.4 of IAEA 75-INSAG-3:1999).

NOTE 1 Overall commissioning refers to commissioning of the whole plant and includes all plant systems, not only the I&C systems (see 3.7).

The overall I&C integration and the overall commissioning processes complete the validation and installation of the individual systems (see 6.2.6 and 6.2.7). The following requirements apply:

a) Following integration of the I&C systems on site, the overall functional and performance requirements specification of the I&C functions important to safety distributed within the systems shall be validated in all specified modes of plant operation.

b) The extent of the integration and commissioning activities to be performed on the overall level may be defined taking into account the extent of testing in other design phases, e.g. the integration and function tests performed in the factory or on site, or tests done for sister plants when the NPP is not a first-off plant. These reductions of the overall verification and validation shall be justified and documented.

NOTE 2 It is good practice to minimize the on-site tests of the integrated I&C system by performing significant parts of the integration testing already in the factory. An overall strategy how to distribute the required testing to different environments (testing by use of simulation or emulation, tests in an integration test field in the factory, tests on site) should be developed early in the project, see e.g. 7.18 of IAEA NS-G-1.3:2002.

Typically, these tests form part of the process of acceptance of the I&C systems by the plant owner. IEC 62381 [11] provides practical hints for performing and documenting factory acceptance test (FAT), site acceptance test (SAT) and site integration test (SIT).

5.5.4.2 Overall I&C integration plan

An overall I&C integration plan shall be developed within the framework of the quality assurance program. In addition to the generic requirements of 5.5.2 on quality assurance and verification, the following requirements apply:

a) Testing of interconnected systems shall be performed to confirm that
   - all interfaces of interconnected systems operate correctly,
   - failure detection, corrective actions and the display of associated data are operating in accordance with the requirements specification of the I&C functions.

b) Electromagnetic interference immunity verification of interconnected systems shall be performed according to the requirements of IEC 61000-4-1 to IEC 61000-4-6.

   NOTE Immunity verification requires typically a combination of measurements (e.g. for establishing the in-situ conditions), testing (e.g. of subsystems) and analysis. Also, other parts of the IEC 61000-4 series provide guidance on measurements and testing.

c) Earthing and equipotential bonding of all equipment and cable screens to ground planes shall be verified as correct.

d) Testing of the systems’ response to the loss and return of external power supplies and to power spikes as required, shall be performed to verify the systems’ behaviour and availability in case of interruption and recovery of power supplies.

e) The environmental conditions at the location of use of the I&C systems shall be verified to be as specified.

f) Analogue and logic signals exchanged between the systems shall be tested to show that correct values and states are provided to the different functions important to safety. Where the display, alarm, record and calculation functions are performed in a system not important to safety, this testing should be carried out in conjunction with the system not important to safety unless a simpler method of demonstrating the correctness of all data sent to it can be devised.

g) Closed-loop control functions and logic control functions shall be tested, from inputs to outputs including actuators, operator interfaces and control transfer (e.g. manual/automatic).

h) Tests shall confirm that correct information is provided to each system in case of failure of redundant equipment, of communication links, of sensors or of control actuators. They should confirm that control mode switching and timing are correct.

i) Data communication shall be tested for correct data transmission and acceptable response time, from issuing of commands to the receipt of a correct indication of actuator state. Tests should be performed under simulation of normal operating conditions, relevant accident conditions, worst-case conditions, and in the presence of simulated hardware failures.

5.5.4.3 Overall commissioning plan

An overall plan to complete the validation of the I&C systems shall be developed within the framework of the commissioning programme of the plant systems (see 4.4.253 of IAEA 75-INSAG-3:1999). The following requirements cover the I&C-specific aspects to be included in the overall plant commissioning programme:

a) Setting of setpoints, thresholds, parameters, and instrumentation calibration values shall be verified and adjusted during commissioning of the plant systems to confirm that the systems functionality and performance comply with the overall requirements specification.

b) The operating and test procedures of the I&C systems shall be verified and updated during plant commissioning.

5.5.5 Overall operation plan

Overall operation planning addresses the operation of the interconnected I&C systems. The overall operation plan complements the operation plans for the individual I&C systems (see 6.3.7).

An overall operation plan shall be developed within the framework of the quality assurance program. In addition to the generic requirements of 5.5.2 on quality assurance and verification, the following requirements apply:

a) The plan shall describe

   - the means of starting-up, initialising, and keeping the interconnected systems in a fully operational state;
   - the means of verifying that the systems are available to perform the functions important to safety;
   - the routine actions, for example periodic tests, which need to be carried out during operation of the plant to maintain the required reliability of the functions important to safety.

b) The plan shall specify the conditions under which the modification of system parameters or controls can be carried out, and the effects of such modifications on the operation of the systems, and on the operation and the safety of the plant. It shall also state what modifications may be carried out:

   - under administrative control alone;
   - under administrative control and after designer approval and appropriate tests and verifications.

   NOTE The process for modifications and the authorities who permit these modifications may depend on the utility organisation and the national regulations.

c) The plan shall identify all modes of operation of the interconnected systems and specify how the systems shall be operated in each mode, including:

   - the actions to be taken and the constraints on the operation of the systems and of the plant in the event of system failure or of a hazard external to the systems;
   - the constraints on the operation of the systems and of the plant during periodic testing, maintenance, and/or incorporation of modifications;
   - when the constraints above may be removed, the procedures for returning to normal operation and to confirm that normal operation has been achieved.

5.5.6 Overall maintenance plan

The overall maintenance plan addresses maintenance at the level of the interconnected I&C systems. It complements and co-ordinates the maintenance plans of the individual I&C systems (see 6.3.8).

An overall maintenance plan shall be developed in the framework of the quality assurance program. In addition to the generic requirements of 5.5.2 on quality assurance and verification, the following requirements apply:

a) Constraints shall be placed on maintenance activities of the individual I&C systems to ensure that any effect on the plant safety is acceptable. In particular, where required, the systems shall continue to meet the single-failure criterion during maintenance. The plan shall identify what equipment may be removed from service, the consequences of removal, and the means for returning and verifying its correct return to service.

b) A systematic approach to test and replacement shall be implemented to make CCFs unlikely within those parts of the I&C architecture which are subjected to changed environmental conditions in the event of an accident. The approach should ensure that those parts of the system subject to radiation, and thereby to possible rapid ageing, or changes in physical properties (cables, sensors), or whose loading is changed in response to a challenge (for example, switching of power amplifiers, relays) are replaced prior to unacceptable deterioration in their ability to perform their safety functions.

   NOTE 1 Replacement intervals may be determined by accelerated ageing of representative equipment.

   NOTE 2 See IEC 62342 [12] for guidance on management of ageing.

c) Where maintenance activities involve the adjustment of configuration or calibration data, they shall be controlled by documented procedures which shall ensure that

   - maintenance adjustments are within defined limits (such limits may be imposed by the system design and plant design base in which case no formal restrictions need to be placed upon the maintenance staff);
   - where such adjustments are performed while a system is in use, the requirements of 5.5.5 above apply;
   - a record of all maintenance adjustments is preserved.

5.5.7 Planning of training

5.5.7.1 Training programme

This subclause deals with requirements related to the training of plant personnel working with the I&C systems.

a) A training programme for the operating and maintenance staff shall be provided both for plant operators and instrumentation and control specialists.

   NOTE Training of plant operators will be focussed on operator interfaces, with a basic knowledge about the I&C systems' technology, maintenance and diagnostics aspects, whereas I&C staff's training will be focussed on maintenance diagnostics and modifications, in accordance with their task definitions.

b) The training programme should be established based on a systematic approach that comprises

   1) an analysis of the tasks of the involved staff categories, and establish training objectives, an overall schedule and overall definition of training courses,
   2) availability of qualified trainers, and comprise training material for trainers and trainees,
   3) an evaluation of the training undertaken,
   4) enhanced use of feedback for the improvement of the training.

c) Operator training shall address operations under normal and abnormal plant conditions using all relevant operator interface devices and I&C functions.

d) Specific training in the recognition of hardware failures and software abnormalities should also be included in the programme.

5.5.7.2 User documentation

a) User documentation for the I&C system shall be provided for use by the operations and maintenance staff.

b) The user documentation should define each operator interface device. Each function of each device shall be explained and illustrated in accordance with its complexity.

c) Training shall allow operators and maintenance staff to get familiarized with the user documentation relevant for their tasks.

5.5.7.3 Training systems

In addition to class room activities, training should be based on the use of training systems. For operator training, part- and full-scope training simulators should be used.

a) Operator and maintenance staff training shall be conducted on training systems which are fully representative for the system and equipment characteristics to be trained. Limitations in the capabilities and use of the training systems shall be known and documented.

b) Simulators for operator training shall provide realistic control room interfaces and capability for real-time simulation of the plant's behaviour including the I&C systems. The simulator shall be capable of simulating normal and abnormal reactor conditions, including combinations of equipment failures and abnormalities.

5.6 Output documentation

5.6.1 General

The output documentation of the I&C architectural design and functional assignment process provides the necessary inputs for the requirements specification of the individual systems of the I&C architecture (see 6.2.2).

5.6.2 Architectural design documentation

a) The output documentation shall define for the individual I&C systems
   - the design constraints derived from the plant design framework (see 5.2.4);
   - the design constraints from the architectural design (see 5.4.2);
   - the physical and functional boundaries between systems.

b) The engineering tools used should be documented to address how each tool is to be used to support the design activities of the system life.

   NOTE Requirements on software engineering methods and tools for class 1 systems are given in Clauses 7, 14 and 15 of IEC 60880:2006 for class 1 systems, and in 5.1.1 and 6.1.1 of IEC 62138:2004 for class 2 and class 3 systems.

5.6.3 Functional assignment documentation

a) The output documentation shall define the functional, performance and reliability requirements of the application functions (see 5.4.3) assigned to each system. The requirements may be documented in text, flow diagrams, matrices, logic diagrams, etc., providing the functions are clearly conveyed.

b) The requirements specifications of the application functions should be defined in such a way that it is as far as possible independent of the technology that may be used to implement the function, i.e. computers, relays.

c) The main users of the requirements documents are the authors of the system requirements specification of the individual I&C systems, and the plant operators. Software and system engineering methods and tools should be selected appropriate for this staff.

6 System safety life cycle

6.1 General

The I&C architectural design defines the individual I&C systems which implement the functions important to safety (see 5.4.2). This clause sets out the objectives and requirements for such individual I&C systems. The requirements of this clause address CB systems.

NOTE Most of these requirements may also be applied to non-CB I&C systems.

To ensure that all the safety relevant requirements to be met by the system are captured, implemented and maintained, a systematic approach is required. This is achieved by placing the activities associated with development, implementation and operation of the system in the framework of a system safety life cycle. This life cycle refers in turn to the activities of the overall I&C safety life cycle (see Clause 5 and Figure 4).

The phases of the typical system safety life cycle include:

- the system requirements specification;
- the system specification;
- the system detailed design and implementation;
- the integration of the system;
- the validation of the system;
- the installation of the system;
- the modifications of the design of the system (if any).

The qualification of the system is considered separately because it may be performed partially independently of the system development life cycle. This approach is consistent with present practice, which relies increasingly on pre-existing equipment.

Figure 5 shows the typical system safety life cycle and indicates the relations with the software and hardware life cycles of IEC 60880, IEC 62138 and IEC 60987.

Table 3 gives an overview of the objectives, inputs and outputs of the typical system life cycle activities and provides references to the relevant subclauses.

This clause includes

- generic requirements to be applied equally for all systems important to safety,
- requirements to be applied, in addition to the previous ones, to specific classes of systems or categories of functions.

The system life cycle is an iterative process. A phase may start before the activities of the preceding phase are complete; however, a phase shall only be terminated if the preceding phases have been completed and if its outputs are consistent with the inputs provided by these preceding activities.

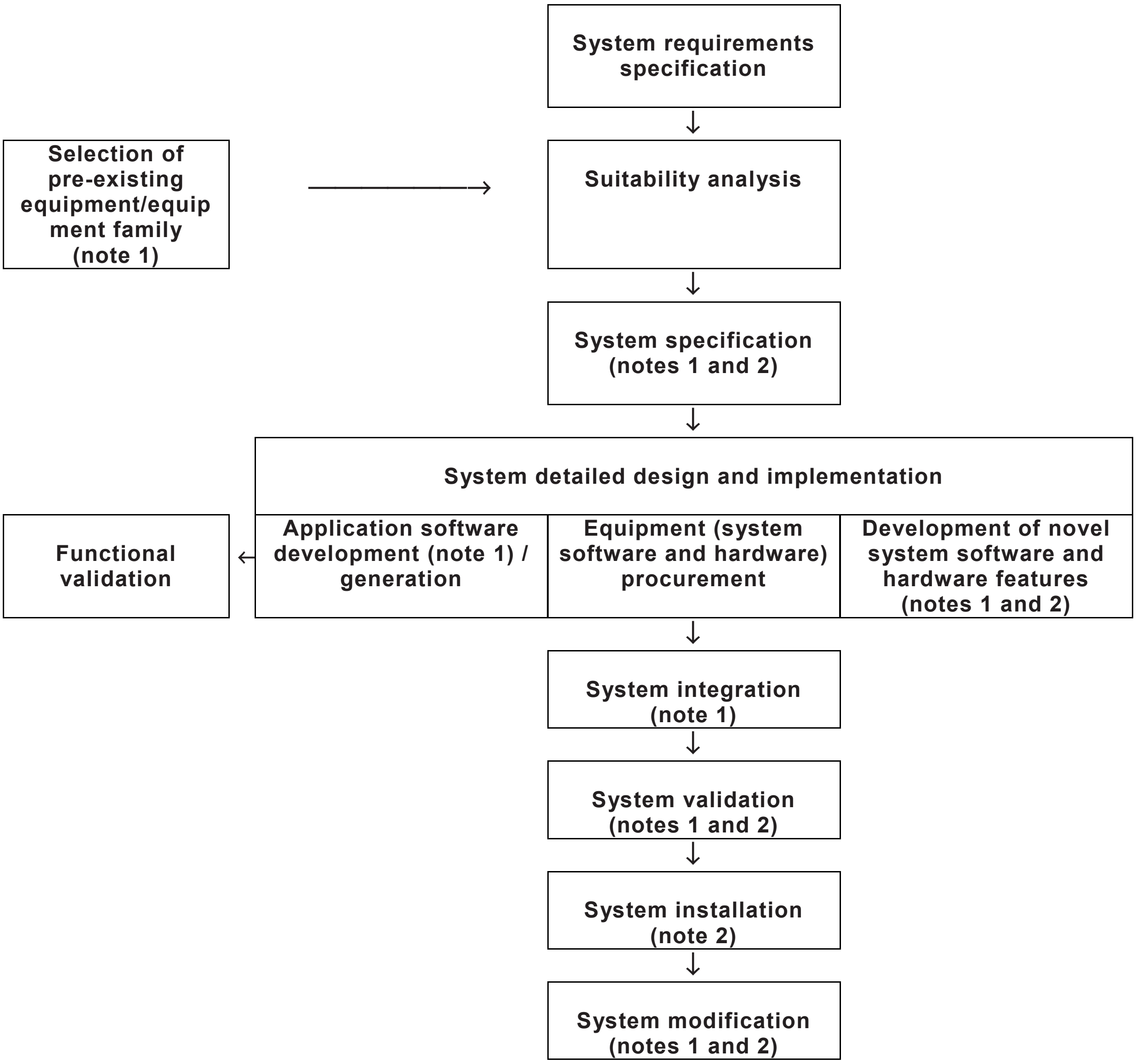
Table 3 – Overview of the system safety life cycle

Clause or subclause	Inputs	Objectives of the activity	Outputs
6 Requirements concerning the system life cycle and its relation with the overall I&C safety life cycle			
6.2.2 System requirements specification	Outputs of 5.6; 5.5 Outputs of 6.3.2, 6.3.3	To develop the system requirements specification for – the functions,	System requirements specification Application functions requirements specification

Clause or subclause	Inputs	Objectives of the activity	Outputs
		– the design constraints – the boundaries and interfaces with other systems and tools, – the interfaces with persons, – the environmental conditions	
6.2.3 System specification	Outputs of 6.2.2 Documentation of candidate pre-existing equipment Outputs of 6.3.2, 6.3.3	To evaluate and assess the suitability of candidate pre-existing equipment to be integrated in the system design To develop the design of the system architecture in order to implement the system requirements specification To assign the application functions to subsystems	System specification documentation (see 6.4.3) including: – identification of selected equipment and suitability analysis, – system architecture, – software specification
6.2.4 System detailed design and implementation	Output of 6.2.3 Output of 5.2.2 Outputs of 6.3.2, 6.3.3	To expand and refine the architectural design To develop the hardware and (system or application) software To validate the application functions requirements	System detailed design documentation (see 6.4.4) Functional validation and reliability assessment (see 6.2.4.2) Hardware and software subsystems and components
6.2.5 System integration	Output of 6.2.4 Outputs of 6.3.2, 6.3.3, 6.3.4	Assembly of the individual hardware and software components that make up the system	Integration report Integrated system
6.2.6 System validation	Outputs of 6.2.3 and 6.2.5 Outputs of 6.3.2, 6.3.3, 6.3.5	Validation of the system (see Note 1)	System validation report
6.2.7 System installation	Outputs of 6.2.6 Outputs of 6.3.2, 6.3.3, 6.3.6	Installation and testing of the system	Installation report System installed and tested on site
6.2.8 System design modifications	Modification request (if any) Outputs of 6.3.2, 6.3.3, 6.3.8	To make corrections, enhancements or adaptations to the system	Modification reports System modified
6.3 System planning	Outputs of 5.5, 6.2	To develop the validation plan, installation plan, operation and maintenance plan, security plan	System plans
6.5 System qualification	Outputs of 6.3.2, 6.3.3	To develop the qualification plan, and to execute it	Qualification documentation

NOTE 1 Validation of individual I&C systems is completed in the framework of overall I&C integration and plant commissioning (see 5.5.4). Plant commissioning itself is outside the scope of this standard

NOTE 2 For a comparison of this definition of phases with that of IEC 61508-2, see Annex D.


System requirements specification
Selection of pre-existing equipment/equipment family (note 1)
Suitability analysis
System specification (notes 1 and 2)
System detailed design and implementation
Functional validation
Application software development (note 1) / generation
Equipment (system software and hardware) procurement
Development of novel system software and hardware features (notes 1 and 2)
System integration (note 1)
System validation (notes 1 and 2)
System installation (note 2)
System modification (notes 1 and 2)

IEC 1899/11

NOTE 1 Software requirements on this activity are defined in IEC 60880 and IEC 62138, including use of pre-existing software.

NOTE 2 For class 1 and 2 systems, hardware requirements on this activity are defined in IEC 60987.

Figure 5 – System safety life cycle

6.2 Requirements

6.2.1 General

This subclause defines the requirements for the system safety life cycle.

These requirements encompass features related to

- specific functions assigned to the system by the functional assignment process,
- generic characteristics which, according to the system classification, make the system suitable to implement functions important to safety of specified categories.

NOTE Clause 7 of IEC 61226:2009 gives basic requirements for I&C functions and requirements specific to the different classes of I&C systems and equipment. These requirements are appropriately taken into account in this standard when developing the requirements for systems or functions respectively.

6.2.2 System requirements specification

6.2.2.1 General

The objective of this phase is to provide a high-level description of the system requirements, independent of the decision to adopt any specific technical solution. However, specific requirements defined at the overall I&C architecture level may impose constraints at the technology to be used, e.g. CCF-considerations.

The output documentation describing the I&C architecture and functional assignment (see 5.6) is one of the inputs to the system requirements specification.

The output documentation of this phase constitutes the reference document used to communicate between those defining the problem ("specifier") and those who are going to provide a technical solution ("designer").

The system requirements specification shall indicate

- the functions of the system,
- the global performance requirements,
- the constraints on the design of the system,
- the boundaries and interfaces with other systems,
- the interfaces with the users,
- the environmental conditions applicable to the system,
- the qualification required.

6.2.2.2 Functions

6.2.2.2.1 General

The requirements to be considered include requirements upon the individual application functions and the system service functions. The following apply:

6.2.2.2.2 Application functions

The requirements specifications of the application functions important to safety are defined by the functional assignment process (see 5.4.3).

a) The requirements specification of each application function shall establish
   1) the functionality, including input/output ranges and setpoints (respectively allowed ranges). For trip functions, the specification defines the margins between setpoints and allowable values (i.e. those including all uncertainties due to calibration errors or instrument drifts);
   2) the performance, including accuracy and response times. Where appropriate, performance requirements are defined for different initial plant conditions and PIEs.
   3) appropriate signal filtering, signal validation and interlocks shall be specified to implement back-up modes of operation and to minimize the potential of spurious actions.
b) The requirements specification of each application function shall state its categorisation and whether there are independence constraints from other functions in a safety group.

The functional assignment process defines for each category of functions a minimal class of I&C system. Together with the requirements for independence between functions of the same safety group (single-failure criterion, defensive design against CCF), such factors allow a qualitative estimation of the reliability of the function or the group of functions in a safety group to be made.

A quantitative reliability target may be associated with each application function to complement the deterministic design process and to aid verification of the system design and of the plant design basis. The ability of equipment to meet such targets may be evaluated using well established techniques for hardware components, but there is no generally recognised method available for the quantitative evaluation of software design reliability (see 6.2.4.2.2).

6.2.2.2.3 Service functions

The service functions, unlike the application functions, are not directly related to the performance of process-related functions, but relate to specific activities on the system, including the functions necessary for the configuration, validation, qualification, installation, commissioning, operation, periodic testing, maintenance, incorporation of design modifications and security.

The requirements specifications of the service functions are defined by the specifier of the system. The precision of the requirements for these functions is determined on a case by case basis. In some cases, they may be finalised in the system specification and architectural design phase, after selection of an appropriate technical solution for hardware and software.

Service function requirements should take into account the interactions and constraints that can be derived from the system plans (see 6.3).

NOTE For example, the controls for the modification of parameters should be consistent with the provisions specified by the system security plan (see 6.3.3), the system operation plan (see 6.3.7) and the system maintenance plan (see 6.3.8).

6.2.2.3 Design constraints

6.2.2.3.1 General

The following requirements define constraints which restrict the choice of potential solutions for the system design and the assignment of the functions in the system. The constraints are dependent upon the class of the system and the categories of the function and shall be taken into account during system specification and architectural design in order to

- fulfil the requirements associated with the categorisation of the application functions,
- ensure that the system will function as specified,
- enable or facilitate the demonstration of the correct operation of the system.

6.2.2.3.2 System architecture

The architecture of the system is constrained by the category of functions to be implemented within the system (see 5.4.3) and the defence in-depth concept (see 2.9 of NS-R-1:2000 and 3.8 and 4.23 of IAEA NS-G-1.3:2002).

a) The system may implement functions of the highest category allowed for its class (see 5.4.3) and functions of lower categories. The system may include subsystems of lower classes provided that the following requirements are fulfilled:
   1) the design requirements for each subsystem shall not be lower than those required by the function of the highest category implemented by the subsystem;
   2) the design of the system shall ensure that the requirements of the subsystems or equipment of the higher classes are satisfied in case of failure of the equipment of the lower class.
b) The design of the system shall include redundancy and other features necessary to provide tolerance to failure (see 6.2.3.3.4) and to accommodate the assignment of the application functions important to safety (see 6.2.3.5).

   NOTE 1 The system may also include redundancy to fulfil availability requirements. The need for such redundancies is defined at the level of system design.

c) The design of the system shall satisfy any independence requirements (see IEC 60709 and 6.2.3.3.3) to

- prevent propagation of failures from systems of lower importance to safety;
- prevent propagation of failures between redundant trains providing category A functions.

d) The design of systems in safety groups performing category A functions shall include sufficient redundancy to meet the single-failure criterion during operation and maintenance (see item e) of 6.2.3.5).

NOTE 2 Failures due to software are systematic and not random failures. Therefore, the single-failure criterion cannot be applied to the software design of a system in the same manner as it can be applied for hardware design. Possible effects of CCF due to software inside each defence line and between redundant subsystems are considered at the level of each system and of the I&C architecture (see IEC 62340).

6.2.2.3.3 Internal behaviour of the system

a) The design of the CB system should ensure a predictable behaviour consistent with the performance requirements of the implemented functions.

NOTE 1 A CB system may be said to have a predictable behaviour if the time delay between stimulus and response has a guaranteed maximum and minimum under all required conditions.

b) The communication technology shall be selected and sized to meet the performance requirements under all data loads generated by anticipated plant transients (including avalanches of changes of state in case of general loss of power supplies).

c) In order to provide a high degree of assurance of deterministic behaviour, class 1 systems should be developed using techniques such as those of Annex B of IEC 60880:2006 (notably B2.d “Execution time” and B2.e “Interrupts”). Techniques using static scheduling of operations (see Note 2) are preferable to those using interrupts.

NOTE 2 “Static” is defined as persistent during the operation of a computer program (examples are data structures that are neither created nor destroyed during operation after start-up, or scheduling parameters that are fixed after start-up). Thus, in static scheduling, the scheduling of an instruction or task does not vary depending on the sequence of external events and does not lead to varying use of computer resources, although there might be a finite number of different schedules depending upon the execution path.

NOTE 3 See 5.5.3 of IEC 60880:2006 concerning the role of the annexes to the standard and what is required if practices differing from those of the annexes are used.

d) Class 2 systems may be developed by techniques other than those defined in c). In such cases, the system design should ensure that the system will perform adequately under all required plant conditions (see IEC 62138 for details).

e) To increase the ability of class 1 and 2 systems to sustain unanticipated conditions:

- the adequacy of the design margins set for the use of resources, (such as CPU power, memory, communication bandwidth, operating system resources), and the internal timings within the system shall be justified;
- features should be provided to monitor any deviation from the deterministic behaviour and to reconstitute the correct plant status in case of temporary losses of input information, for example: watchdog, cyclic refreshing superposed to change of state activated detection of plant events.

6.2.2.3.4 Self-supervision and tolerance to failures

a) Systems should be designed so that errors and failures are detected sufficiently early to maintain the required system availability. The detection of failures by self-test facilities should be balanced against the complexity that is introduced. The requirements of 6.2 and A.2.2 of IEC 60880:2006 on self-supervision should be supported as far as possible for each class of system.

b) Adequate, timely and properly highlighted diagnostic information of failures should be provided to the plant operators so that they can carry out appropriate corrective actions.

c) The design of the system should enable the safe restoration to an appropriate back-up mode of operation when failures are detected (graceful degradation; fail-safe characteristics; switching outputs off in case of failure).

d) For class 1 systems, self-test facilities shall be in accordance with IEC 60880 and IEC 60987.

6.2.2.3.5 Testability

a) Systems shall have test provisions that permit verification of their ability to perform their functions important to safety.

NOTE In accordance with 4.83 of IAEA NS-G-1.3:2002, tests are preferably overall checks from the input sensors to the output actuation, but overlapping tests are acceptable. Tests include notably:

a) alteration of the state or value of any input signal, and monitoring of the alteration at the receiving equipment;

b) interruption of transmission, and confirmation that the receiving equipment will detect this and take a correct action;

c) testing and calibration of sensors;

d) testing of output actuation.

b) The principles of IEC 60671 shall be applied.

6.2.2.3.6 Maintainability

a) The system shall be designed in such a way that it facilitates maintenance and, in case of failure, easy diagnosis, safe repair or replacement, and re-calibration (see 4.97 to 4.100 of IAEA NS-G-1.3:2002).

b) Means for maintenance should be designed so that impacts on plant safety during maintenance are acceptable.

c) Human capabilities and limitations in relation to the environmental factors (temperature, humidity, space, accessibility, etc.) shall be taken into account to minimize the risk to, and workload on personnel during maintenance.

d) The system shall be designed to enable the repair and re-calibration of the system to be confirmed as correct. This shall include the checking of

- correct restoration of circuit continuity,
- correct calibration of analogue measurements and of any associated alarm thresholds,
- the ability of the system to perform as specified its functions important to safety.

NOTE The maintenance and testing requirements of Clause 11 of IEC 60987:2007 apply to CB systems important to safety of class 1 and class 2.

e) Special consideration should be given to the design of equipment in locations which cannot normally be accessed (for example the reactor containment). This may imply additional redundancy, or redundant communication lines.

6.2.2.4 Boundaries and interfaces with other systems and tools

In order to ensure the integration of the system in the I&C architecture, the following information shall be specified in accordance with the corresponding requirements of Clause 5:

- the intended location and the physical constraints relevant to the installation of the system in the plant (see 5.2.4);
- the physical and functional interfaces of the system with the supporting systems and equipment (see 5.2.4);

NOTE Requirements for electrical supplies of I&C systems important for safety are defined in IEC 61225 [16].

- the physical and functional interfaces of the system with other systems and equipment with which it exchanges information (see 5.4.2.4);
- the interfaces with software tools used to define the exchange of data between systems and the verification of consistency of such data (see 5.4.2.5).

6.2.2.5 Interfaces with users

The HMI requirements shall ensure that the risk of human error is minimized, for example, inadvertent errors, oversights, omissions during installation, operation, test and maintenance of the system and the plant, or when incorporating design modifications.

NOTE Protection against malicious modifications is handled in the security plan (see 6.3.3).

6.2.2.6 Environmental conditions

The normal and extreme ranges of environmental conditions that the system is required to withstand shall be specified in accordance with the constraints imposed from the plant design framework (see 5.2.4). Environmental conditions to be specified include:

- environmental conditions, including: temperature, humidity, pressure, radiation and electromagnetic interference during normal operation and accident conditions;

  NOTE 1 The following standards provide detailed guidance related to EMI: IEC 61000-6-2 [13] and IEC 61000-6-4 [14] specify minimum immunity levels and emission limits. The IEC 61000-4 series provides acceptable methods for qualification testing. IEC 62003 [15] provides additional clarification concernign the qualification parameters and criteria of the standards of the IEC 61000 series to ensure that nuclear safety requirements are met, e.g. for class 1 and/or class 2 systems..

- environmental conditions imposed by potential hazards external to the system including seismic conditions or flooding;
- power supply and heat removal conditions.

NOTE 2 Environmental conditions may also include issues such as ultraviolet radiation (e.g. degrades cable sheathing, erases EEPROMS), dust or particulate, arc welding.

6.2.2.7 Qualification

Systems important to safety shall be qualified. For computer-based systems, this qualification includes the hardware (including compliance with the applicable environmental conditions), the system software and the application software, both integrated in the hardware (see 6.5).

NOTE 1 Qualification of tools also needs to be addressed. The approach to be chosen depends on the required reliability and risk of errors and faults to be introduced by the tools, and the extent to which the tools' outputs will be verified. Guidance is provided in IEC 62138 and IEC 60880.

The qualification confirms the compliance of the design and of the equipment with the requirements. It covers all aspects provided in the system specification, i.e. compliance of the system characteristics with the system requirements as defined according to sections 6.2.2.2 to 6.2.2.6.

It is good practice to subdivide the requirements into requirements on system level and on the level of pre-existing hard- and software to be used for the system. This approach facilitates qualification using a staggered approach, i.e. by taking credit from existing qualification evidence for pre-existing equipment (pre-qualification, generic qualification), by qualifying hard- and software components separately, and then concluding by considering the hardware/software integration aspects.

The system specification shall identify the methods to be applied during design in order to ensure the feasibility of qualification of the hard- and software of the underlying equipment, and of the whole system. Subclause 6.5 provides details.

NOTE 2 The most efficient way for passing qualification is by having hard- and software design based on requirements and processes complying with the applicable IEC standards. See also Note 1 in 1.1 of this standard.

6.2.3 System specification

6.2.3.1 General

The objective of this phase is to provide the top-level description of the hardware and software architecture of the system, to specify the equipment to be used or developed for its implementation and to assign the application functions.

The system requirements specification and the documentation of pre-existing candidate equipment are among the inputs to the system specification.

The output documentation of this phase (see 6.4.3) forms the input for the activities which are to implement the combined hardware and software system during the subsequent phases of the system life cycle.

This phase includes the activities necessary to produce the software requirements, the hardware requirements, and the integration requirements of the system.

The system specification shall define

- the equipment to be used;
- the architecture of the individual I&C system;
- the software requirements;
- the assignment of the application functions in the subsystems.

6.2.3.2 Selection of pre-existing components

It is very common for pre-existing components (individual hardware and software components or components of an equipment family) to be used to implement a part, or the whole of a "new" system.

NOTE 1 Pre-existing components may be commercial off-the-shelf (also called "COTS") or proprietary products internally utilised by a manufacturer.

NOTE 2 Clause 15 of IEC 60880:2006 addresses acceptance criteria for reusable pre-existing software for category A functions; 5.2 and 6.2 of IEC 62138:2004 do so for category B and category C functions respectively. IEC 60987 provides guidance on the use of pre-existing hardware.

a) The suitability of the candidate components shall be evaluated and assessed to demonstrate that their characteristics comply with the system requirement specifications.
b) The suitability evaluation and assessment of the candidate components should be based on the comparison of two sets of documents: the requirements specifications of the system and the documentation related to the pre-existing components. The latter includes the product specifications, and (if available) pre-qualification documentation.
c) The following requirements apply:
    - it shall be analysed whether the documentation supplied defines explicitly the functionality and properties of all components;

      NOTE 3 Typical elements expected to be defined are: run time and memory consumption of software components, failure rates for the components, failure modes and fail-safe characteristics of the equipment for hardware faults and software errors, environmental conditions for the system configuration, requirements for the mounting in cabinets, for wiring and connections to power supply, power consumption, service tools.

    - those properties that are not explicitly defined shall be determined by analysis or test and made explicit;
    - the documentation shall allow the reliability and performance to be determined for the plant application functions in the anticipated configuration(s) of components;
    - the documentation shall define the functionality and properties of the associated software engineering methods and tools;

- unused functions (i.e. functions that are included in the equipment, but that are not going to be used) shall be identified. It shall be demonstrated that these functions cannot jeopardise the required functions.

  NOTE 4 If there are properties and characteristics of pre-existing components, which are not explicitly identified in the equipment's supplied documentation, or if the use of properties, characteristics or functions is to be restricted in order to satisfy system requirement specification, this may require the issue of a special, tailored version of the component's documentation which may then be basis for application-specific qualification (see 6.5.2). Tailored documentation focussing on safe utilization of a component is sometimes called "documentation for safety".

d) If discrepancies between the requirements specification of the system and the equipment family specification are identified which render the equipment unsuitable for the intended system class, the equipment shall be rejected. The assessment of the suitability shall establish that the specification of the candidate equipment complies with its intended use as defined by the system requirements specification (see 6.4.3.2).

NOTE 5 The characteristics of available products and equipment families as found during the evaluation may influence the subsequent design of systems, or possibly lead to iterations in the design of the overall I&C architecture.

e) For class 1 and 2 systems, the feasibility of qualification in accordance with the requirements of 6.5 shall be verified.

NOTE 6 Evaluation of feasibility of qualification involves not only technical properties of the candidate components but also contractual and organizational issues, e.g. the accessibility of detailed design documentation, and the availability of sufficient time, assuming that component qualification activities should be initiated at the latest with the beginning of system specification.

f) If results from pre-qualification are to be used (e.g. from a generic, plant-independent qualification program, or from a different project), the properties included in this pre-qualification shall be explicitly identified. The accessibility of the corresponding justifications through documentation shall be ensured. The additional work and constraints necessary for plant specific qualification shall also be identified.

6.2.3.3 System architecture

6.2.3.3.1 General

The system architecture is partitioned into a number of interconnected subsystems and components which provide the required redundancy and reconfiguration capability. The goal of system partitioning is to achieve an optimally simple arrangement of hardware and software which satisfy the functional and performance requirements, and which meet reliability and maintainability requirements.

The arrangement of system subsystems shall

- satisfy the design constraints of 6.2.2.3,
- allow the requirements on functional assignment of the application functions to be met (see 6.2.3.5),
- be consistent with the reliability requirements of the application functions important to safety (see 6.2.2.2.2).

6.2.3.3.2 Geographical distribution of subsystems (centralised/decentralised)

When defining the geographical locations of the subsystems in the plant and the transmission paths between subsystems, the following factors should be considered:

- the separation of redundant channels of majority voted equipment may be necessary to reduce the effect of localised hazards such as fire, and to meet the single failure criterion when this is required (see 6.2.2.3.2);
- the centralisation of functions important to security may be necessary to meet the requirement on control of unauthorised access (see 5.5.3);
- the centralisation of complex equipment may facilitate operation, periodic testing, maintenance, and environmental control;

- the use of serial or multiplexed data communication may reduce the quantity of cabling and ease the implementation of physical separation.

6.2.3.3.3 Independence

Independence includes provisions to prevent adverse interaction between subsystems of the system or with other systems which might result from abnormal operation or from failure of any component in either subsystem or system, including from common-cause failure. Adverse interactions could result from occurrences such as electromagnetic induction, short circuits, earthing faults, fires, chemical explosion, aircraft crash, and propagation of corrupted data.

a) When independence is required (see 6.2.2.3.2), it should be achieved by using:
   - electrical isolation, which can be achieved by fibre optics, optical isolators, cable shields;
   - physical separation, which can be achieved by distance, barriers, or a combination of the two;
   - independence of communication for CB systems, which can be achieved by selecting appropriate data communication architectures and protocols (see also 5.4.2.4).

   NOTE 1 Requirements for electrical isolation and physical separation are given in 4.36 to 4.48 of IAEA NS-G-1.3:2002.

b) In a class 1 system, the physical separation and electrical isolation between redundant subsystems shall meet the requirements of IEC 60709.

c) The separation and isolation between systems important to safety, and systems and equipment not important to safety, shall meet the requirements of IEC 60709.

   NOTE 2 The preferred method of physical separation and protection of the cables of a safety system, whether carrying electrical or optical signals, is the use of dedicated cable enclosures or trunking, providing full protection against hazards.

6.2.3.3.4 Defence against propagation and side-effects of failures

Due to the high degree of concentration of functions in computer based systems, measures should be taken to restrict the effects of failures within a single subsystem by good design practice, in addition to measures against propagation of failures between independent subsystems.

An equipment failure should not require too many manual control actions of the operating staff to manage the consequences of this event. This should especially be taken into account for the design of closed-loop controls in class 2/class 3 systems where the operator is frequently considered as a backup controller.

The following techniques may be considered to minimize the risk and the consequences of failure propagation and side-effects of failures in the architecture:

- internal isolation, where failures cannot propagate due to the lack of propagation paths and shared resources;
- system monitoring by internal means (i.e., self-supervision) or external means (i.e. other systems or operators) enabling early detection of corrupted data and/or deteriorated resources;
- defensive interfaces, enabling the system and its subsystems to identify corrupted inputs and/or erroneous interactions;
- on-line validation of redundant input signals used as input for the downstream processing;
- well-defined modes of behaviour to be taken when failures are detected, enabling the system to reduce its potential for, and/or the effects of, failure propagation.

NOTE 1 For class 1 systems, detailed requirements for avoidance of error-prone software structures and for verification and tests of software modules are given in IEC 60880.

NOTE 2 Detailed requirements for defence against propagation and side-effects of failures are given in IEC 62340.

6.2.3.4 Software specification

The software specification includes:

- specification of the application functions (application software specifications);
- specification of the software architecture;

  NOTE 1 The software architecture defines the major components and subsystems of the software, how they are interconnected, and how the required attributes will be achieved. The requirements for software architecture are outside the scope of this standard. (For class 1 systems, refer to IEC 60880; for class 2/class 3 systems, refer to IEC 62138.)

- specification of the service functions and system software functions.

  NOTE 2 When using pre-existing equipment families, system software specifications are mostly part of the equipment documentation.

Requirements for software specification are provided in IEC 60880 (for class 1 systems) and IEC 62138 (for class 2 and class 3 systems).

6.2.3.5 Assignment of the application functions in the system

This includes assignment of

- input signals to functions and of functions to specific processor units,
- voting process, priority handling, equipment protection functions,
- links of output control actions to actuators.

The following requirements apply:

a) The assignment of the application functions important to safety to the system and subsystems shall meet the functional, performance and categorization requirements specification of the functions (see 6.2.2.2.2).

b) The assignment shall take into account the containment of failures.

c) Processing of redundant functions and signals important to safety shall be assigned to separate subsystems, so that if a failure or a localised hazard occurs in one subsystem, the system can still perform its functions.

d) Functions of different categories assigned to the same system or subsystem shall all be considered as being of their highest safety category, except if it can be demonstrated that lower category data and functions cannot jeopardise higher category functions, for example, by stopping or causing spurious actuation of the higher category function. This may lead to the separation of the functions in different subsystems or to the decision to implement the lower category functions in other systems (iteration process with the overall assignment – see 5.4).

e) For category A functions, the single-failure criterion shall be met in operation, even when one redundant protection line is bypassed during maintenance.

6.2.4 System detailed design and implementation

6.2.4.1 General

The objective of this phase is

- to develop/procure the detailed design of the system hardware,
- to develop (design and coding), respectively procure, the computer programs which constitute the operational and support system software,

  NOTE 1 The normal situation (see 6.2.3.3) is that there are only limited new developments, for example, interfaces to other systems.

- to develop (design and coding) respectively automatically generate the application software of the system.

NOTE 2 It is common, when using pre-existing equipment families, that the application software code is automatically generated by tools from the application software specification (see 6.2.3.4).

The system specification documentation and the integration plan of the system are the main inputs of the detailed design and implementation phase.

The outputs of this phase are

- the hardware and software subsystems and components for the following phase of integration of the system,
- the computer programs to be run in the system.

The development/procurement of hardware and software are part of the hardware or software life cycles and outside the scope of this standard.

Requirements for software development are established in IEC 60880 for class 1 systems, in IEC 62138 for class 2/3 systems and in IEC 60987 for hardware requirements.

6.2.4.2 Required analysis

6.2.4.2.1 Functional validation of the application functions requirements specification

Functional validation aims to detect errors or omissions in the application function specification which may not be detected by the system validation (see 6.2.6). Functional validation involves modelling of actuation equipment and NPP operation. An I&C emulator, an engineering simulator or even a full-scope training simulator may be used as test environment.

a) The correctness of the application function specification versus the functional and performance requirements of the plant functions (see 5.2.2) shall be validated for functions of category A.

b) The functional validation of the application functions should be performed prior to the development of the application software, using analyses and simulations. The functional validation can also be performed during the detailed design phase, e.g. running the final application software with plant simulation models.

NOTE The validity of this validation depends on the quality of the simulator.

6.2.4.2.2 Reliability assessment

a) The reliability of the application functions performed by the system shall be justified as adequate. The rigour of the demonstration should be higher for the functions of the highest category:

   - the demonstration shall be based on deterministic criteria completed, when appropriate, by quantitative reliability analysis;
   - the estimation of the contribution of possible hardware failures to the reliability of the function shall be determined by a probabilistic quantitative analysis based on failure rates of components. The analysis embraces the system architecture and components and should consider both permanent and transient failures;
   - the estimation of the contribution of software potential design faults to the reliability of the function should be based on a qualitative evaluation, taking into account the complexity of design, the quality of the development process and the feed-back of operational experience. The evaluation should be based on a prior agreed method and should demonstrate that the software quality is consistent with the target reliability.

NOTE The results of analysis and simulation tests could be used for a quantitative evaluation, but there is no recognised method which could be used. For hard-wired systems, usually no quantification for failure resulting from design faults has been given.

b) The potential of system service functions to jeopardise the application functions shall be analysed with a rigour appropriate to the importance to safety of the application functions.

c) Where the function performed by the system is part of a safety group and there are reliability requirements placed by the I&C architecture on this safety group (see 5.4.4.2), the reliability analysis shall take into account the effects of single failures, CCFs and propagation of failures within all the systems contributing to this safety group.

d) For class 1 systems, the reliability analysis shall also assess the adequacy of the test facilities of the system with respect to the requirements of 6.2.2.3.5.

6.2.5 System integration

The objective of this phase is to assemble the hardware and software modules and to verify compatibility of the software loaded into the hardware.

NOTE 1 For the application of 6.2 and 6.3 to complex, programmable hardware such as PLD or FPGA, the requirements with respect to software are also applicable to such hardware's programming and configuration data.

System integration consists of the following steps:

- assembling and interconnecting hardware modules and subsystems as defined in design documents;
- building the target software from software modules;
- loading the target software into the target hardware;
- verifying that
  - the software complies with its design specification,
  - the hardware/software interface requirements have been satisfied,
  - the software is capable of operating in that particular hardware environment;
- documenting the configuration and releasing it formally for validation testing.

The subsystems and components of the system, the detailed design documentation, and the integration plan of the system are main inputs of the system integration phase. The following requirements apply:

a) Integration shall be performed in accordance with the integration plan and the configuration management plan defined in 6.3, with the underlying hardware modules having passed the manufacturing tests.

b) The performance requirements shall be verified when all the application software (either developed by the equipment family tools or specifically developed) has been integrated in the system.

c) The system shall be as complete as is practical for this testing.

d) The test cases selected for system integration testing shall exercise the interface characteristics of software modules and subsystems as well as the basic operation characteristics of the modules and subsystems themselves, with these characteristics taken from the requirement specification (e.g. timing, application-specific protocols). The tests shall demonstrate that performance of all equipment involved is adequate.

e) There shall be test cases which demonstrate that each selected application function performs its task.

NOTE 2 Depending on the design techniques used to ensure the predictable behaviour of the system (see 6.2.2.3.3), test cases including random data with high rates of change as inputs of the other functions inside the same CB system may be necessary.

f) Equipment used for system verification shall be calibrated as required.

g) Quality assurance measures shall be established for software tools used for verification, commensurate with the importance of those tools for verification.

h) The integrated system test report shall be reviewed and the test results shall be evaluated by a verification team with a good knowledge of the system specification.

i) If the resolution of a fault requires a modification to any verified hard- or software component or any design document, that fault shall be reported according to the procedures established (see 6.3.2.4). Any faults detected during the system integration that are strictly mistakes in the integration process itself, and that do not affect any project document, may be corrected without formal fault report.

6.2.6 System validation

The objective of this phase is to test the integrated system to demonstrate compliance with the functional, performance and interface specifications.

Testing shall be performed to validate the system and its software, programming and configuration data to be in accordance with the system requirements.

Validation shall comprise tests performed on the system in the final assembly configuration including the final version of the software and other programming data.

The integrated system, the system specification documentation and the validation plan of the system are main inputs of the system validation phase.

a) System validation shall be performed in accordance with the validation plan defined in 6.3.5.

b) The system shall be exercised by static and dynamic simulation of input signals present during normal operation, anticipated operational occurrences and accident conditions requiring action by the system under test.

c) Each function of the system shall be confirmed by representative tests with respect to functionality, performance requirements and interfaces. Not covered requirements shall be justified.

d) For category A and B functions, each trip or protection parameter shall be covered singly and for relevant combinations. The tests shall:

   - cover all signal ranges, and the ranges of computed or calculated parameters in a fully representative manner;
   - cover the voting and other logic and logic combinations comprehensively;
   - be made for all trip or protective signals in the final assembly configuration;
   - ensure that accuracy and response times are confirmed, and that correct action is taken for the relevant equipment failure or failure combination;
   - be made for all other functions which have a direct impact on reactor safety (e.g. vetoes, interlocks).

e) For category C functions:

   - Each function shall be covered by an appropriate and justified set of tests, based on representative ranges of signals, parameters and combinations of logics. Every individual signal shall be checked.
   - Critical accuracy or response time requirements of signals should be confirmed by tests.

f) For class 2 and class 3 systems, there may be a need for specific tests, e.g. tests of failure recovery features, or tests of effects from changing system loads (if the system is programmed not to be independent of the plant demand).

g) The system shall be checked to provide defences against operator errors and failures of other systems and equipment, as defined in the system requirement specification.

h) Equipment used for validation shall be calibrated and configured (hardware and software parameters) as appropriate.

i) Equipment used for validation should be shown to be suited to the purpose of the system validation.

The system validation report shall document the results of the validation of the system.

a) The report shall identify the hardware, the software and the system configuration used, the equipment used and its calibration and the simulation models used.

b) This report shall also identify any discrepancies.

6.2.7 System installation

The objective of this phase is to install, interconnect and test the system on site.

The subsequent activities related to the overall integration of the system with the other systems and the overall commissioning are part of the overall I&C safety life cycle (see Clause 7).

a) System installation shall be performed in accordance with the installation plan defined in 6.3.6.

b) Appropriate means, for example tagging or colour coding, shall be used for unique identification of the components, cables and equipment making up the system to reduce the likelihood of installation, operation and maintenance errors.

6.2.8 System design modification

Modifications to the design of the system may be required due to the identification of new system requirements or due to the discovery of system design defects during the evaluation of operation records and reports.

a) The implementation of a modification to a system shall be carried out in accordance with defined procedures (see 6.4.7).

b) Testing of the correct operation of the system shall be done after a modification.

c) No hardware/software modifications, other than those specified in the maintenance procedures, shall be allowed as a matter of routine.

d) Should replacement hardware be required, it shall be demonstrated/justified that the replacement meets the specification of the original hardware.

e) The modification process of software shall be in accordance with Clause 11 of IEC 60880:2006 for class 1 systems and 5.10 and 6.10 of IEC 62138:2004 for class 2/class 3 systems. The modification process of class 1/class 2 hardware shall be in accordance with Clause 12 of IEC 60987:2007.

6.3 System planning

6.3.1 General

The objective of the requirements of this subclause is to develop system plans to ensure that the requirements of the I&C functions important to safety implemented in the system will be achieved and maintained*.*

The requirements of 5.5 address complementary overall plans for functions distributed within interconnected systems.

NOTE The following requirements on plans do not preclude that the plans may be organised in a different number of documents.

The system plans shall be established in an early stage of the system life cycle before any of the activities addressed are initiated.

6.3.2 System quality assurance plan

6.3.2.1 General

a) A quality assurance plan shall be established and implemented to cover each of the activities of the system safety life cycle. The requirements for the system quality assurance plan shall be derived from IAEA GS-G-3.1 and ISO 9001.

b) The system quality assurance plan shall include the activities that are necessary to, achieve the appropriate quality of the system, for verifying that the required quality is achieved, and to provide objective evidence to that effect. The requirements on verification activities are established in the system verification plan (see 6.3.2.2).

c) The system quality assurance plan shall address system quality and quality aspects related to the integration of hardware and software. Hardware or software specific quality assurance plans are outside the scope of this standard.

NOTE The requirements for the software quality assurance plan of safety systems are defined in 5.5 of IEC 60880:2006 (for class 1 systems) and in 6.1 and 5.1 IEC 62138:2004 (for class 2/class 3 systems).

d) The system quality assurance plan shall include:

- identification of the governing standards and procedures to be used for the project;
- identification of the phases of the system life cycle, the elementary tasks and the expected results of each phase;
- description of relationships and interactions between the different tasks;
- description of the organisational structure;
- procurement of components from external suppliers;
- product identification and traceability. The corresponding requirements are established in the configuration management plan (see 6.3.2.3);
- identification of all inspection and testing procedures;
- identification of QA activities and tasks;
- identification of personnel/organisations responsible for QA activities and tasks, including requirements for organisational independence between relevant activities in the project lifecycle;
- procedures for reporting and disposition of non-conformance to requirements, standards and procedures. The procedures shall include consideration of the impact upon NPP safety and shall ensure that all effects of the non-conformance are identified, for example interchangeability, maintenance, spares, operating instructions, etc.

e) The quality assurance plan shall be established at an early stage of the system life cycle and shall be planned within the general schedule of the other activities of the I&C safety life cycle. The plan may be either a part of the system specification or a companion document (see 5.5 of IEC 60880:2006 for class 1 systems and 6.1 and 5.1 of IEC 62138:2004,or class 2/class 3 systems).

6.3.2.2 System verification plan

a) A system verification plan shall be developed describing

- the verification process across all the phases of the system safety life cycle,
- the corresponding organisation and responsibilities.

b) The outputs generated by each phase of the system safety life cycle shall be verified against its identified inputs.

c) Every verification step shall produce a report of the analysis performed and the conclusions reached. When a phase is completed, a final report shall be produced, showing the compliance of the outputs of the phase with the inputs requirements and the resolution of anomalies.

d) Verification shall be carried out by persons competent in the subjects addressed, who have a good understanding of the inputs against which the verification is made;

involvement of the representatives of those concerned with the use of the results is recommended.

e) The thoroughness of the verification plan shall be commensurate with the safety class of the system. The verification plan shall highlight the safety relevant aspects to be verified and should recognise that the probability of fault or omission in complex items is greater than in simpler ones.

f) The documents subject to a verification review shall be identified in the system quality assurance plan.

g) The documents involved in a verification review, i.e. inputs and outputs of activities, verification reports, and possibly the tools used to elaborate the outputs, shall be placed under configuration management.

h) For class 1 systems, the verification plan shall be developed and implemented by individuals independent of the designers of the system (according to 8.2.1 of IEC 60880:2006).

6.3.2.3 System configuration management plan

a) Configuration identification:

   - appropriate baselines shall be defined at control points within the system life cycle and the items to be controlled in the baseline shall be defined. Controlled items may be intermediate and final outputs (such as hardware, software, verification documentation, user documentation) and elements of the support environment (such as compilers, tools, test beds);
   - all of the items to be controlled shall be identified. Every unique item shall have a unique reference and different versions shall be uniquely identified;
   - the links between the items in the baseline and the item(s) from which they were developed shall be established and recorded;
   - the configuration management system shall be able to re-construct the configuration of all system baselines;
   - search facilities should be provided so that links and multiple occurrences of items can be identified easily.

b) Configuration control:

   - the configuration control shall provide the facilities required to initiate a design freeze. Procedures and authority required for any further modification following a design freeze shall be defined including the allocation of responsibilities and authorities for CM activities to organizations and individuals within the project structure;
   - the status of each controlled item shall be tracked; this includes information on the initial approved version, the status of requested changes and the implementation of approved changes;
   - the configuration management plan shall identify the configuration audits and reviews to be held;

   NOTE 1 It is good practice to distinguish between internal items (i.e. those developed within the project) and external items (those provided by vendors/subcontractors), and to define activities to control the interface to external items.

c) The configuration management plan shall be defined at the beginning of the system project and be maintained during the whole system life cycle.

   NOTE 2 ISO 10007 [17] provides definitions and guidelines for configuration management, IEEE 828 [18] provides guidelines for software configuration management plans.

6.3.2.4 Fault resolution procedures

Procedures for the reporting and resolution of faults found during system integration verification, during system validation and in later phases shall be established before the corresponding phases begin.

a) These procedures shall be referenced by the system integration and system validation plan.

b) These procedures shall apply to all faults found during the system integration phase and system validation phase that require modifications to verified software, hardware or system design documents.

c) They shall ensure that any required re-verification of system design, hardware or software is performed according to the system configuration management plan.

d) They shall ensure that any required modification of system design, hardware or software is carried out according to the modification procedure of 6.2.8 and 6.4.7 and to the system configuration management plan.

e) An evaluation of each fault reported shall be made to determine whether any systematic deficiency exists and also to determine whether the fault was of such a nature that it should have been detected at an earlier phase of the verification.

f) If this is found to be the case (i.e. it should have been detected at an earlier phase), then an investigation of that phase shall be conducted to determine whether any systematic deficiency of the verification exists.

g) If the evaluation of faults shows that there is a systematic deficiency of the verification, causing faults in software or hardware to remain undetected, then the deficiency shall be identified and corrected or justified.

6.3.3 System security plan

The system security plan is defined to be consistent with the overall security plan (see 5.5.3).

a) During system specification and design the requirements for technical counter-measures identified for the system in the overall security plan (see 5.5.3) should be transformed into technical design requirements and documented.

b) An assessment of the design documentation shall take place to verify that the counter-measures identified within the system security analysis have been correctly implemented.

c) During verification and validation of the system, the effectiveness of the security functions shall be demonstrated through suitable tests with the system in its final configuration.

6.3.4 System integration plan

The system integration plan addresses the procedural and technical measures used to integrate subsystems into the system and to integrate hardware and software.

a) A system integration plan shall be prepared describing the types of tests to be performed, test environment and acceptance criteria.

b) The integration test shall be based on a concept of stepwise integration.

c) A distinction should be made between system-related tests (functions of system software and hardware) and plant-specific tests (application functions).

NOTE Tests of modules (hardware, software, combined modules, programming of complex electronic components such as PLDs or FPGAs) performed during product development, pre-qualification or preceding projects may be used in order to avoid repetition of identical or unnecessary test cases.

d) In the system integration plan, the simulation of any part of the system or its interfaces shall be demonstrated to be essential and equivalent to the actual part. The plan shall identify tests performed on the actual system and those performed using simulation of interfaces. The equivalence of simulation shall be demonstrated. The simulator shall be put under configuration control.

e) The system integration plan shall identify the tests to be performed for each computer unit or subsystem interface requirement.

f) The system integration test plan shall be reviewed by a verification team with a good knowledge of the system specification.

6.3.5 System validation plan

The system validation plan addresses the procedural and technical measures taken to demonstrate that the system meets its system specification and its system requirements specification. The validation of the application functions requirements is considered in the functional validation phase (see 6.2.4.2.1).

a) A system validation plan shall be developed describing the configuration(s) of the system for validation, the tests and analyses to be performed and the reports to be produced.

   1) Validation test documents shall specify the system configuration to be tested, the input data, methods, tools and calibrations to be used and the relevant acceptance criteria. When relevant, the accuracy and the influence of the observation tools on the behaviour of the system should be assessed.

   2) Validation analysis documents shall specify what the tests should demonstrate, the expected results and the relevant acceptance criteria.

   NOTE 1 It is good practice that preparation of the system validation plan and of the test specifications starts with the completion of the first version of the system requirement specification, so that the observations during preparation of the test specifications can be used as an early feedback to the preparation of the requirement specification.

b) For category A functions, the system validation plan shall be developed, validation activities shall be performed and results evaluated by teams independent from the ones who designed, implemented, or modified the system (Clause 10 of IEC 60880:2006).

   NOTE 2 Independence is not required between individuals involved in the execution of the validation plan and the production of the validation report.

c) For category B functions, the development of the system validation plan shall include, and shall be the responsibility of, persons who did not participate in the design, implementation, and/or modification of the system.

d) For category A and B functions, the system validation plan shall provide traceability between the specification and the corresponding tests and verifications.

e) For category C functions, the system validation plan should provide traceability between the specification and the corresponding tests and verifications.

It is good practice to implement the validation testing in several stages in the factory and on site. A strategy for staggered validation testing (see also 5.5.4) may include steps such as

- simulation/emulation tests validating the application software,
- first set of validation tests in the integration test field in the factory,
- second set of validation tests during the integration testing on site,
- completion of validation tests in the framework of the overall plant commissioning program.

6.3.6 System installation plan

The system installation plan addresses the procedural and technical measures for installation of the system on site and for the checking needed to provide assurance that the system is ready for operational use. The plan is complemented by the overall integration and commissioning plans (see 5.5.4).

a) A system installation plan shall be developed to describe the measures to be taken to ensure and verify that the configuration of the system and of any modifiable parameters is correct, that the system is complete, correctly installed, assembled, connected and is operational as required and specified.

b) For class 1 systems, the installation plan shall meet the requirements of Clause 10 of IEC 60987:2007.

c) For category A functions, each safety channel shall be demonstrated to be correct on site.

6.3.7 System operation plan

The system operation plan addresses the way the system shall be operated and the requirements applicable during system operation.

a) A system operation plan shall specify how the system is to be operated in all modes of operation. The plan shall be consistent with the system maintenance plan (see 6.3.8) and the overall operation and maintenance plans (see 5.5.5 and 5.5.6).

b) The system operation plan should specify the conditions to be met before the system is put into operation. In particular:
   - the system shall have completed installation, integration and commissioning (see 5.5.4);
   - the system maintenance plan (see 6.3.8) and user documentation shall be available.

c) When periodic testing is required (see 6.2.2.3.5), the system operation plan shall specify
   - the frequency and duration of each test, the conditions to be met prior to the initiation of a test and the effects, if any, on the operation of the system and of the plant;
   - the steps necessary to perform each test, the tools and tool calibrations to be used, the analysis of the correctness of results;
   - the verification of complete restoration to normal state, if temporary changes in the system are required.

   NOTE Periodic testing involves both the operation and maintenance teams. This activity may also be considered as part of routine maintenance (see 6.3.8).

d) The system operation plan shall specify the records to be maintained during system operation. The records shall include details of failures, records of tests of the system and a record of the demands on the system.

e) The system operation plan shall be considered for the impact it may have on the safety of the plant.

f) The system operation plan shall define periodic testing in line with the provisions defined in accordance with 6.2.2.3.5.

6.3.8 System maintenance plan

System maintenance includes the procedural and technical measures to be taken to maintain the functionality of the operational system. The system maintenance plan is developed to be consistent with the system operation plan and the overall operation and maintenance plans (see 5.5.5 and 5.5.6).

a) A system maintenance plan shall be developed and it shall specify
   - the routine actions and procedures that will be used to detect unrevealed failures of the system, maintain the "as-designed” functional performance and reliability of the system (preventive maintenance),
   - the actions and procedures which need to be carried out to restore the system to a fully operational state (corrective maintenance).

b) The extent of preventive maintenance should be determined using a systematic analysis method, such as a failure mode and effect analysis, or by application of a reliability centred maintenance model, or by examination of fault trees for the system functions.

c) The procedures for replacement of components shall ensure that
   - replacement components are functionally identical to those being replaced and meet the quality requirements;
   - if replacement is performed on line, its impact upon the functionality of the system is assessed and documented prior to replacement;
   - a record is maintained of all replacements, enabling any requirements for traceability to be achieved.

d) The procedures for re-calibration shall ensure that

- the new calibration is within defined limits (when such limits are enforced by the system, no formal constraint need be placed upon the maintenance staff),
- if re-calibration is performed on line, its impact on the functionality of the system is assessed and documented prior to re-calibration,
- a record of all re-calibrations is maintained, enabling any requirements for traceability to be achieved.

6.4 Output documentation

6.4.1 General

This subclause defines the output documentation of the phases of the system life cycle: content, characteristic and the main topics which need to be verified.

The output documentation shall constitute a set of appropriately cross-referenced mutually consistent documents, which ensures the traceability of the final design to the input requirements.

6.4.2 System requirements specification documentation

6.4.2.1 Content

The system requirements specification shall be complete, providing all information needed for the subsequent activities of the system safety life cycle, and for the qualification of the system.

6.4.2.2 Characteristics

Characteristics of the system requirements specification document:

a) the requirements shall be unambiguous and verifiable;

b) main users of the requirements specification are the reviewers and those in charge of the system specification and the functional validation. The requirements shall be clear, concise, complete, consistent and correct, and prepared with these intended readers in mind;

c) the requirements of the application functions should be stated in functional terms rather than in terms of computer technology in order to allow their verification by I&C functional engineers and plant operators, who may have limited knowledge of computer technology;

d) the requirements should be specified using documented system engineering methods, tools and guidelines;

NOTE Detailed requirements regarding software tools for class 1 systems are given in Clause 14 of IEC 60880:2006.

e) the requirements should be written and structured to facilitate compliance assessment for the system specification, and provide a reference for the system qualification plan.

6.4.2.3 Verification

The following points shall be verified:

a) requirements shall be traceable and consistent with the requirements for the system established in the architectural design and functional assignment (see 5.6);

b) interface requirements shall be consistent with those of the interfacing systems and equipment;

c) requirements that unnecessarily increase the complexity of the system should be identified (complexity may increase the risk of faults in the system requirements specification and/or in the system itself).

6.4.3 System specification documentation

6.4.3.1 Content

a) The system specification documentation shall be complete and unambiguous and shall provide all the information needed for the subsequent activities of the system safety life cycle, notably for the system design and validation phases.

b) The system specification documentation shall identify the equipment to be used, i.e. pre-existing or to be developed. The suitability of selected equipment shall be justified.

c) The system specification documentation shall describe the architecture of the system:

- the decomposition of the system into subsystems, and/or into hardware and software components;
- the internal behaviour of the system (see 6.2.2.3.3), including the description of the main postulated events internal to the system and its defence to these events (see 6.2.3.3.4);
- the boundaries, environmental conditions, expected hardware reliability, behaviour, functions, performances and interfaces of each subsystem;
- the classification of each subsystem; justification should be provided if the subsystem class is lower than the class of the system or subsystem in which it is included;
- the conditions of use and the connection of the identified subsystems within the system.

NOTE The subsystem description may be organised into a hierarchy so as to facilitate understanding from a general overview down to elementary subsystems (i.e. subsystems that are not further decomposed by the system design documentation). "Horizontal" information may also be useful.

d) The system specification documentation shall include the software specification (see 6.2.3.4).

e) In a class 1 or 2 system, the assignment of the functions to the subsystems shall be identified, i.e. the system specification shall indicate which subsystems contribute and/or are necessary to the performance of a given function.

6.4.3.2 Characteristics

Characteristics of the system specification documentation:

a) main users of the system specification documentation are the reviewers and those producing the system design and completing integration and validation. The documentation should be clear, concise, complete, consistent and correct, and written in a way adequate for these staff;

b) the specification of the application functions should be stated in terms that ease verification and facilitate their understandability by I&C functional engineers and plant operators;

c) the system specification should be developed using documented system engineering methods, tools and guidelines. These methods, tools and guidelines should minimize the “gap” between the methods, tools and guidelines used for the system requirements specification activity;

NOTE Software engineering methods and tools can improve the quality of the final system design specification, even in comparison with the design specification of a hard-wired system.

d) the system specification should be written and structured to facilitate the assessment of its consistency with the system requirements specification, and to provide an effective reference for system validation, i.e. it should facilitate a comprehensive identification of specifications (as opposed to explanations and other information).

6.4.3.3 Verification

a) The verification of the system specification with respect to the system requirements specification should be carried out before the detailed design activity is finished. It should enable corrective actions before the system is implemented and integrated.

b) Effective communication between those in charge of the specification of the system and the suppliers should be established to enable the suitability of the selected equipment to be verified.

c) The verification shall document consistency and record any non-conformance of the system specification with respect to the system requirements specification.

d) The translation of the application function requirements specification into the application software specification shall be verified to be correct.

e) For class 1 and 2 systems, any non-conformance shall be corrected or shall be justified with respect to safety, taking into account possible compensatory measures.

f) For class 1 and 2 systems, features that increase system complexity and that are not required by the system requirements specification shall be identified and justified with respect to safety.

NOTE The presence of system features not required by the system requirements specification may significantly increase the complexity of the system, which could potentially decrease confidence in its correct operation.

6.4.4 System detailed design documentation

6.4.4.1 General

The detailed design may be implemented in a number of iterations. The requirements of this subclause address the final documentation of the system that is available when the detailed design, integration and validation of the system are completed and the system is ready for delivery and installation on site.

The system detailed design documentation may normally be divided up into four groups of documents. These are

- the system design documents,
- the required analysis (see 6.2.4.2),
- the application software design documents,
- the system hardware components and system software design documents.

NOTE 1 If the system is implemented with pre-existing equipment, the system hardware and system software design documents are part of the pre-existing equipment documentation.

Only the first two groups are addressed, as software and hardware design is outside of the scope of this standard (see 6.2.4).

NOTE 2 For class 1 and class 2/3 systems, requirements on software documentation are established in IEC 60880 and IEC 62138, and requirements on hardware documentation in IEC 60987.

6.4.4.2 Content

a) The system design documents shall be complete, unambiguous and shall provide all information needed for the subsequent activities of the system safety life cycle including integration, validation, installation, operation, and maintenance.

b) The system design documents expand the specification documents and shall provide a detailed description of the internal structure and the internal behaviour of the system. The level of detail of this description may be adapted to the safety class of the system.

c) The system design documents shall include the description of the installation of the equipment in the plant and of the provisions for system testing.

d) The system design documents shall include the description of the validated functionality and performance of the system, in particular the expected response time under different plant conditions, the nominal safety settings of set points and control algorithms, and the margins of safety settings.

6.4.4.3 Characteristics

Characteristics of the system design documentation:

a) Main addressees of the system design documentation are the authors and reviewers of the system integration plan, the system qualification plan, the system installation and commissioning plan, and the system maintenance plan, maintenance staff, authors and reviewers of design modifications. The documentation should be written in a way adequate for these staff.

b) The detailed design documentation shall be maintained during system development to ensure that the final version of the documents corresponds to the "as built" design.

6.4.4.4 Verification

a) The verification of the system detailed design and its documentation should be carried out before the implementation of new hardware and software; sufficient time should be allowed to enable the implementation of any corrective actions arising from the verification.

b) The reliability requirements specified for the application functions of the system (see 6.2.4.2.1) should be verified as achievable at an early stage of the detailed design.

   NOTE The system reliability analysis may require amendment of the detailed design, the system architecture, for example the degree of redundancy and even the choice of the overall I&C architecture solutions.

c) The potential of system service functions to jeopardise the application functions shall be rigorously analysed by means appropriate to the safety role of the application functions.

d) The assumptions made in the detailed design verification shall be stated and documented.

6.4.5 System integration documentation

6.4.5.1 Content

The system integration documentation shall include the integration plan, integration test reports and all information needed for the subsequent validation phase.

6.4.5.2 Characteristics

Integration test reports shall contain the following information:

- the versions of the hardware and software modules, the test specification used, the tools and equipment used, together with any relevant calibration and equipment set-up data, any equipment or interface simulations used;
- the results of each test listing any discrepancies between the expected and actual results, and, for each discrepancy, a record of the analysis made and the decisions taken on whether to continue the test or implement a change;
- the resolution of all reported faults and the results of the subsequent evaluation shall be documented in sufficient detail and in a manner that is auditable by persons not directly engaged in the system development and verification plan.

6.4.5.3 Verification

a) The verification of the system integration reports with respect to the system integration plan should be carried out before the validation activity.

b) For class 1 and class 2 systems, traceability from the design documentation to the corresponding component and integration tests and analyses shall be provided, so as to enable the assessment of the tests and analyses with respect to test coverage. The granularity of traceability for class 2 systems may be less stringent than for class 1 systems.

c) For class 3 systems, traceability from the design documentation to the corresponding component and integration tests and analysis should be provided, so as to enable the assessment of the tests and analyses with respect to test coverage.

6.4.6 System validation documentation

6.4.6.1 Content

The system validation documentation shall include the validation plan, the validation test reports and all information needed for the system qualification.

6.4.6.2 Characteristics

a) The system validation report shall document the results of the software aspects of the validation of the system.

b) The report shall identify the hardware, the software, other programming and configuration data and the system configuration used, the equipment used and its calibration and the simulation models used.

c) The report shall also identify any discrepancies between the expected and actual results, and, for each discrepancy, a record of the analysis made and the decisions taken on whether to continue the test or implement a change.

d) The report shall summarize the results of the system validation.

e) The report shall assess the system compliance with all requirements.

f) The results and the results of the subsequent evaluation shall be retained in a form and sufficient detail to be auditable by persons not directly engaged in the validation.

g) Software tools used in the validation process should be identified as an item in the validation report. Simulations of the plant and its systems used for the validation shall be documented.

6.4.6.3 Verification

The results of validation testing and analysis shall be documented and reviewed against the requirements expressed in the system validation plan to confirm that the functional performance of the system meets those requirements.

NOTE The validation documentation together with the functional validation documentation (see d) of 6.4.4.2) confirms the system compliance with both system specification and system requirements specification.

6.4.7 System modification documentation

6.4.7.1 Content

a) Modification request

   This document shall state

   - the justification for the change and the effect (if any) on the safety of the NPP,
   - the functional description of the change (with marked-up drawings, flow diagrams, configuration drawing, etc.) and the proposed means of implementing the change,
   - the relationship of the modification to any other related plant modifications.

b) Modification package

   When the design change has been completed, i.e. the software components, hardware components and documentation reflect the revised design, a change package should be prepared to introduce the change in the operational system. The documentation package shall describe the hardware modules, software modules and means of implementing the change, i.e. what equipment should be powered down, what procedure shall be followed to load new software, or a reference to approved existing modification procedures may be provided.

6.4.7.2 Characteristics

The modification request shall be uniquely identified and shall be subject to assessment and authorisation or rejection by competent and appropriate persons. The result of the assessment (accept or reject) shall be recorded.

6.4.7.3 Verification

a) For class 1 systems, the implementation package shall be reviewed for completeness and technical correctness by personnel who were not directly involved in the design modification, but who are technically competent to assess the change.

b) The modification package shall not be incorporated into the system without an assessment of the change.

6.5 System qualification

6.5.1 General

This subclause sets out requirements for the qualification for classified I&C systems (see 6.2.2.7). This process provides assurance that an I&C system is capable of meeting, on a continuing basis, the design basis functional and performance requirements needed for the functions important to safety while subject to the specified environmental conditions and specified constraints (see 6.2.2.2 to 6.2.2.6).

NOTE The IEC 61508 series can be used as complementary guidance for the qualification and assessment of components.

6.5.2 Generic and application-specific qualification

It is convenient to take credit from evidence of qualification of hardware and software components, established outside the framework of a plant design or specific application context (i.e. pre-qualification or generic qualification of COTS products or of an equipment family), so as to split essential parts of the qualification effort over several projects (see 6.2.3.2). Generic qualification may have been performed as a joint effort for several NPP projects, or by a vendor of an equipment platform for safety-related applications. Pre-qualification may also have been performed for products initially oriented towards other domains than design of nuclear power plants, not necessarily fully in line with the methods and procedures required for the project.

NOTE 1 Certification of COTS products to SIL 1, 2 or 3 safety integrity levels according to the IEC 61508 series by an independent and accredited safety assessor is an example of a form of pre-qualification of COTS equipment. Since the IEC 61508 series is the umbrella standard of IEC 61513, such a certification provides a good starting point for application-specific qualification of COTS products, and for demonstrating the compliance with the requirements of IEC 61513 and its daughter standards.

Relying on pre-qualification of pre-existing equipment requires that application-specific qualification is performed, in order either to confirm the compliance of the evidence of pre-qualification with the requirements of the I&C system, or to fill the gaps identified. This application-specific qualification may imply a variety of activities such as accepting the existing qualification results based on analysis of the existing documentation, performing audits, performing supplementary functional, environmental and seismic testing and evaluating feedback from experience.

a) Depending on the extent of the available documentation and evidence of pre-qualification, an appropriate qualification program shall be defined and included in the qualification plan (see 6.5.3).

b) The application-specific qualification shall address the properties and characteristics not covered by pre-qualification.

c) The application-specific qualification shall address the differences between the qualification methodology and procedures applied for pre-qualification, and those imposed by the system requirement specification (see 6.2.2.7).

NOTE 2 Application-specific qualification typically considers the following:

- that pre-qualification evidence is applicable and complies with the requirements of the I&C system;
- that any gaps in the evidence are identifies and filled;
- if replacing equipment, that any design differences with respect to the current equipment or system are examined and no adverse effects are confirmed;

- that the acceptance and performance criteria used in pre-qualification testing are suitable for the current application.

The system qualification process may be accomplished in stages: first by qualifying the individual hardware and software components of an I&C system, and then by qualifying the integrated I&C system (i.e. the final realized design).

d) The qualification of the hardware and system software of a system built up by configuring an equipment family or connecting pre-existing components may be derived from the qualification performed on individual components and configurations of interconnected components. In such cases, an analysis shall be completed to demonstrate that the qualification covers the final configuration of the system used in the plant, including mounting arrangement, load and temperature distribution inside the cabinets.

e) Based on the previous analysis, the qualification plan should identify all novel features of the system design and define whether complementary qualification tests and evaluations are to be carried out.

6.5.3 Qualification plan

6.5.3.1 General

A qualification plan shall be developed which identifies all the topics to be evaluated and assessed in order to qualify the system and the functions important to safety that it implements and to maintain the qualified status.

The qualification plan includes hardware, software and system aspects. Even if hardware and software components will be used that have passed pre-qualification in line with the applicable qualification standards, as a minimum the available qualification documentation shall be assessed against the system requirements so as to confirm the suitability and the integrated system aspects shall be evaluated (suitability analysis).

Figure 6 provides an overview of the activities.

NOTE Qualification of a pre-existing component or COTS product is always specific to a particular version of that product. Any modifications to the design constitute a change of version and the qualification will need to be reassessed.

6.5.3.2 Functional and environmental qualification

NOTE 1 Functional and environmental qualification is also called “hardware qualification”.

Several techniques may be used to perform the functional and environmental qualification of the system. Typically, it is performed in separate steps, first on the level of individual components or subsystem assemblies, and then on the level of the whole system. Qualification of components and subsystem assemblies include type-testing, functional testing, design assessments and analyses and operating experience in similar applications. Type testing is the preferred method (see 4.1 of IEC 60780:1998).

NOTE 2 Typically, functional qualification involves the operation of equipment integrated with its firmware or system software and being operated with representative applications. Also, it typically constitutes the latest step of firmware/hardware integration testing in the development cycle of CB equipment.

a) Class 1 and class 2 systems shall be qualified for their environmental conditions in accordance with the requirements of IEC 60780 and IEC 60980. Environmental conditions shall include those specified in 6.2.2.6.

b) Class 3 systems for which specific environmental qualification is required (e.g. resistance to seismic conditions, or operation under specific environmental conditions), may be qualified to industrial standards. Claims for operation in abnormal environmental conditions, seismic qualification to industrial standards or other credited functional performances shall be justified by documentary evidence. Where significant ageing factors exist, and when qualified life cannot be demonstrated in accordance with the definition given in IEC 60780, an on-going qualification program shall be proposed and justified compliant with IEC 60780.

c) EMC qualification shall be performed in accordance with the applicable requirements of the IEC 61000-4 series. Environmental conditions shall include those specified in 6.2.2.6.

d) Test sequences including acceptance criteria shall be defined for the testing of components or configurations of components or the whole system as appropriate in order to

   - check the functional characteristics under normal ambient conditions and at all specified limits of operation,
   - check the specified self-surveillance, fail-safe characteristics and degraded modes of operation,
   - demonstrate the resistance to the relevant environmental conditions (including seismic and electromagnetic environment).

e) Analyses shall be performed as necessary to justify system characteristics which cannot be adequately substantiated by other means. These may include

   - reliability analyses providing or justifying reliability data,
   - failure mode and effect analyses confirming the specified failure modes and providing coverage data for self-surveillance functions,
   - analyses of circuitry confirming the specified functionality, accuracy or margins.

6.5.3.3 Software evaluation and assessment

NOTE 1 Software evaluation and assessment is also called “software qualification”.

The evaluation and assessment of software takes into account the rigour of software development process and the extent of testing and validation performed on the integrated system. For pre-existing software (PDS), feedback of operating experience may constitute under certain conditions a compensating factor for lack of information of the development process.

The software of the CB system to be qualified includes:

- the system software, which may be pre-developed software not specific of the plant;
- the application software integrated into the system, which is plant-specific.

a) The qualification shall evaluate and assess both the system software and the application software to provide adequate assurance that the software quality is appropriate for achieving the required reliability of the functions performed by the system.

b) For class 1 systems, newly developed software shall be evaluated and assessed in accordance with the requirements of IEC 60880.

c) Software of pre-existing equipment selected for class 1 systems should have been developed according to recognised guides and standards appropriate to the high level of quality required for category A functions (see 7.2.2.1 of IEC 61226:2009). In particular, the requirements of IEC 60880 on pre-existing software and tools and the requirements of IEC 60987 shall be met.

   NOTE 2 Subclause 15.3.3 of IEC 60880:2006 defines acceptance criteria and restrictions on use of documented feed-back of experience in the qualification process.

d) Software of pre-existing equipment selected for class 2 systems should have been developed according to recognised guides and standards. Otherwise, the software may be qualified according to the criteria of IEC 62138, taking into account a documented history of satisfactory operation of the software in similar applications.

e) Criteria for evaluation, assessment and acceptance of software for class 3 systems are provided by IEC 62138.

6.5.4 Additional qualification of interconnected systems

a) A plan shall be developed for the additional testing that may be required at the level of the interconnected I&C systems to complete their individual qualification, for example electromagnetic interference tests of the interfaces for the specific lay-out and grounding, robustness of system behaviour in case of network misbehaviour and overloading.

b) The feasibility and consistency of the additional testing shall be verified as part of the verification of the I&C architectural design.

6.5.5 Maintaining qualification

a) A complementary plan shall be established for maintaining the qualification during operation and maintenance of the system when replacing parts of the system with other parts which are not identical and in the case of functional modifications.

b) The complementary plan shall allow the identification of modules that carry out category A and B functions respectively, to ensure consistency with the validated versions.

NOTE This complementary plan may be treated by a specific section of the qualification plan (see 6.5.2) dealing with modifications, or a specific, separate document. It is recommended to establish this complementary plan sufficiently early. It is also recommended to establish guidance on qualification of modifications already during the initial design process, and to have it available latest during commissioning.

6.5.6 Documentation

a) Information which will be provided to the licensing authority should be listed.

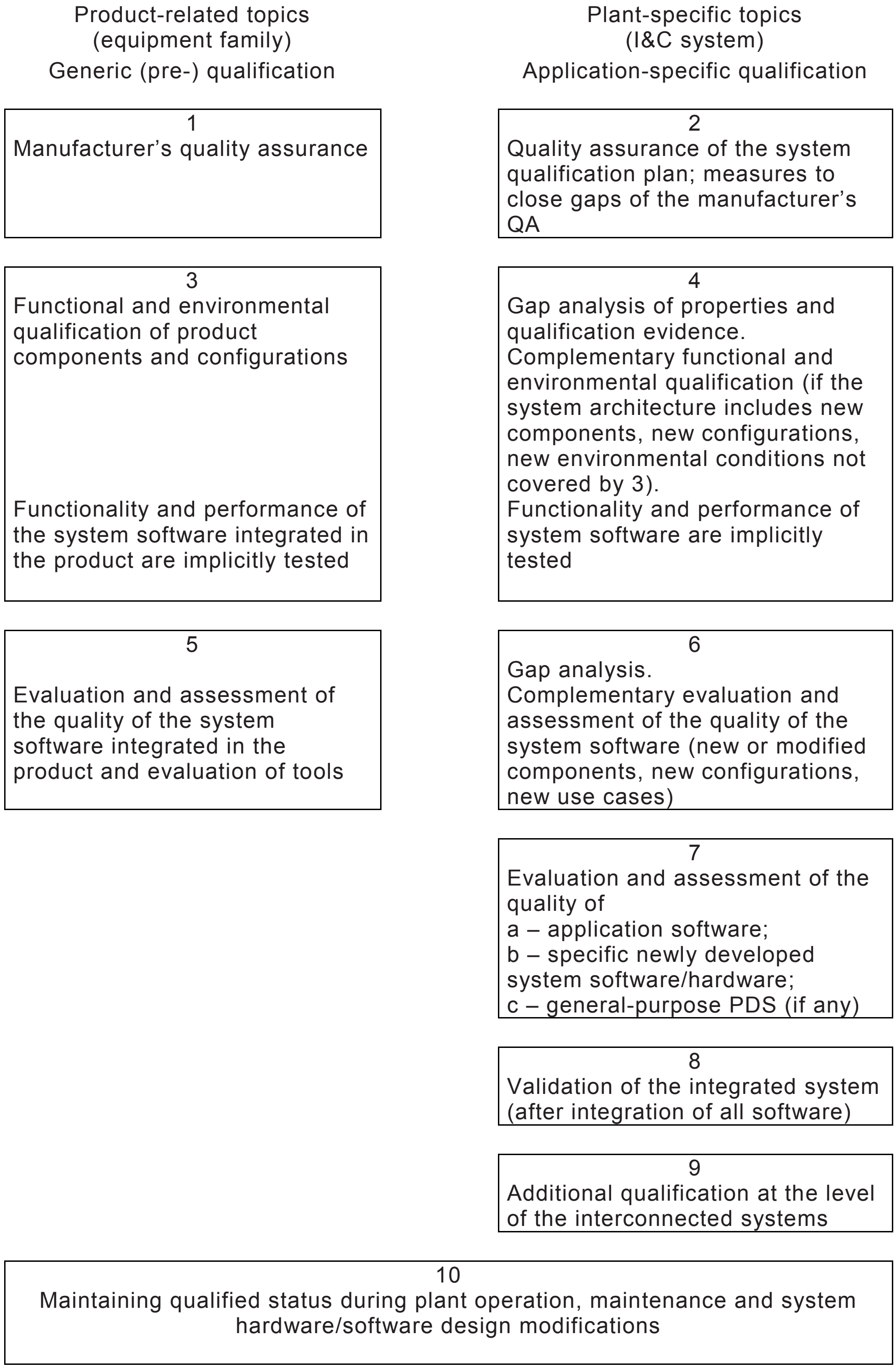
   NOTE Typically, the I&C system qualification reports for class 1 and 2 systems, and selected class 3 systems (e.g. those associated with the main or auxiliary control rooms) would be submitted to the regulator as part of the licensing process.

b) The list should distinguish between information necessary before the installation of a system and information to be provided by the licence applicant in parallel with installation and commissioning, for example test reports. Types of information that may be required include

   - descriptions (extensive representations of facts),
   - explanations (representations of facts with reasoning),
   - demonstrations,
   - justifications,
   - proofs (traceable declarations which prove assertions).

c) The documentation may be grouped according to the purpose for which it is needed but its content shall include

   - preliminary safety analysis report and summarising documents, in order to assess the conceptual and basic design of the system,
   - detailed descriptions of the whole system or parts of it, to allow independent verification and validation. This documentation may comprise detailed information about type testing of components,
   - detailed or summary explanations, demonstrations or proofs, necessary to justify design decisions and to simplify the independent verification and validation process,
   - information concerning installation, integration, commissioning, factory and site acceptance tests, in order to verify those parts of the safety life cycle which are between design and operation,
   - documentation of information necessary for operation of the system in order to verify procedures to maintain the quality of the system in the long term.



Product-related topics (equipment family)
Generic (pre-) qualification

Plant-specific topics (I&C system)
Application-specific qualification

1
Manufacturer’s quality assurance

2
Quality assurance of the system qualification plan; measures to close gaps of the manufacturer’s QA

3
Functional and environmental qualification of product components and configurations

Functionality and performance of the system software integrated in the product are implicitly tested

4
Gap analysis of properties and qualification evidence.
Complementary functional and environmental qualification (if the system architecture includes new components, new configurations, new environmental conditions not covered by 3).
Functionality and performance of system software are implicitly tested

5
Evaluation and assessment of the quality of the system software integrated in the product and evaluation of tools

6
Gap analysis.
Complementary evaluation and assessment of the quality of the system software (new or modified components, new configurations, new use cases)

7
Evaluation and assessment of the quality of
a – application software;
b – specific newly developed system software/hardware;
c – general-purpose PDS (if any)

8
Validation of the integrated system (after integration of all software)

9
Additional qualification at the level of the interconnected systems

10
Maintaining qualified status during plant operation, maintenance and system hardware/software design modifications

IEC 1900/11

Figure 6 – Product- and plant-application-specific topics to be addressed in the system qualification plan

7 Overall integration and commissioning

7.1 General

The objective of this phase is to integrate the I&C systems on site and ensure that all I&C functions important to safety perform as expected during the commissioning tests of the plant.

The commissioning plan of I&C systems is included in the commissioning programme of the plant systems (see 4.4 of IAEA 75-INSAG-3:1999).

7.2 Requirements on the objectives to be achieved

a) The activities shall be carried out in a systematic way, with a strategy developed in accordance with the system installation plans, the overall integration and commissioning plans, and the security plans defined in 5.5 and 6.3.

b) The overall integration activity should be carried out with all the related I&C systems installed and individually tested (see 6.2.7).

c) Software and data bases with parameters shall be loaded and stored values shall be justified and tested.

d) The hardware and software of the CB systems shall be under configuration management.

e) Verification and validation of all functions important to safety shall be completed before these functions are placed in service.

7.3 Output documentation

a) The I&C systems integration documentation with records of chronological evolution of on site verification and validation activities shall be available before the beginning of operation activity.

b) The report on the overall commissioning activity shall confirm that the I&C systems satisfy all expectations for intended use and functions important to safety comply with the overall requirements specifications (see 5.3).

c) Variations from the design intent that are found are assessed, corrected or referred to the operating organisation so that any effect on plant operation can be taken into account.

NOTE The exact requirements for documentation will depend on the specific operating organisation.

8 Overall operation and maintenance

8.1 General

Operation of the I&C systems may start after evaluation of commissioning reports has shown the activity was completed successfully. Operation may continue while records from operation do not require repair or modification. Operation may start again after successful repair or modification and after evaluation of the corresponding reports.

The conditions to be met before entering the operation phase should be agreed before handover from overall commissioning to the operating organisation. The following requirements are independent of this agreement:

- the systems should have completed sufficient testing to confirm that the specified functionality has been provided. Where testing has identified defects, these shall be documented and, if possible, corrected prior to handover;
- adequate user documentation and maintenance plans shall be available.

8.2 Requirements on the objectives to be achieved

The I&C systems are operated and maintained in order that the requirements for the I&C functions important to safety are maintained.

a) The plans for operation, maintenance and security defined in 5.5 and 6.3 shall be implemented.

b) Procedures to be followed by plant operators or maintenance staff in normal operation and accident conditions shall be available in the control room or nearby. Their form and content should be in accordance with international or national regulations.

c) Procedures maintenance, testing and modifications to hardware and software shall be implemented in accordance with the IEC 62138, IEC 60880 and IEC 60987.

8.3 Output documentation

Chronological documentation of operation, repair and maintenance shall be maintained. Operational records should be subject to regular review to assess for negative performance trends, and any trends which indicate unacceptable deterioration of I&C equipment should result in appropriate corrective actions.

NOTE The exact requirements for documentation will depend on the specific operating organisation.

Annex A
(informative)

Basic safety issues in the NPP

A.1 General

This annex identifies the main safety concepts that are considered in this standard for the design of NPP I&C systems. The annex provides an overview of the contents of IAEA documents but does not intend to enhance the requirements stated in these documents.

A.2 Plant safety objectives

Any industrial activity that presents risks to workers, members of the public and the environment requires the operator to take all reasonably practicable measures to keep these risks low. One typical risk of nuclear energy is the potential hazard of ionising radiation (see Clause 2 of IAEA NS-R-1:2000).

The general nuclear safety objective is to protect individuals, society and the environment by establishing and maintaining an effective defence against radiological hazard from NPPs.

The technical safety objective for existing NPPs has a “target likelihood” for the occurrence of severe core damage of below 10^{-4} events per plant operating year. Implementation of all safety principles for future plants should lead to the achievement of an improved goal of not more than 10^{-5} events per plant operating year**.** Severe accident management and mitigation measures should reduce the probability of a large off-site release requiring an off-site response by a factor of at least 10 (see 2.3 of IAEA 75-INSAG-3:1999).

A.3 Plant safety analysis

A.3.1 General

A safety analysis of the nuclear plant design is performed to establish and confirm the design basis for the items important to safety and to ensure that the overall plant design is capable of meeting the limits and reference levels for radiological doses and releases set by the regulatory authority for each plant condition category (see Clause 5 of IAEA NS-R-1:2000).

The scope of the safety analysis might include:

- the demonstration that operational limits and conditions are satisfied for the normal operation of the plant;
- characterisation of the PIEs that are appropriate for the plant design and its location;
- an analysis and evaluation of event sequences which result from PIEs;
- comparison of the results of the analysis with radiological acceptance criteria and design limits;
- establishing and confirming of the design basis;
- a demonstration that the management of anticipated operational occurrences and accident conditions is possible by response of the automatic safety systems in combination with prescribed operator actions.

This plant safety analysis process is carried out in an iterative manner from the time of initial plant conceptual design to the final plant safety assessment and it takes into account all details of the plant configuration that may have an influence on safety. The plant safety analysis takes proper account of potential human errors in operational states and under accident conditions.

The objective of this analysis is to demonstrate that the actions which are specified to be carried out by the automatic systems and the operators will result in plant behaviour which maintains radiation doses to site personnel and the public below prescribed limits for normal operating, anticipated operational occurrences and accident conditions.

A.3.2 Analysis of event sequences

The purpose of analysing an event sequence is to identify systematically and in detail all possible consequences of a PIE on the plant, including those arising from auxiliary and support systems and from possible operator error. The results of this event sequence analysis can then be used to determine if the safety requirements set down in the IAEA Code of Design have been met (see the appendices of IAEA NS-R-1:2000).

Useful analytical tools for identifying possible plant states after a PIE are event tree analysis (qualitative) and fault-tree analysis (quantitative).

It is noted that it is neither possible nor necessary to include in the safety analysis every event sequence that might occur. However, the safety analysis has to identify and consider in detail those PIEs and event sequences that produce bounding cases for safety design. In making the choice of these event sequences, experience with existing plants is taken into account.

Even with the restriction to bounding case event sequences, as described above, the rigorous application of event tree methodology will, in many practical situations, lead to the identification of many more plant configurations for each PIE than can be realistically analysed in detail. Therefore, it is usually admissible to restrict the detailed analysis to a number of representative event sequences.

A.3.3 Assessment of design basis: deterministic/probabilistic methods

Methods have been developed to assess whether safety objectives have been met (see IAEA 75-INSAG-3).

In the deterministic approach, design basis events are chosen to bound a range of related possible initiating events which could lead to a challenge to the safety of the plant.

Probabilistic analysis is used to evaluate the likelihood of any particular sequence and its consequences. This evaluation may take into account the effects of mitigation measures inside and outside the plant.

Deterministic versus probabilistic approach: The lack of sufficient data on component or system behaviour or the inability to specify a suitable mode may prevent a rigorous quantitative probabilistic approach. However, a partial probabilistic approach may often be supplemented by qualitative engineering judgement. A deterministic approach on the other hand requires engineering judgement that implicitly contains some qualitative probabilistic considerations.

In essence, current practice is to use the deterministic approach to design the systems and the probabilistic approach to optimise appropriate parts of the design and to evaluate the overall safety.

A.4 Defence in depth

A major contribution to the safety philosophy is provided by the defence-in-depth concept. This concept should be applied to all safety activities, whether organisational, behavioural or design related, to ensure that there are overlapping safety provisions so that if a failure does occur, it would be compensated for or corrected (see IAEA NS-R-1; IAEA 75-INSAG-3; IAEA INSAG-10 and IAEA-NS-G-1.3).

A first application of the concept of defence in depth to the design process is to provide independent but complementary sets of equipment and procedures in order to prevent accidents or to ensure appropriate protection in the event of prevention failing.

Examples of the multiple levels of protection:

- provision of multiple means for ensuring each of the basic safety functions, i.e. reactivity control, heat removal and the confinement of radioactivity;
- use of reliable protective devices in addition to the inherent safety features;
- supplementing of the plant control by automatic and operator actions;
- provision of equipment and procedures to mitigate accident consequences.

In general, all the lines of defence have to be available at all times as specified for the various operational modes.

- The aim of the first line of defence is to prevent deviation from normal operation. This requires that the plant be soundly and conservatively designed, constructed and operated in accordance with appropriate quality levels and engineering practices.
- The aim of the second line of defence is to detect and intercept deviations from normal operation conditions in order to prevent anticipated operational occurrences from escalating into accident conditions.
- For the third line of defence it is assumed that, although very unlikely, the escalation of certain anticipated operational occurrences may not be arrested by a preceding line of defence and so additional equipment and procedures are provided to control the consequences of the resulting accident conditions. A further major objective of this line of defence is to achieve stable and acceptable conditions following the accident.
- Beyond the third line of defence, there are further contributions to the protection of the public by complementary plant features (not claimed as important to safety) and plans for emergency preparedness, which are largely independent of reactor design.

A second application of the defence-in-depth concept is to construct and operate the NPP in such a manner that the radioactive materials are contained within a succession of physical barriers. These physical barriers are essentially passive and usually include the fuel itself, the fuel cladding, the reactor coolant system boundary, and the containment envelope. The design has to provide for the appropriate effectiveness and for the protection of each of these barriers.

A complementary application of the defence-in-depth concept is single or multiple backup of I&C systems. To minimize the magnitude of a disturbance and to achieve defence in depth, more than one I&C system may be used, which act progressively as the controlled variable deviates from the desired value. At first, as the variable deviates from normal conditions, non classified control systems take action. Following the action of these control systems, one or more levels of additional control systems important to safety may intercede, prior to the actuation of the protection system, if the event grows from a minor operational disturbance to a minor transient and to a significant transient. At each stage, the purpose is to terminate the event and return the system to normal operation for minor events and to shut down safely for events which become more serious.

Annex B
(informative)

Categorisation of functions and classification of systems

B.1 Background for the categorisation/classification scheme

IAEA NS-R-1 establishes a list of safety functions which enable the plant design to meet the general safety requirements, from the means of safely shutting down the reactor to removing the residual heat from the core, and reducing the potential for the release of radioactive material. It establishes the idea of classification of fluid-containing components necessary to perform safety functions according to their importance to safety. It introduces a methodology for ranking safety functions and for the assignment of design requirements, based on the consequence of a failure of safety function, the probability that the function would be required and the probability that the function would not be accomplished when required.

IAEA NS-G-1.3 expands the idea of classification to the instrumentation and control systems. It divides I&C systems into "systems important to safety" and "systems not important to safety". It then subdivides the systems important to safety into "safety systems" and "safety-related systems" and provides design requirements.

IEC 61226 classifies the functions important to safety into three categories: A, B and C. It provides criteria for assignment of I&C functions to categories and design requirements for the associated systems and equipment.

The number of classes defined by IAEA differs from that of IEC 61226 (safety and safety-related systems versus categories A, B and C). Furthermore, IAEA and IEC do not use identical definitions and concepts (system classification in IAEA versus categorisation of functions/classification of systems in IEC), and these discrepancies may be the source of different interpretations.

This standard follows IEC 61226 concerning the subdivision in three classes, this fits typically to the different levels of assurance of the performance required and reliability achievable when using present I&C techniques and products (e.g. developed according to nuclear standards, selected and qualified commercial off-the-shelf equipment, selected commercial off-the-shelf equipment). However, in order to avoid ambiguities in the interpretation of requirements, separate gradation schemes respectively for the functions and the systems are adopted.

The basic assumptions on categorisation/classification of this standard are developed below.

B.2 Rationale for the categorisation and classification principles adopted in this standard

B.2.1 General

Functions, systems and equipment of the NPP may be considered from two points of view (Figure B.1):

- Functional point of view

  This point of view considers only the functions to be performed. While it is recognised that sensors, processing units, interface units, etc are required to implement a function, the functional point of view does not consider that these items may be integrated into larger assemblies of equipment that also perform other functions (see "Systems point of view").

The means necessary to implement a function are called the systems and equipment associated with that function.

- Systems point of view

  This point of view considers the systems as an organised collection of equipment which implements multiple functions/subfunctions; for example, protection system, automation and control system, HMI system. The individual functions executed within a system may belong to different categories.

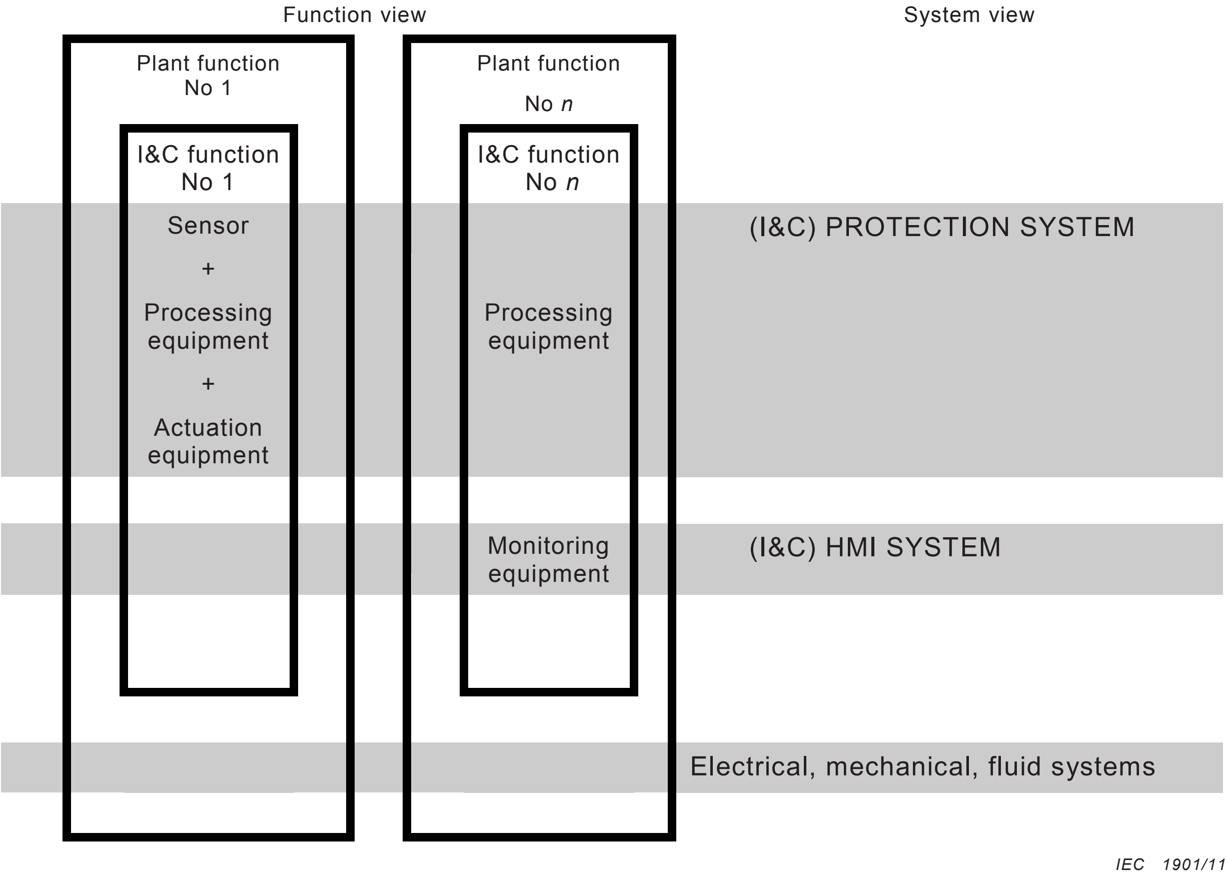


Figure B.1 – Relations between I&C functions and I&C systems

B.2.2 NPP process design phase

The NPP process designers analyse the plant and associated systems from a functional point of view. They define the plant and reactor specific PIEs and the functions important to safety needed to handle these PIEs to prevent them from developing into accident conditions. A number of independent functions (or subfunctions) may be required for each PIE according to the principle of defence in depth. The functions (or subfunctions) are assigned to categories A, B or C depending whether they play a principal, complementary, auxiliary or indirect role in the safety of the nuclear plant.

Categorisation methods are normally based on deterministic, probabilistic and risk reduction considerations. They take into account different factors such as the probability and potential severity of the consequences of PIE if the I&C system provided fails, the length of time for which the function is required once it is initiated, the timeliness and reliability with which alternative actions may be taken or any failure in the I&C system may be remedied.

The categorisation process may allow I&C functions in a safety group to be placed in different categories, for example, a diverse reactor trip may be needed to function only under the unlikely conditions of an anticipated transient combined with the failure of the primary protection function. In this case, rather than being an I&C function of category A (to be implemented in a class 1 system), it may be down-graded to category B or C.

The categories indicate the level of design requirements as well as the minimal required class of the associated systems and equipment necessary for the implementation of the function.

B.2.3 NPP I&C design phase

The NPP I&C designers analyse the I&C functions and associated systems and equipment from a systems point of view. They have the task of providing a number of I&C systems to implement the I&C functions with the level of quality and independence required by the process designers. The systems are assigned to classes depending on the achievable level of quality.

The process of classification and assignment of functions to computer based systems differs from the approach used for hard-wired technology because

- in hard-wired technology, the functions are generally implemented singly in chains of separate electronic components or relays, but CB systems allow a number of functions to be executed within the same hardware components;
- CB systems include a number of ancillary functions, for example self-supervision functions, diagnosis functions, which are not part of the plant design categorisation. These functions may need a lower level of qualification but require functional isolation;
- the choice of system architecture may be restricted in order to limit the complexity to facilitate implementation of functions of high safety category;
- there is a potential for the designer to include requirements on the architecture of the systems, for example functional separation, internal behaviour, complexity, provisions against CCF, which are not associated with the individual functions but are associated with the I&C systems and the properties of the equipment family used to implement these systems and the qualification of such systems.

This leads to the perceived need to establish a system of classification for I&C systems dependent on the function with the highest category that they execute.

B.3 Categorisation of the I&C functions important to safety

It is assumed in this standard that the plant safety design base provided by the process designers defines the categorisation of the individual I&C functions important to safety in three categories A, B, C. The categorisation requirements identify, by implication, the degree of quality of the items that are used to implement the function.

The categorisation of I&C functions is completed to the subfunctions level (see Note) so that no additional analysis at the process level is required by the I&C engineers to complete the categorisation.

NOTE A same function important to safety may be accomplished by the use of a number of subfunctions or by a unique function including all the subfunctions. This may create ambiguities when defining the requirements for the categorisation because the subfunctions may have different importance for safety and, as a consequence, different categories assigned to each of them.

In addition to the categorisation requirements, the plant safety design base defines the independence and diversity requirements of the individual functions to provide defence-in-depth. Independence is required between functions providing different lines of defence in the same safety group, between a protection function and a risk reduction function.

The independence and diversity requirements are inputs to the process of assignment of the I&C functions to the I&C systems. The I&C functions may be distributed to different I&C systems, provided that these have adequate safety classification (see Clause B.2).

B.4 Classification of the I&C systems

The I&C systems that make up the overall I&C architecture usually group together a number of I&C functions or subfunctions that perform similar tasks for the plant. The systems may normally be characterised by the functionality they provide. The number of I&C systems and their functionality is plant-specific. Typical examples of I&C systems important to safety are given below.

a) Automation and control systems

   These systems control plant or equipment parameters to

   - maintain process variables within limits assumed in the safety analysis of the plant,
   - maintain a safe operation of plant systems and equipment important to safety,
   - minimize the magnitude and rate of disturbances which are credible,
   - minimize the frequency of occurrence of events which challenge the protection system. This can be accomplished by providing high-quality, redundant diverse automation and control systems or providing more than one level of action. For example, a combination of automatic control action and manual control actions if there is sufficient time to react correctly, or two or more of the above in combination.

   Automation and control systems can affect safety because their performance, reliability, and consequences of failure form part of the design basis for the protection system. Automation and control systems may also be the principal means of accomplishing functions important to safety, for example, where an extensive period of time is available for corrective action.

   Typical functionality of these systems includes open-loop control, closed-loop control and execution of manually initiated control actions.

b) HMI systems

   These systems inform the plant operator and others of the status of the plant and its systems important to safety. They are also used to support the operator decision-making process and allow initiation of manual control actions to maintain plant safety.

   Typical functionality of these systems is to

   - convert information from sensors or signals from other systems into information suitable for display or recording on indicators, CRTs, printers, etc. The system produces information such as overviews, alarm reduction, and operation guidance,
   - display alarms, warnings and other information,
   - provide interfaces to initiate manual control.

c) Protection and safety actuation systems

   These systems ensure that specified design limits are not exceeded as a result of anticipated operational occurrences and that the consequences of accidents are contained within the design basis.

   The typical functionality of these systems is as follows:

   - sensing accident conditions and automatically initiating the operation of appropriate systems including reactor shut-down;
   - prioritising between functions of different categories (for example, override actions of the control system).

d) Emergency power actuation system

   Typical functionality:

   - load shedding;
   - load sequencing of diesel generators and other supplies.

The I&C systems implementing functions important to safety are assigned to one of three classes which conform to defined design, manufacturing and qualification requirements, which make these systems suitable for implementing functions of one or more of the categories A, B or C or unclassified (see Clause B.2). A typical classification of I&C systems is given in Table B.1.

Table B.1 – Typical classification of I&C systems

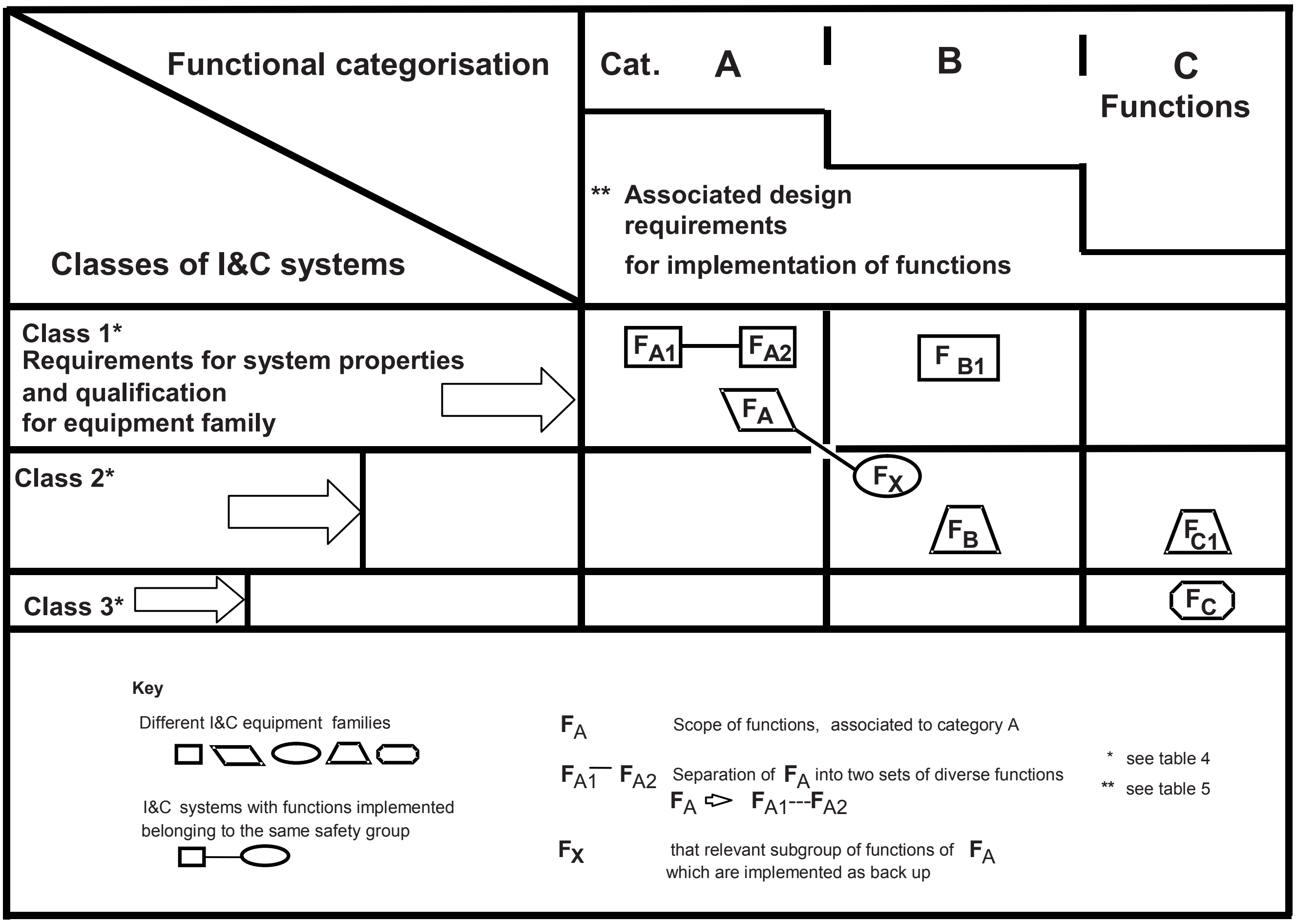
	Class 1	Class 2	Class 3	Not classified
Plant automation and control systems		x	x	x
HMI systems (class 1 HMI may be restricted to a few critical indicators and push-buttons)	x	x	x	x
Protection system and safety actuation system	x			
Emergency power actuation system	x			

The requirements of the function with the highest safety category determine the class of the system.

Annex C
(informative)

Qualitative defence approach against CCF

C.1 Example of assignment of functions of a safety group to systems


Functional categorisation
Classes of I&C systems
Cat. A
B
C
Functions
** Associated design requirements for implementation of functions
Class 1*
Requirements for system properties and qualification for equipment family
Class 2*
Class 3*
FA1
FA2
F B1
FA
FX
FB
FC1
FC
Key
Different I&C equipment families
I&C systems with functions implemented belonging to the same safety group
FA Scope of functions, associated to category A
FA1 FA2 Separation of FA into two sets of diverse functions
FA ⇨ FA1---FA2
FX that relevant subgroup of functions of FA which are implemented as back up
* see table 4
** see table 5

IEC 1902/11

Figure C.1 – Examples of assignment of functions of a safety group to I&C systems

The requirements on equipment properties and qualification, as for example, environmental and software robustness may be obtained by a suitable selected equipment family. The requirements for the systems focus on design features, as for example, the fault tolerances of the system architecture and the adequacy of the V&V design procedures adopted to ensure correct functionality.

Figure C.1 shows some examples for the assignment of the functions of a safety group to I&C systems which reflect different design strategies to meet the required reliability. The strategies are chosen based on the analysis of the effectiveness of different measures against CCF.

FA1---FA2: The scope of the safety group includes two functional diverse category A functions FA1 and FA2. The assessment of CCF analysis would need to show that for this case the application of functional diversity has given effective protection against CCF. The two functions are then implemented in independent class 1 systems based on the same equipment family.

FA---FX: The scope of the safety group includes a main category A function FA1 and an additional category B or C, FX function as a means of back-up. The CCF analysis shall show in this case that the application of equipment diversity gives sufficient protection against the CCF of concern. The FA function is assigned to one class 1 system and the Fx function is implemented in a class 2 system based on a different equipment family to give equipment diversity.

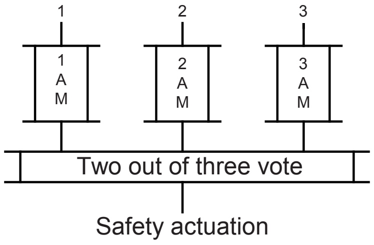
FB1---FB: The scope of the safety group includes two functional diverse category B functions FB1 and FB. The CCF analysis shall show that the application of equipment diversity and functional diversity gives sufficient protection against CCF that are of concern. The FB1 function is assigned to one class 1 system and the FB function is implemented in a class 2 system based on a different equipment family to give equipment diversity.

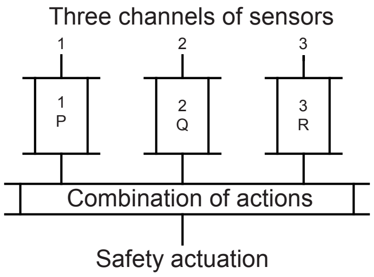
The case of FC1 and FC is similar to the previous one.

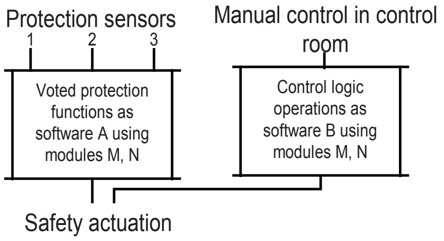
C.2 Examples of CCF sensitivity in safety groups

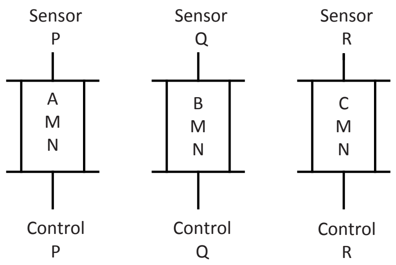
The following typical situations may exist.

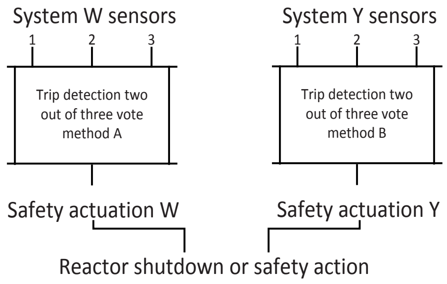
Table C.1 – Examples of CCF sensitive in safety groups

Example 1 Safety group consisting of a system with three identical redundant channels implementing a single protection function A	 1 2 3 1 A M 2 A M 3 A M Two out of three vote Safety actuation
Potential causes of CCF Potential: (H) = High; (M) = Medium; (L) = Low	**Possible defence** Effectiveness: (H) = High; (M) = Medium; (L) = Low
– An error in the requirement specification of the application function A (H)	Independent verification of the specification (M)
– A fault in the specification or development of the application software or a fault in the system software module (M). A failure may occur as a consequence of similar signal trajectories in the three channels ((L) for class 1 systems)	System development class 1 (H)
– A simultaneous failure in the hardware of the three channels due to a plant hazard	Physical, electrical independence (H)
– A failure in the 2 out of 3 voting (or other actions taken by channels)	System development class 1 (H); reliable feedback of experience (standard module) (H)

Example 2 Safety group consisting of a system with redundant channels implementing a single protection function A with common requirement specification and different software implementation (units P, Q, R)	 Three channels of sensors 1 2 3 1 P 2 Q 3 R Combination of actions Safety actuation
Potential causes of CCF Potential: (H) = High; (M) = Medium; (L) = Low	**Possible defence** Effectiveness: (H) = High; (M) = Medium; (L) = Low
– An error in the requirement specification of application function A (H)	Same as example 1
– A fault in the specification or development of the application software or a fault in the system software module (M). A failure may occur as a consequence of similar signal trajectories in the three channels (L)	System development class 1 (H) Drawback: multiple software implementation
– A simultaneous failure in the hardware of the three channels due to a plant hazard	Same as example 1
– A failure in the two out of three voting (or other actions taken by channels)	Same as example 1

Example 3 Safety group consisting of a system with two channels operating differently the same protection action* * It supposes the operator has sufficient time and information to react	 Protection sensors 1 2 3 Manual control in control room Voted protection functions as software A using modules M, N Control logic operations as software B using modules M, N Safety actuation
Potential causes of CCF Potential: (H) = High; (M) = Medium; (L) = Low	**Possible defence** Effectiveness: (H) = High; (M) = Medium; (L) = Low
– An error in the requirement specification of both functions (L)	Defence is provided by the functional diversity (automatic; manual) (H)
– A fault in the specification or development of the application software or a fault in the common system software modules M, N ((L) for asynchronous operation)	System development class 1 (H)
– A simultaneous failure in the hardware of the system channels due to a plant hazard	Same as example 1
– A failure in the two out of three voting (or other actions taken by channels)	Manual control acting downstream of voter (H)

Example 4 Safety group consisting of distributed diverse protection functions P, Q, R using different sensors and actuators and similar hardware in each control channel	
Potential causes of CCF Potential: (H) = High; (M) = Medium; (L) = Low	**Possible defence** Effectiveness: (H) = High; (M) = Medium; (L) = Low
– An error in the requirement specification of three functions (L)	Defence is provided by the functional diversity (P, Q, R) (H)
– A fault in the specification or development of the application software or a fault in the common system software modules M, N ((L) for asynchronous operation). Signal trajectories are different (L)	Fully independent hardware System development class 1 (H)
– A simultaneous failure in the hardware of the system channels due to a plant hazard	Same as example 1
– A failure in the two out of three voting (or other actions taken by channels)	Manual control acting downstream of voter (H)

Example 5 Safety group consisting of diverse protection functions W and Y distributed in two different systems (diverse hardware and system software with possible similarities, for example possible similar algorithms, similar timing, similar documentation, common staff)	
Potential causes of CCF Potential: (H) = High; (M) = Medium; (L) = Low	**Possible Defence** Effectiveness: (H) = High; (M) = Medium; (L) = Low
– An error in the requirement specification of both functions (L)	Defence is provided by the functional diversity (W, Y) (H)
– A fault in the specification or development of the application software or a fault in the common system software modules M, N ((L) for asynchronous operation) Signal trajectories are different (L) Possibility of some similar signal trajectories	Fully independent hardware System development class 1 (H)
– A simultaneous failure in the hardware of the system channels due to a plant hazard	Same as example 1
– A failure in both safety actuation actions (L)	Different (diverse) actuation systems (H)

System W sensors
1 2 3
System Y sensors
1 2 3
Trip detection two out of three vote method A
Trip detection two out of three vote method B
Safety actuation W
Safety actuation Y
Reactor shutdown or safety action

Annex D
(informative)

Relations of IEC 61508 with IEC 61513 and standards of the nuclear application sector

D.1 General

This annex compares this standard with IEC 61508-1:2010, IEC 61508-2:2010 and IEC 61508-4:2010.

Parts 3, 5, 6 and 7 of IEC 61508 are not considered because they are outside the scope of this standard. For example, the scope of Part 3 of IEC 61508, on software, is partially dealt with by IEC 60880 and IEC 62138.

This annex includes four clauses:

- Clause D.2 identifies the main differences in the scopes and concepts of the two standards
- Clause D.3 compares this standard with IEC 61508-1 (general requirements)
- Clause D.4 compares this standard with IEC 61508-2 (system aspects)
- Clause D.5 compares this standard with IEC 61508-4 (definitions)

Abbreviations

E/E/PES	Electrical/electronic/programmable electronic system
EUC	Equipment under control
SIL	Safety integrity level

D.2 Comparison of scopes and concepts

The comparison first considers some important differences in the scopes of the two standards.

The systems discussed in IEC 61508 can be of any electric, electronic or programmable electronic technology, and, although this standard includes the principles of architectural requirements for the three technologies, its main focus is on computer-based systems.

IEC 61508 refers to “safety-related systems” in general while this standard follows IAEA practice and refers to “systems important to safety” (i.e. important to nuclear safety).

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, chemical hazards, process energy hazards) international or national standards would be applied that are also based on the requirements of the basic safety standard IEC 61508.

a) Scope of the overall safety life cycle

The overall safety life cycle of IEC 61508 includes all of the systems provided by the safety design of the equipment under control including I&C systems (E/E/PE), other technology systems, and external risk reduction facilities.

This standard does not specifically discuss the plant safety analysis nor does it identify the means of assessing the adequacy of the performance and reliability requirements arising from the analysis. The nuclear sector practice is for the plant safety design to be performed according to specific IAEA principles, IEC rules and national regulations that are outside the scope of this standard. The plant design base defines the PIEs, their sequences, the defence in-depth concept of the plant, the categorisation of functions required to provide the defence. However, this standard does identify the input information required from the plant design base and safety analysis which shall be made available to the I&C developers to guide the subsequent design of the I&C systems.

b) Overall safety validation/assessment

In this standard, the overall verification and validation of each distributed function important to safety is recorded in the overall integration and commissioning report.

In the nuclear sector the assessment of the adequacy of this report with respect to safety is regulated in the framework of the licensing procedures.

c) I&C systems and I&C architecture

The I&C systems of this standard are equivalent to E/E/PE systems in IEC 61508. In this standard, the system architecture (see Clause 5) defines a number of individual systems with defined classes and independence requirements which perform the functions important to safety. For each of these individual systems, Clause 6 defines an individual safety life cycle. In IEC 61508, any splitting into multiple systems is covered in Part 2.

This difference has to be kept in mind in order to avoid misunderstandings.

d) Safety integrity level and classification

IEC 61508 grades the safety integrity level required for a CB system according to the risk reduction the system is required to provide. This is arrived at by determining the severity of the risk associated with the hazard, and assessing the frequency of the hazard and the protection to be provided by the system to reduce the risk from the hazard to a tolerable level.

The nuclear industry has traditionally used a deterministic method to determine the safety significance of a system and its impact on the severity of risk associated with possible discharge of activity (see IAEA Safety Guides and IEC 61226).

The highest practicable integrity is generally deemed necessary for any system which prevents or mitigates the consequences of radioactive releases. A lower level of integrity may be acceptable for systems which support protection against there being releases, but do not directly prevent or mitigate them. Consequently, there is not an equivalent scheme to the reliability/risk reduction SIL levels proposed in IEC 61508 in common use in the nuclear sector. This deterministic approach has been found generally sufficient in the nuclear industry and has resulted in practice in the setting of very high targets of all protective functions. However, the nuclear sector does recognise the numerical approach, and methods of probabilistic safety analysis (PSA) may provide clearer targets for the reliability of CB systems.

The assignment of safety functions to “integrity levels” of IEC 61508 is very similar to the categorisation of nuclear safety functions applied in the nuclear industry. However, there is a significant difference in the assignment procedure:

- in IEC 61508, the assignment to safety integrity levels is based on a probabilistic hazard and risk analysis;
- in IEC 61226, the assignment of nuclear safety functions to categories is based on deterministic criteria and engineering judgement about consequences in case of malfunction.

D.3 Correspondence between IEC 61508-1 and this standard

IEC 61508-1	IEC 61513
5 Documentation	5.6 Output documentation
6 Management of functional safety	5.5.2 In line with IAEA GS-R-3 and IAEA GS-G-3.1, all the activities connected to a nuclear plant are covered by a QA program or preferably an integrated management system
7 Overall safety life-cycle requirements	5 Overall I&C safety life cycle framework

IEC 61508-1	IEC 61513
7.1 General	
The overall safety life cycle encompasses the E/E/PES, other technology, external risk reduction	The overall I&C safety life cycle encompasses the I&C functions, systems and equipment important to safety and the overall architecture of I&C systems (see item a) of Clause D.2)
7.2 Concept	
Description of the EUC, its required control functions and physical environment	Review of the plant safety design base (5.2): – to identify imposed environmental conditions (5.2.4) – the I&C functions important to safety – automatic versus operator actions
Identification of sources of hazard	The internal and external hazards are defined by the safety design base of the plant and are an input for the I&C (5.2.4) (see item a) of Clause D.2)
7.3 Overall scope definition	
To determine the boundary of the EUC	To identify imposed plant/I&C boundaries (5.2.4)
To specify the scope of hazard and risk analysis and accident-initiating events	The events (PIEs) are defined by the safety design base of the plant and are an input for the I&C (5.2) (see item a) of Clause D.2)
7.4 Hazard and risk analysis	
Identification of hazard of EUC…	Outside the scope of this standard, is part of the plant design base (see item a) of Clause D.2)
… and of the EUC control system	Deterministic constraints for I&C, for example single-failure criteria for category A functions, functional isolation, are derived from the plant design base
To determine the sequence of events to hazardous events	The PIEs sequences are defined by the safety design base of the plant and are an input for the I&C (see 5.2) (see item a) of Clause D.2)
To determine the EUC risk	The categorisation of I&C functions is an input for the I&C (see 5.2.3) (see item a) of Clause D.2)
7.5 Overall safety requirements	5.3 Overall requirements specification of the I&C functions, systems and equipment
The safety functions necessary are specified. They include:	The overall requirements specifications for the I&C functions important to safety are derived from the plant design base. They include
- safety functions requirements specification	functionality and performance requirements specification (see (a) 1) and a) 2) of 5.3)
- safety integrity requirements specification	categorisation of the I&C functions (see a) 3) of 5.3) Independence requirements specification (see b) of 5.3)
The overall safety requirements specification encompasses I&C (E/E/PE systems), other technology systems and risk reduction facilities	Other technology and risk reduction measures are defined by the plant safety design base according to the principle of defence in depth. They are outside the scope of this standard (see item a) of Clause D.2)
7.6 Safety requirements allocation	5.4.2 Design of the I&C architecture 5.4.3 Functional assignment
Allocate the safety functions to the systems and allocate a safety integrity level to each function. The possibility of CCF is considered (7.6.2.7) and target safety for a single E/E/PE integrity is limited (7.6.2.11)	Decompose the overall I&C into sufficient individual I&C systems of appropriate class Allocate the I&C functions to the I&C systems according to classification, defence in depth and taking into account CCF
Overall planning	5.5 Overall planning

IEC 61508-1	IEC 61513
6 Management of functional safety	5.5.2 Overall quality assurance programs
7.8 Overall safety validation planning	5.5.4 Overall integration and commissioning plans
	5.5.3 Overall security plan
7.9 Overall installation and commissioning planning	5.5.4 Overall integration and commissioning plans
7.7 Overall operation and maintenance planning	5.5.5 Overall operation plan
	5.5.6 Overall maintenance plan
	5.5.7 Planning of training
7.10 Safety requirement specification	6.2.2 System requirements specification
7.11 Realisation: E/E/PES	6 System safety life cycle
See IEC 61508-2 (system aspects)	See Clause 6 (system safety life cycle)
See IEC 61508-3 (software requirements)	Software is outside the scope of this standard
7.12 Other risk reduction measures – Specification and realization	Outside the scope of this standard (see item a) of Clause D.2)
7.13 Overall installation and commissioning	7 Overall integration and commissioning
7.14 Overall safety validation To validate that the E/E/PE meet the overall requirements specification according to the allocation	7.2 Overall commissioning To verify and validate functions important to safety distributed in more than one system 6.5 System qualification
7.15 Overall operation, maintenance and repair	8 Overall operation and maintenance
7.16 Overall modification and retrofit	1 Scope The standard (or a subset) applies to the I&C of new NPPs as well as to up-grading or back-fitting. 6.2.8 System design modification
7.17 Decommissioning or disposal	Outside the scope of this standard
7.18 Verification	5.5.2 Overall quality assurance programs
8 Functional safety assessment To investigate and arrive at a judgement on the functional safety achieved by the E/E/PE systems	In the nuclear sector, this assessment is connected to the licensing process and depends on the safety bodies and national regulations

D.4 Correspondence between IEC 61508-2 and this standard

IEC 61508-2	IEC 61513
5 Documentation	6.4 Output documentation
6 Management of functional safety	5.5.2 Overall quality assurance programs
7 E/E/PES safety life-cycle requirements The E/E/PES safety life-cycle frame encompasses the objectives and requirements for the E/E/PES systems	6 System safety life cycle The system safety life-cycle frame encompasses the objectives and requirements for the individual I&C systems of the I&C architecture (see item c) of Clause D.2)
7.1 General Table 1 indicates, for all phases, the objectives and requirements, the scope of the phase, the required inputs to the phase, the required outputs	Table 3 indicates for all phases the objectives and requirements, the required inputs to the phase, the required outputs
7.2 E/E/PES design requirements specification It includes:	6.2.2 System requirements specification It includes:
- safety function requirements	application functions requirement specifications service functions requirements specification environmental conditions (6.2.2.6)

IEC 61508-2	IEC 61513
- safety integrity requirements	categorisation of the I&C functions (input from 5.3); system design constraints requirements (6.2.2.3) system classification
NOTE These clauses of IEC 61508 and this standard cover the same topics, but this standard makes a distinction between the requirements for the I&C functions and those for the I&C systems which implement such functions.	
7.3 E/E/PES safety validation planning	6.3 System planning
	– System validation plan (6.3.5) – Functional validation of the application functions requirements specification (6.2.4.2.1) – System qualification (6.5)
7.4 E/E/PES design and development	6.2.3 System specification 6.2.4 System detailed design and implementation
7.4.2 General requirements	– design constraints (6.2.2.3) – system architecture (6.2.2.3) – system specification documentation (6.4.3)
7.4.3 Synthesis of elements to achieve the required systematic capability	– system safety cycle (Clause 6) – design constraints requirements (6.2.2.3)
7.4.4 Hardware safety integrity architectural constraints	– design constraints requirements (6.2.2.3)
7.4.5 Requirements for quantifying the effect of random hardware failures	– reliability assessment (6.2.4.2.2)
7.4.6 Requirements for the avoidance of systematic faults	– design of the overall I&C architecture (5.4.2), so as to comply with the defence-in-depth principle – assessment of reliability and defences against CCF (5.4.4.2) – human-factors assessment (5.4.4.3) – geographical distribution of subsystems (6.2.3.3.2) – independence (6.2.3.3.3) – defence against propagation and side-effects of failures (6.2.3.3.4)
7.4.7 Requirements for the control of systematic faults	
7.4.8 Requirements for system behaviour on detection of a fault	– system architecture (6.2.2.3.2) – self-supervision and tolerance to failures (6.2.2.3.4)
7.4.9 Requirements for E/E/PES implementation	– selection of pre-existing components (6.2.3.2)
7.4.10 Requirements for proven in use elements	– selection of pre-existing components (6.2.3.2), with references to specific guidance in IEC 60880, IEC 62138, IEC 60987
7.4.11 Additional requirements for data communications	– data communication requirements (5.4.2.4), completed by IEC 61500 – internal behaviour of the system (6.2.2.3.3)
7.5 E/E/PES integration	6.2.5 System integration
7.6 E/E/PES operation and maintenance procedures	6.3.7 System operation plan
7.7 E/E/PES safety validation	6.2.6 System validation
7.8 E/E/PES modification	6.2.8 System modification
7.9 E/E/PES verification	6.3.2.2 System verification plan
8 Functional safety assessment See IEC 61508-1	See Clause D.3, last item

D.5 Correspondence between some important terms of IEC 61508-4 and the definitions of this standard and of the nuclear application sector

Topic: Risk analysis	
IEC 61508-4	**IEC 61513**
3.1.2 hazard Potential source of harm (ISO/IEC Guide 51)[19] NOTE The term includes danger to persons arising within a short-time scale (for example, fire and explosion) and also those that have a long-term effect on a person's health (for example, release of a toxic substance).	**3.25 hazard**

Topic: Defence in depth	
IEC 61508-4	**IEC 61513**
3.4.2 other risk reduction measure measure to reduce or mitigate risk that is separate and distinct from, and does not use, E/E/PE safety-related systems	**defence-in-depth concept** (see Clause A.4) The risk reduction concept is implicit in the safety analysis of the nuclear plant with the defence-in-depth concept and the lines of defence

Topic: Systems important to safety	
IEC 61508-4	**IEC 61513**
3.4.1 safety-related system Designated system that both - implements the required safety functions necessary to achieve or maintain a safe state for the EUC; and - is intended to achieve, on its own or with other E/E/PE safety-related systems, other technology safety-related systems or external risk reduction facilities, the necessary safety integrity for the required safety functions	**3.33 item important to safety**

Topic: I&C systems	
IEC 61508-4	**IEC 61513**
3.2.13 electrical/electronic/programmable electronic (E/E/PE) Based on electrical (E) and/or electronic (E) and/or programmable electronic (PE) technology	**3.29 I&C system**

Topic: Reliability	
IEC 61508-4	**IEC 61513**
3.5.4 safety integrity Probability of a safety-related system satisfactorily performing the required safety functions under all the stated conditions within a stated period of time. NOTE 3 In determining safety integrity, all causes of failures (both random hardware failures and systematic failures) which lead to an unsafe state should be included, for example hardware failures, software induced failures and failures due to electrical interference. Some of these types of failure, in particular random hardware failures, may be quantified using such measures as the failure rate in the dangerous mode of failure or the probability of a safety-related protection system failing to operate on demand. However, the safety integrity of a system also depends on many factors which cannot be accurately quantified but can only be considered qualitatively.	**3.43 reliability** In this standard, the assessment of reliability is normally qualitative (see 6.2.2.2.2) (see 6.2.2.2 and 6.2.4.2.2)

Topic: Classification of systems important to safety	
IEC 61508-4	**IEC 61513**
3.5.8 safety integrity level discrete level (one of the four possible) for specifying the safety integrity requirements of the safety functions to be allocated to the E/E/PE safety-related systems, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest	**3.6 class of an I&C system** All safety-related components, structures and systems are classified on the basis of their functions and significance with regard to safety, and they are so designed, manufactured and installed that their quality is commensurate with that classification (Clause 78 of IAEA 75-INSAG-3:1999) IEC 61226 sets a limit on the reliability that may be claimed (10^{-4}) for systems which incorporate software. For some systems, reliability targets may exceed values which can be demonstrated. If it is necessary to ensure this greater functional reliability, additional independent systems are used, each of which is capable of performing the assigned safety function. Diversity and physical separation of these systems reduce the possibility of common cause failures (reliability targets (Clauses 174-176 of IAEA 75-INSAG-3:1999)

Topic: Common cause failure	
IEC 61508-4	**IEC 61513**
3.6.10 common cause failure Failure, which is the result of one or more events, causing concurrent failures of two or more separate channels in a multiple channel system, leading to system failure. NOTE Subclauses 7.6.2.7 and 7.6.2.8 of IEC 61508-1:2010 give allocation requirements for the independence of two systems.	**3.8 common cause failure** See 5.4.2.6

Annex E
(informative)

Changes to be performed in later revisions of SC 45A standards to adapt to this version of IEC 61513

IEC 60880:2006	Change to be performed
3 Terms and definitions	The definitions need to be aligned
6.3 Testing	Delete all except 6.3.1 and 6.3.2. Now covered by 6.2.2.3.5 of IEC 61513
9.3 Integrated system verification	Delete the subclause. It is covered by 6.2.5 and 6.3.4 of IEC 61513
9.4 Resolution procedure	Delete the subclause. It is covered by 6.3.2.4 of IEC 61513
9.5 Software aspects of integrated system verification report	Delete the subclause. It is covered by 6.4.5 of IEC 61513
10.1 Software aspects of the system validation plan	Delete the subclause. It is covered by 6.2.6 and 6.3.5 of IEC 61513
10.3 Software aspects of system validation report	Delete the subclause. It is covered by 6.4.6 of IEC 61513
10.4 Fault resolution procedure	Delete the subclause. It is covered by 6.3.2.4 of IEC 61513
12.4 Operator training	Delete the subclause. It is covered by 5.5.7 of IEC 61513

IEC 62138:2004	Change to be performed
3 Terms and definitions	The definitions need to be aligned
5.6 and 6.6 Software aspects of system integration	Consider deletion of the subclause. It is covered by 6.2.5 and 6.3.4 of IEC 61513
5.7 and 6.7 Software aspects of system validation	Consider deletion. It is covered by 6.2.6 and 6.3.5 of IEC 61513

IEC 61226:2009	Change to be performed
3 Terms and definitions	The definitions need to be aligned
New annex	Take over the contents of Annex B

Bibliography

[1] IEC 61508-1:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements*

[2] IEC 61508-3:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements*

[3] IAEA Safety Glossary – *Terminology used in Nuclear Energy and Radiation Protection – 2007 Edition*

[4] IEEE 610:1992, *IEEE standard Computer Dictionary, Compilation of IEEE Standard Computer Glossaries*

[5] IEC 61069-1:1991, *Industrial-process measurement and control – Evaluation of system properties for the purpose of system assessment – Part 1: General considerations and methodology*

[6] ISO 9000:2005, *Quality management systems – Fundamentals and vocabulary*

[7] ISO 8402:1994, *Quality management and quality assurance – Vocabulary*

[8] ISO/IEC Directives, Part 2, 2004, Part 2: *Rules for the structure and drafting of International Standards*

[9] ISO/IEC 12207:2008, *Systems and software engineering – Software life cycle processes*

[10] IEC 60050-394:2007, *International Electrotechnical Vocabulary – Part 394: Nuclear instrumentation – Instruments, systems, equipment and detectors*

[11] IEC 62381, *Automation systems in the process industry – Factory acceptance test (FAT), Site acceptance test (SAT), and Site integration test (SIT)*

[12] IEC 62342, *Nuclear power plants – Instrumentation and control systems important to safety – Management of ageing*

[13] IEC 61000-6-2, *Electromagnetic compatibility (EMC) – Part 6-2: Generic Standards – Immunity for industrial environments*

[14] IEC 61000-6-4, *Electromagnetic compatibility (EMC) – Part 6-4: Generic Standards – Emission standard for industrial environments*

[15] IEC 62003:2009, *Nuclear power plants – Instrumentation and control important to safety – Requirements for electromagnetic compatibility testing*

[16] IEC 61225, *Nuclear power plants – Instrumentation and control systems important to safety – Requirements for electrical supplies*

[17] ISO 10007, *Quality management systems – Guidelines for configuration management*

[18] IEEE 828, *IEEE Standard for Software Configuration Management Plans*

[19] ISO/IEC Guide 51:1990, *Guidelines for the inclusion of safety aspects in standards*

____

This page deliberately left blank

This page deliberately left blank

British Standards Institution (BSI)

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

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

About us

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

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

Information on standards

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

Buying standards

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

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

Subscriptions

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

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

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

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

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

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

Revisions

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

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

Copyright

All the data, software and documentation set out in all British Standards and other BSI publications are the property of and copyrighted by BSI, or some person or entity that owns copyright in the information used (such as the international standardization bodies) and has formally licensed such information to BSI for commercial publication and use. Except as permitted under the Copyright, Designs and Patents Act 1988 no extract may be reproduced, stored in a retrieval system or transmitted in any form or by any means – electronic, photocopying, recording or otherwise – without prior written permission from BSI. Details and advice can be obtained from the Copyright & Licensing Department.

Useful Contacts:

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

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

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

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

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

bsi.

...making excellence a habit.™