

INTERNATIONAL STANDARD

NORME INTERNATIONALE

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

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



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2011 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester.

If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de la CEI ou du Comité national de la CEI du pays du demandeur.

Si vous avez des questions sur le copyright de la CEI ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de la CEI de votre pays de résidence.

IEC Central Office
3, rue de Varembe
CH-1211 Geneva 20
Switzerland
Email: inmail@iec.ch
Web: www.iec.ch

About the IEC

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

About IEC publications

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

- Catalogue of IEC publications: www.iec.ch/searchpub

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 It also gives information on projects, withdrawn and replaced publications.

- IEC Just Published: www.iec.ch/online_news/justpub

Stay up to date on all new IEC publications. Just Published details twice a month all new publications released. Available on-line and also by email.

- Electropedia: www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 20 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary online.

- Customer Service Centre: www.iec.ch/webstore/custserv

If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:

Email: csc@iec.ch

Tel.: +41 22 919 02 11

Fax: +41 22 919 03 00

A propos de la CEI

La Commission Electrotechnique Internationale (CEI) est la première organisation mondiale qui élabore et publie des normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications CEI

Le contenu technique des publications de la CEI est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

- Catalogue des publications de la CEI: www.iec.ch/searchpub/cur_fut-f.htm

Le Catalogue en-ligne de la CEI vous permet d'effectuer des recherches en utilisant différents critères (numéro de référence, texte, comité d'études,...). Il donne aussi des informations sur les projets et les publications retirées ou remplacées.

- Just Published CEI: www.iec.ch/online_news/justpub

Restez informé sur les nouvelles publications de la CEI. Just Published détaille deux fois par mois les nouvelles publications parues. Disponible en-ligne et aussi par email.

- Electropedia: www.electropedia.org

Le premier dictionnaire en ligne au monde de termes électroniques et électriques. Il contient plus de 20 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans les langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International en ligne.

- Service Clients: www.iec.ch/webstore/custserv/custserv_entry-f.htm

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions, visitez le FAQ du Service clients ou contactez-nous:

Email: csc@iec.ch

Tél.: +41 22 919 02 11

Fax: +41 22 919 03 00



IEC 61513

Edition 2.0 2011-08

INTERNATIONAL STANDARD

NORME INTERNATIONALE

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

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

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

PRICE CODE
CODE PRIX

XD

ICS 27.120.20

ISBN 978-2-88912-663-7

CONTENTS

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

6.3	System planning.....	59
6.3.1	General	59
6.3.2	System quality assurance plan	60
6.3.3	System security plan	62
6.3.4	System integration plan	62
6.3.5	System validation plan.....	63
6.3.6	System installation plan.....	63
6.3.7	System operation plan	64
6.3.8	System maintenance plan.....	64
6.4	Output documentation	65
6.4.1	General	65
6.4.2	System requirements specification documentation.....	65
6.4.3	System specification documentation	66
6.4.4	System detailed design documentation	67
6.4.5	System integration documentation	68
6.4.6	System validation documentation.....	69
6.4.7	System modification documentation.....	69
6.5	System qualification	70
6.5.1	General	70
6.5.2	Generic and application-specific qualification	70
6.5.3	Qualification plan.....	71
6.5.4	Additional qualification of interconnected systems	72
6.5.5	Maintaining qualification	73
6.5.6	Documentation	73
7	Overall integration and commissioning	74
7.1	General.....	74
7.2	Requirements on the objectives to be achieved	75
7.3	Output documentation	75
8	Overall operation and maintenance	75
8.1	General.....	75
8.2	Requirements on the objectives to be achieved	75
8.3	Output documentation	76
Annex A (informative)	Basic safety issues in the NPP	77
Annex B (informative)	Categorisation of functions and classification of systems	80
Annex C (informative)	Qualitative defence approach against CCF.....	85
Annex D (informative)	Relations of IEC 61508 with IEC 61513 and standards of the nuclear application sector	89
Annex E (informative)	Changes to be performed in later revisions of SC 45A standards to adapt to this version of IEC 61513	96
Bibliography.....		98
Figure 1 – Overall framework of this standard.....		11
Figure 2 – Typical relations of hardware and software in a computer-based system		25
Figure 3 – Relations between system failure, random failure and systematic fault.....		25
Figure 4 – Connections between the overall I&C safety life cycle and the safety life cycles of the individual I&C systems		29
Figure 5 – System safety life cycle.....		46

Figure 6 – Product- and plant-application-specific topics to be addressed in the system qualification plan.....	74
Figure B.1 – Relations between I&C functions and I&C systems	81
Figure C.1 – Examples of assignment of functions of a safety group to I&C systems	85
Table 1 – Overview of the overall I&C safety life cycle	27
Table 2 – Correlation between classes of I&C systems and categories of I&C functions.....	33
Table 3 – Overview of the system safety life cycle	44
Table B.1 – Typical classification of I&C systems.....	84
Table C.1 – Examples of CCF sensitive in safety groups	86

INTERNATIONAL ELECTROTECHNICAL COMMISSION

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

FOREWORD

- 1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
- 2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
- 3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
- 4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
- 5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
- 6) All users should ensure that they have the latest edition of this publication.
- 7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
- 8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
- 9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

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

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

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

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

- to integrate requirements for staff training.

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

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

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

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

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

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

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):

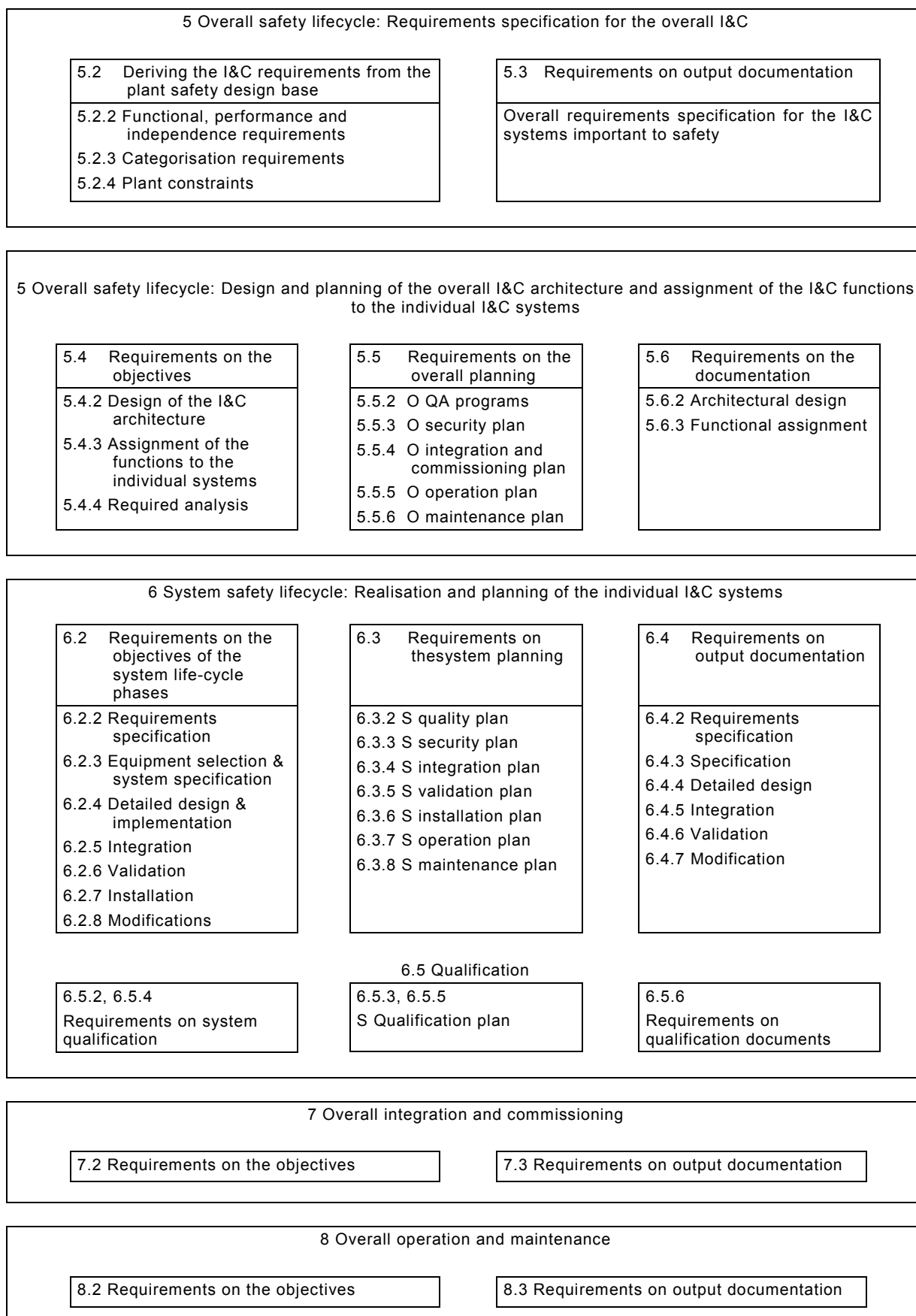
- Clause 5 addresses the overall architecture of the I&C systems important to safety:
 - defining requirements for the I&C functions, and associated systems and equipment derived from the safety analysis of the NPP, the categorisation of I&C functions, and the plant lay-out and operational context;
 - 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.



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.

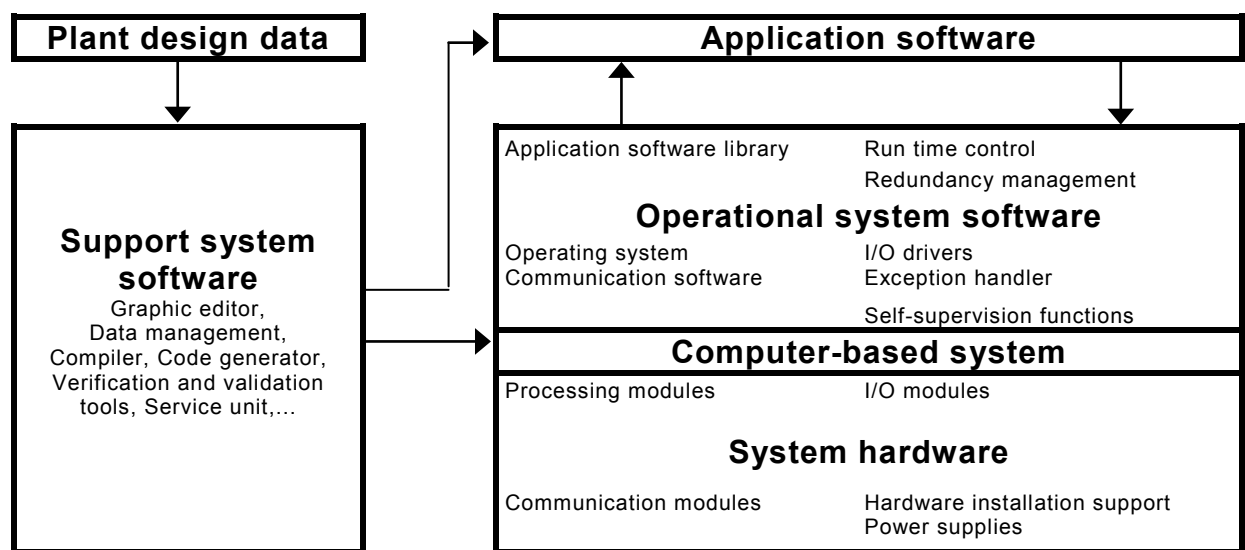
The IAEA definition of “verification” is very similar to the IAEA one of « validation », as both address the final product or service.

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:

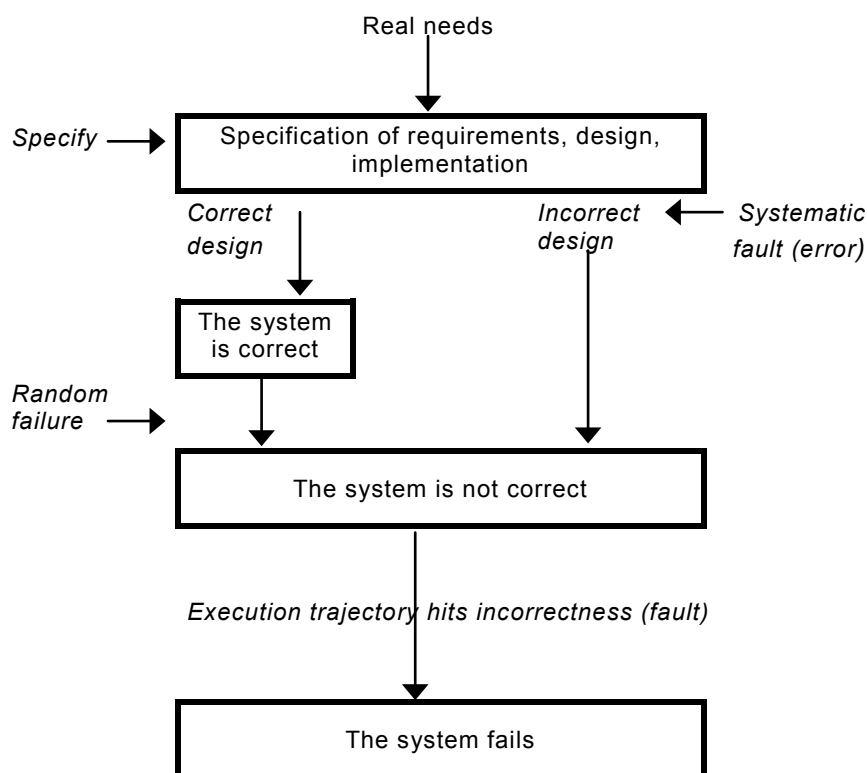
“*Verification*” indicates the assessment of the results of an individual activity against its inputs.

“*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



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.

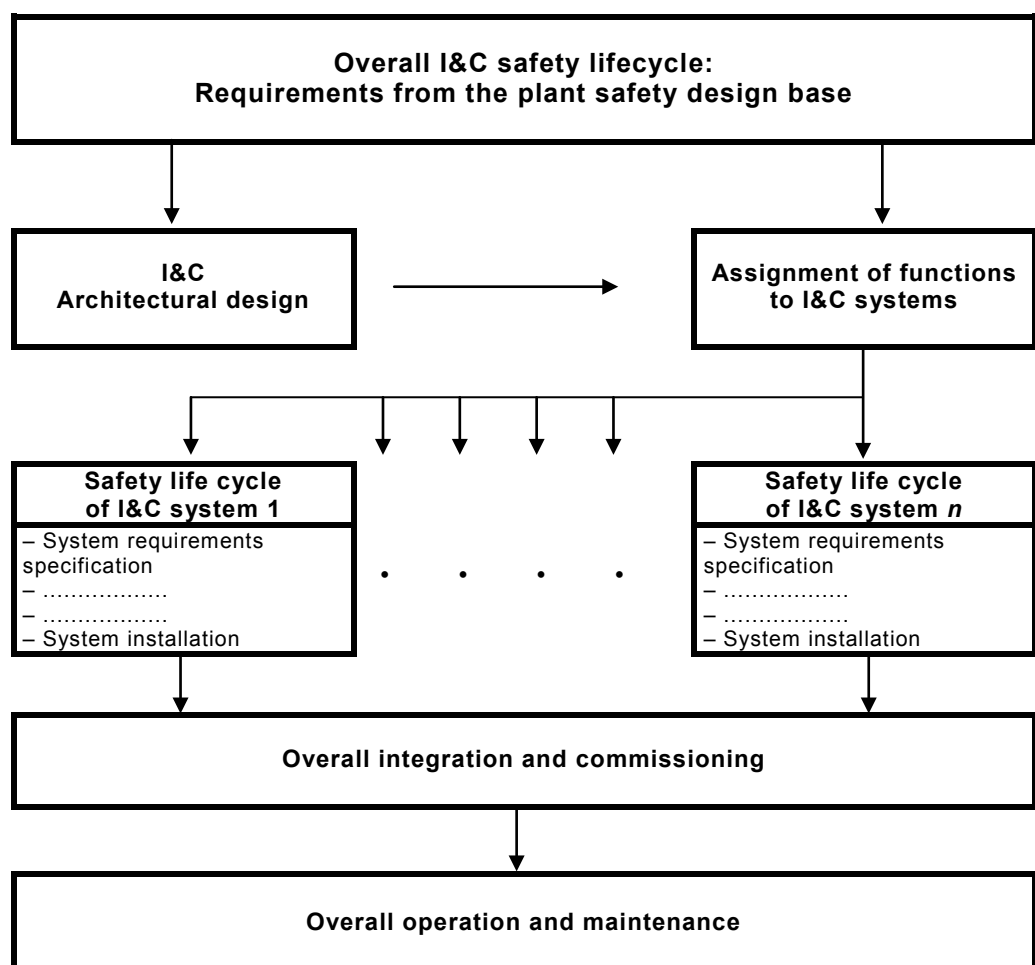
The connections between this life cycle and the safety life cycles of the individual I&C systems are shown in simplified form in Figure 4.

- 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.				



IEC 1898/11

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

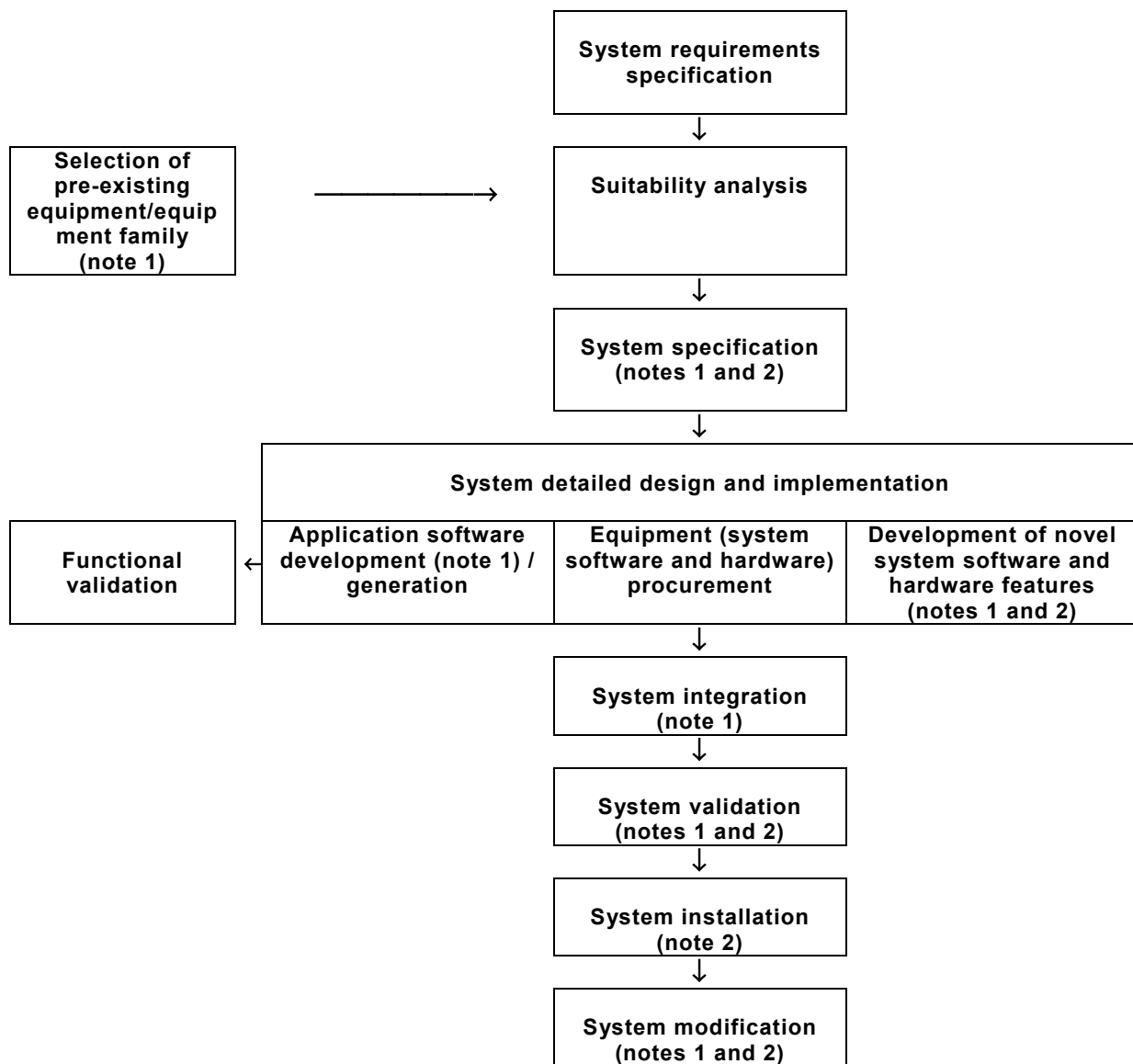
- generic requirements to be applied equally for all systems important to safety,
- requirements to be applied, in addition to the previous ones, to specific classes of systems or categories of functions.

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.			



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.