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

IEC Central Office
3, rue de Varembé
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 It also gives information on projects, withdrawn and replaced publications.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

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);

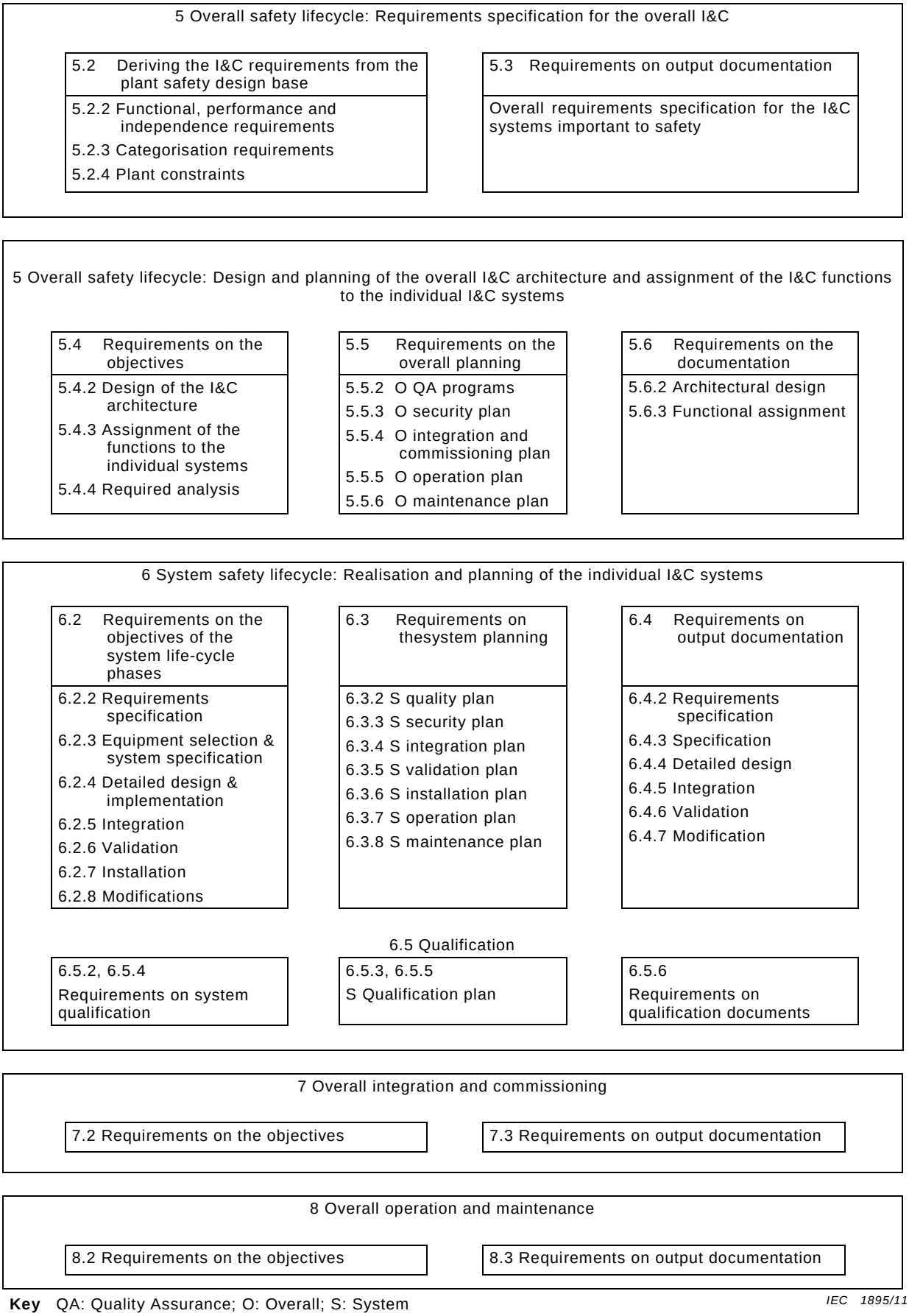
– planning the overall architecture of the I&C systems.

- 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.

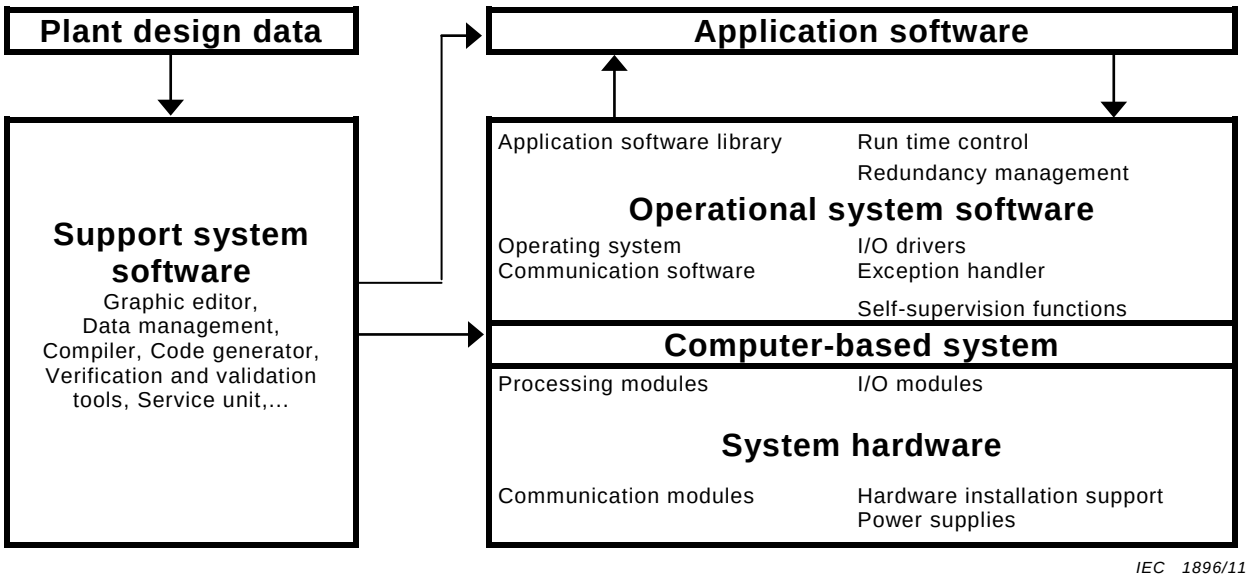


Figure 2 – Typical relations of hardware and software in a computer-based system

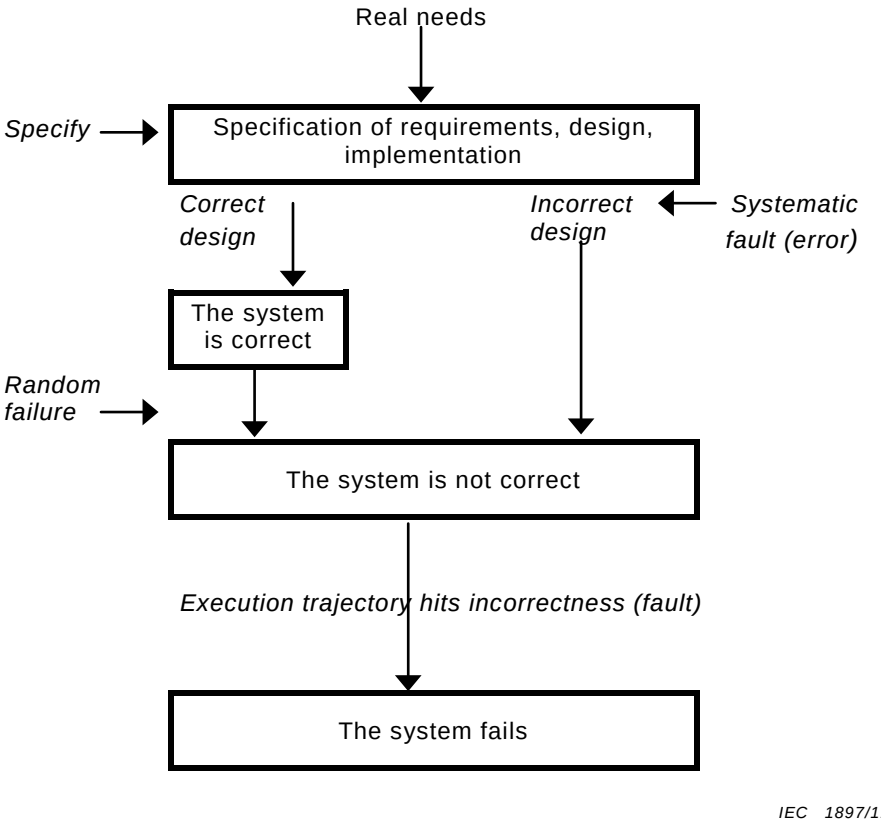


Figure 3 – Relations between system failure, random failure and systematic fault

4 Symbols and abbreviations

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

5 Overall I&C safety life cycle

5.1 General

The objective of this clause is to define how to

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

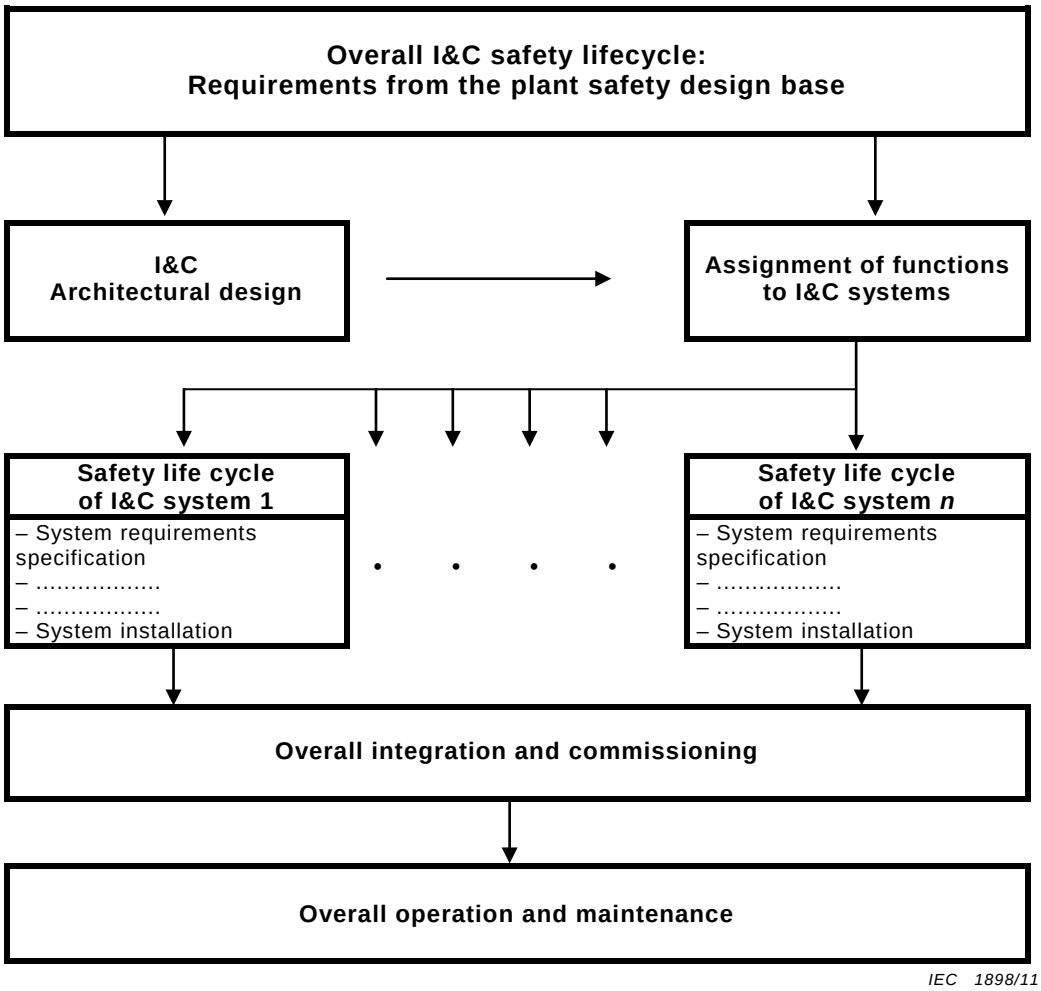


Figure 4 – Connections between the overall I&C safety life cycle and the safety life cycles of the individual I&C systems

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

5.2.1 General

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

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

5.2.2 Review of the functional, performance and independence requirements

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

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

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

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

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

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

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

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

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

5.2.3 Review of the categorisation requirements

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

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

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

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

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

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

requirements for category A are consistent with the requirements for safety systems of the IAEA.

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

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

5.2.3.2 Requirements

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

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

5.2.4 Review of plant constraints

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

a) The I&C project organisation shall identify the constraints placed on I&C equipment by the plant layout, the interfaces with plant equipment, and the events outside the I&C, including

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

b) The I&C project organisation shall identify the constraints placed on I&C equipment by the utility's principles of operation, i.e. constraints from

- security;
- operation and maintenance (see 5.6 of IEC 60964:2009);
- "in-service maintenance" of the I&C systems.

Typically, this will lead to additional requirements guiding the subdivision of the I&C architecture in separate sub-systems. Areas to be considered include:

- the plant is typically subdivided in distinct plant systems, which are grouped in lots so as to organize engineering, installation, start-up and testing activities. The subdivision of the I&C systems should take into account this boundary condition;

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

5.3 Output documentation

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

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

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

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

   3) specification of the category of the function.

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

b) The overall requirements specification shall define any dependency between functions which generate constraints on the assignment of functions to the I&C systems. This includes:
   1) the combinations of functions to be monitored to control protective actions;
   2) the combination of functions ensuring defence in depth;
   3) the combination of functions which constitute a safety group.

c) The requirements specifications of all the I&C functions shall be verified to ensure that a complete and consistent set of functions and constraints are defined for the purpose of assignment of functions to systems and the production of the specification of those systems (see 6.2).

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

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

5.4.1 General

This subclause describes how the

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

5.4.2 Design of the I&C architecture

5.4.2.1 General

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

5.4.2.2 General requirements

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

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

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

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

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

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

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

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

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

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

5.4.2.3 Human machine interfaces

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

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

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

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

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

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

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

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

e) The design of the I&C architecture shall

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

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

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

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

5.4.2.4 Data communication

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

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

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

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

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

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

See IEC 61500 and 60709 for details.

5.4.2.5 Tools

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

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

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

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

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

5.4.2.6 Defence against CCF

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

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

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

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

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

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

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

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

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

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

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

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

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

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

5.4.3 Assignment of functions to systems

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

5.4.4 Required analysis

5.4.4.1 General

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

5.4.4.2 Assessment of reliability and defences against CCF

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

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

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

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

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

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

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

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

5.4.4.3 Human factors assessment

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

5.5 Overall planning

5.5.1 General

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

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

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

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

5.5.2 Overall quality assurance programs

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

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

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

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

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

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

5.5.3 Overall security plan

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

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

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

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

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

a) The security requirements of functions and systems important to safety shall be identified in the system security plan (see 6.3.3).

b) The risk arising from unauthorised access and modification shall be managed in a systematic manner during all phases of the life cycle from inception to disposal. This includes the development and engineering systems as well as the I&C systems to be installed in the plant. Physical access as well as remote access shall be considered.

c) The security provisions for a system shall be such that they do not have a significant impact on its reliability or availability.

d) To maintain security of systems at a continuously high level a site-specific security policy shall be established. It shall contain procedures related to the interface between administrative and technical security, access to systems, security aspects of data handling, security aspects of modification and maintenance, security auditing and reporting, and security training.

e) Systems performing functions important to safety shall be physically protected against unauthorised access (see 4.51 of IAEA NS-G-1.3:2002). Access control shall include identification and authentication of personnel for systems performing category A functions and reliable identification of personnel for systems performing category B and C functions.

f) Features for remote (external to the plant) access shall not be implemented for systems performing category A and B functions, and should not be implemented for systems performing category C functions. If access features via data links (internal or external to the plant) are provided, they shall be analysed and it shall be demonstrated that they do not introduce unacceptable risk of unauthorised system access or unacceptable risk of system failure.

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

g) Access to systems (including attempts to access) should be logged. This comprises recording the personnel, the type of access, the time, and the actions carried out.

h) Security logs shall be formally inspected at defined intervals for systems performing category A functions and should be checked periodically for systems performing category B and C functions.

5.5.4 Overall I&C integration and commissioning

5.5.4.1 General

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

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

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

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

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

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

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

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

5.5.4.2 Overall I&C integration plan

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

a) Testing of interconnected systems shall be performed to confirm that

- all interfaces of interconnected systems operate correctly,
- failure detection, corrective actions and the display of associated data are operating in accordance with the requirements specification of the I&C functions.

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

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

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

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

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

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

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

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

i) Data communication shall be tested for correct data transmission and acceptable response time, from issuing of commands to the receipt of a correct indication of actuator

state. Tests should be performed under simulation of normal operating conditions, relevant accident conditions, worst-case conditions, and in the presence of simulated hardware failures.

5.5.4.3 Overall commissioning plan

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

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

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

5.5.5 Overall operation plan

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

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

a) The plan shall describe

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

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

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

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

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

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

5.5.6 Overall maintenance plan

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

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

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

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

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

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

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

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

5.5.7 Planning of training

5.5.7.1 Training programme

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

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

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

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

1) an analysis of the tasks of the involved staff categories, and establish training objectives, an overall schedule and overall definition of training courses,

2) availability of qualified trainers, and comprise training material for trainers and trainees,

3) an evaluation of the training undertaken,

4) enhanced use of feedback for the improvement of the training.

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

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

5.5.7.2 User documentation

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

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

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

5.5.7.3 Training systems

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

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

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

5.6 Output documentation

5.6.1 General

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

5.6.2 Architectural design documentation

a) The output documentation shall define for the individual I&C systems

- the design constraints derived from the plant design framework (see 5.2.4);
- the design constraints from the architectural design (see 5.4.2);
- the physical and functional boundaries between systems.

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

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

5.6.3 Functional assignment documentation

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

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

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

6 System safety life cycle

6.1 General

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

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

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

The phases of the typical system safety life cycle include:

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

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

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

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

This clause includes

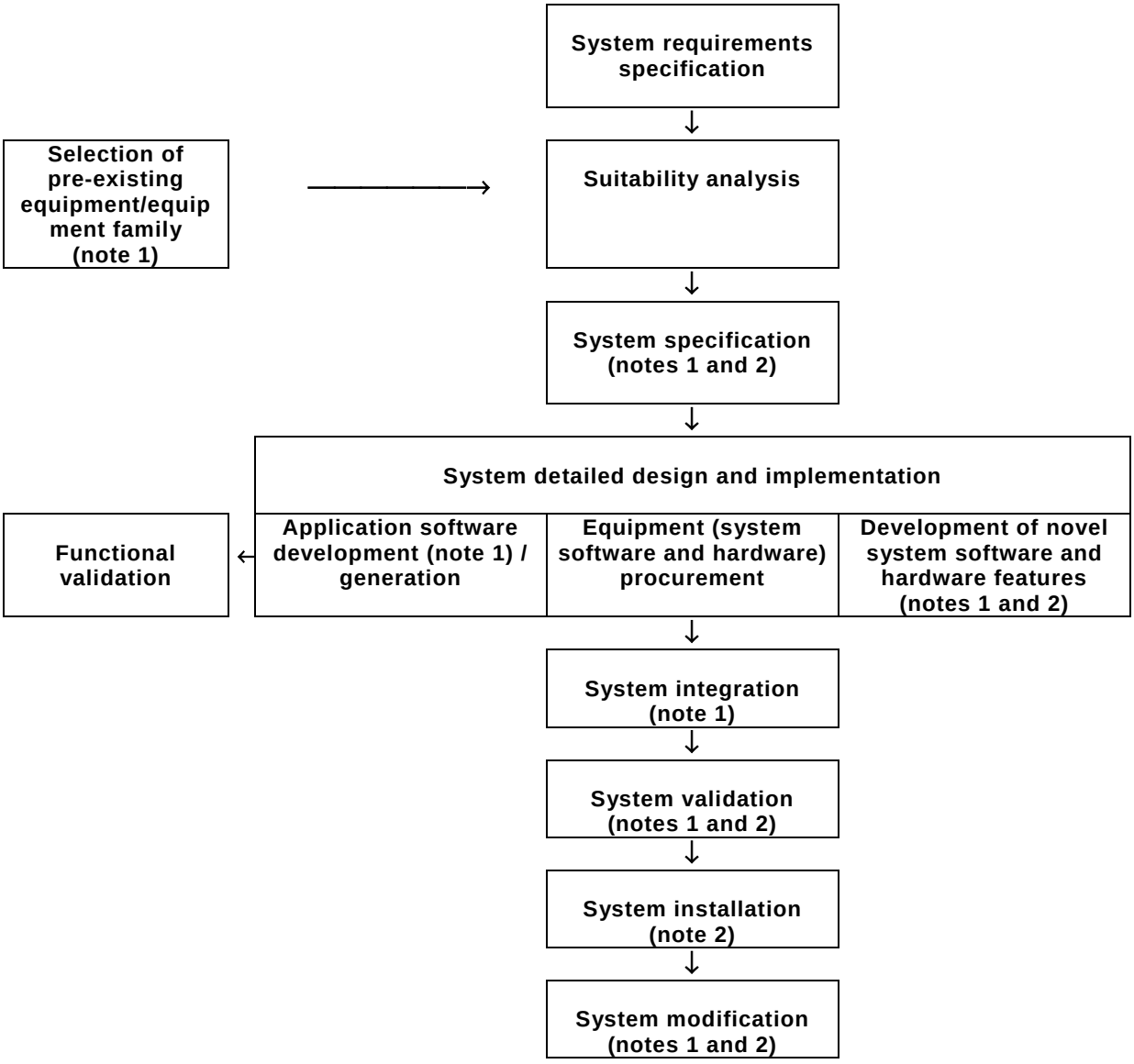
- generic requirements to be applied equally for all systems important to safety,
- requirements to be applied, in addition to the previous ones, to specific classes of systems or categories of functions.

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

Table 3 – Overview of the system safety life cycle

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

Clause or subclause	Inputs	Objectives of the activity	Outputs
		– the design constraints – the boundaries and interfaces with other systems and tools, – the interfaces with persons, – the environmental conditions	
6.2.3 System specification	Outputs of 6.2.2 Documen-tation 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.			



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

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

Figure 5 – System safety life cycle

6.2 Requirements

6.2.1 General

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

These requirements encompass features related to

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

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

6.2.2 System requirements specification

6.2.2.1 General

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

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

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

The system requirements specification shall indicate

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

6.2.2.2 Functions

6.2.2.2.1 General

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

6.2.2.2.2 Application functions

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

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

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

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

6.2.2.2.3 Service functions

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

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

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

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

6.2.2.3 Design constraints

6.2.2.3.1 General

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

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

6.2.2.3.2 System architecture

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

a) The system may implement functions of the highest category allowed for its class (see 5.4.3) and functions of lower categories. The system may include subsystems of lower classes provided that the following requirements are fulfilled:

   1) the design requirements for each subsystem shall not be lower than those required by the function of the highest category implemented by the subsystem;

   2) the design of the system shall ensure that the requirements of the subsystems or equipment of the higher classes are satisfied in case of failure of the equipment of the lower class.

b) The design of the system shall include redundancy and other features necessary to provide tolerance to failure (see 6.2.3.3.4) and to accommodate the assignment of the application functions important to safety (see 6.2.3.5).

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

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

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

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

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

6.2.2.3.3 Internal behaviour of the system

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

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

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

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

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

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

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

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

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

6.2.2.3.4 Self-supervision and tolerance to failures

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

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

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

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

6.2.2.3.5 Testability

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

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

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

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

c) testing and calibration of sensors;

d) testing of output actuation.

b) The principles of IEC 60671 shall be applied.

6.2.2.3.6 Maintainability

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

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

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

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

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

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

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

6.2.2.4 Boundaries and interfaces with other systems and tools

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

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

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

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

6.2.2.5 Interfaces with users

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

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

6.2.2.6 Environmental conditions

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

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

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

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

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

6.2.2.7 Qualification

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

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

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

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

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

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

6.2.3 System specification

6.2.3.1 General

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

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

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

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

The system specification shall define

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

6.2.3.2 Selection of pre-existing components

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

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

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

a) The suitability of the candidate components shall be evaluated and assessed to demonstrate that their characteristics comply with the system requirement specifications.

b) The suitability evaluation and assessment of the candidate components should be based on the comparison of two sets of documents: the requirements specifications of the system and the documentation related to the pre-existing components. The latter includes the product specifications, and (if available) pre-qualification documentation.

c) The following requirements apply:

   - it shall be analysed whether the documentation supplied defines explicitly the functionality and properties of all components;

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

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

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

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

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

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

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

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

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

6.2.3.3 System architecture

6.2.3.3.1 General

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

The arrangement of system subsystems shall

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

6.2.3.3.2 Geographical distribution of subsystems (centralised/decentralised)

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

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

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

6.2.3.3.3 Independence

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

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

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

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

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

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

6.2.3.3.4 Defence against propagation and side-effects of failures

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

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

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

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

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

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

6.2.3.4 Software specification

The software specification includes:

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

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

- specification of the service functions and system software functions.

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

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

6.2.3.5 Assignment of the application functions in the system

This includes assignment of

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

The following requirements apply:

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

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

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

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

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

6.2.4 System detailed design and implementation

6.2.4.1 General

The objective of this phase is

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

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

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

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

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

The outputs of this phase are

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

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

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

6.2.4.2 Required analysis

6.2.4.2.1 Functional validation of the application functions requirements specification

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

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

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

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

6.2.4.2.2 Reliability assessment

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

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

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

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

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

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

6.2.5 System integration

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

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

System integration consists of the following steps:

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

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

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

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

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

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

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

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

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

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

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

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

6.2.6 System validation

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

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

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

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

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

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

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

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

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

e) For category C functions:

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

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

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

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

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

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

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

b) This report shall also identify any discrepancies.

6.2.7 System installation

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

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

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

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

6.2.8 System design modification

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

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

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

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

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

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

6.3 System planning

6.3.1 General

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

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

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

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

6.3.2 System quality assurance plan

6.3.2.1 General

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

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

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

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

d) The system quality assurance plan shall include:

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

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

6.3.2.2 System verification plan

a) A system verification plan shall be developed describing

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

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

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

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

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

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

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

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

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

6.3.2.3 System configuration management plan

a) Configuration identification:

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

b) Configuration control:

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

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

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

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

6.3.2.4 Fault resolution procedures

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

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

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

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

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

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

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

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

6.3.3 System security plan

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

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

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

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

6.3.4 System integration plan

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

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

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

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

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

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

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

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

6.3.5 System validation plan

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

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

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

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

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

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

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

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

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

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

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

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

6.3.6 System installation plan

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

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

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

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

6.3.7 System operation plan

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

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

b) The system operation plan should specify the conditions to be met before the system is put into operation. In particular:

- the system shall have completed installation, integration and commissioning (see 5.5.4);
- the system maintenance plan (see 6.3.8) and user documentation shall be available.

c) When periodic testing is required (see 6.2.2.3.5), the system operation plan shall specify

- the frequency and duration of each test, the conditions to be met prior to the initiation of a test and the effects, if any, on the operation of the system and of the plant;
- the steps necessary to perform each test, the tools and tool calibrations to be used, the analysis of the correctness of results;
- the verification of complete restoration to normal state, if temporary changes in the system are required.

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

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

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

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

6.3.8 System maintenance plan

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

a) A system maintenance plan shall be developed and it shall specify

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

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

c) The procedures for replacement of components shall ensure that

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

d) The procedures for re-calibration shall ensure that

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

6.4 Output documentation

6.4.1 General

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

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

6.4.2 System requirements specification documentation

6.4.2.1 Content

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

6.4.2.2 Characteristics

Characteristics of the system requirements specification document:

a) the requirements shall be unambiguous and verifiable;

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

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

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

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

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

6.4.2.3 Verification

The following points shall be verified:

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

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

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

6.4.3 System specification documentation

6.4.3.1 Content

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

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

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

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

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

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

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

6.4.3.2 Characteristics

Characteristics of the system specification documentation:

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

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

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

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

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

6.4.3.3 Verification

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

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

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

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

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

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

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

6.4.4 System detailed design documentation

6.4.4.1 General

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

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

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

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

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

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

6.4.4.2 Content

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

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

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

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

6.4.4.3 Characteristics

Characteristics of the system design documentation:

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

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

6.4.4.4 Verification

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

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

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

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

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

6.4.5 System integration documentation

6.4.5.1 Content

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

6.4.5.2 Characteristics

Integration test reports shall contain the following information:

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

6.4.5.3 Verification

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

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

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

6.4.6 System validation documentation

6.4.6.1 Content

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

6.4.6.2 Characteristics

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

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

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

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

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

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

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

6.4.6.3 Verification

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

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

6.4.7 System modification documentation

6.4.7.1 Content

a) Modification request

This document shall state

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

b) Modification package

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

6.4.7.2 Characteristics

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

6.4.7.3 Verification

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

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

6.5 System qualification

6.5.1 General

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

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

6.5.2 Generic and application-specific qualification

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

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

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

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

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

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

NOTE 2 Application-specific qualification typically considers the following:

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

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

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

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

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

6.5.3 Qualification plan

6.5.3.1 General

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

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

Figure 6 provides an overview of the activities.

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

6.5.3.2 Functional and environmental qualification

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

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

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

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

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

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

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

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

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

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

6.5.3.3 Software evaluation and assessment

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

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

The software of the CB system to be qualified includes:

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

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

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

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

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

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

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

6.5.4 Additional qualification of interconnected systems

a) A plan shall be developed for the additional testing that may be required at the level of the interconnected I&C systems to complete their individual qualification, for example

electromagnetic interference tests of the interfaces for the specific lay-out and grounding, robustness of system behaviour in case of network misbehaviour and overloading.

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

6.5.5 Maintaining qualification

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

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

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

6.5.6 Documentation

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

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

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

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

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

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

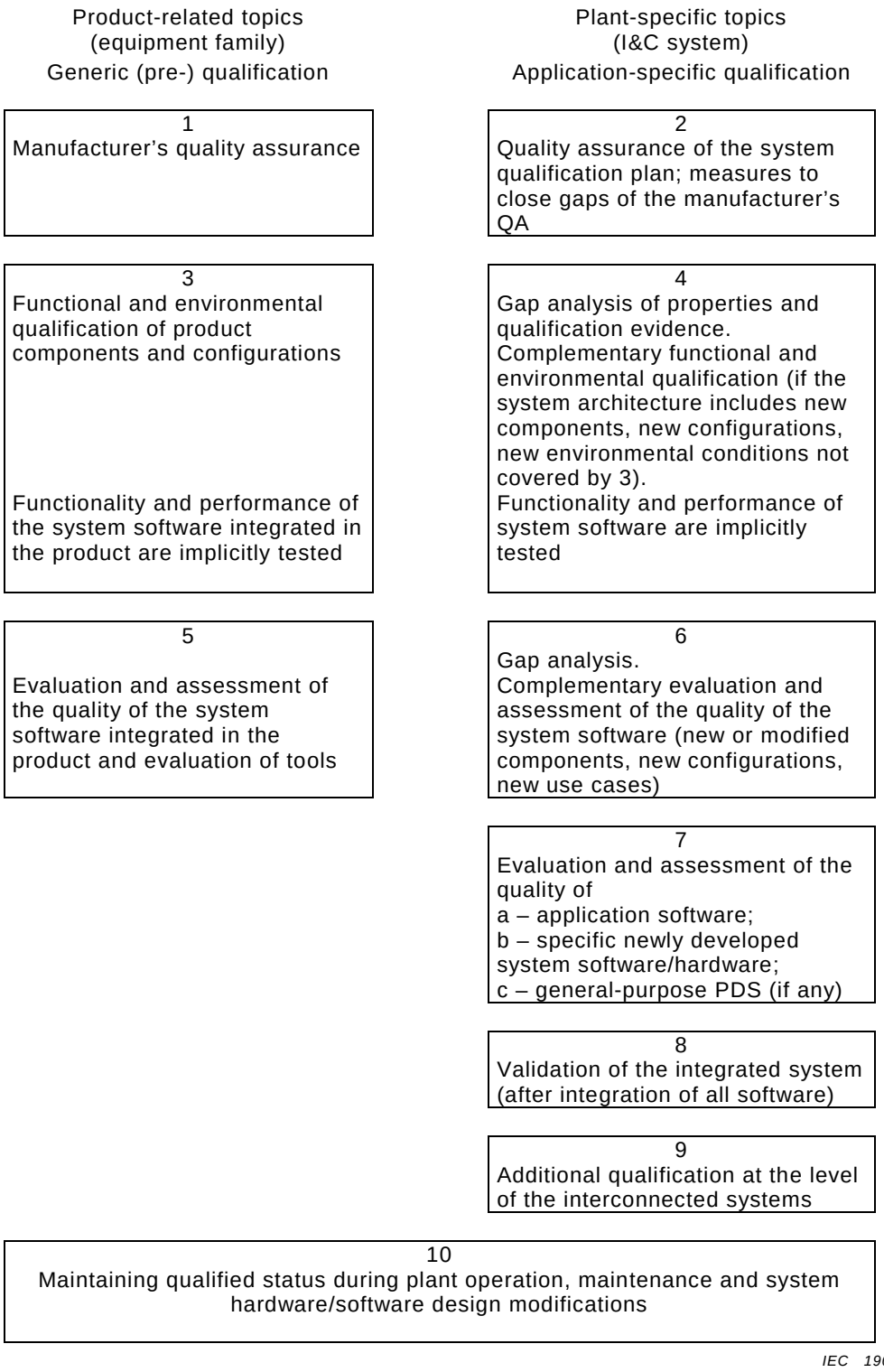


Figure 6 – Product- and plant-application-specific topics to be addressed in the system qualification plan

7 Overall integration and commissioning

7.1 General

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

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

7.2 Requirements on the objectives to be achieved

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

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

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

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

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

7.3 Output documentation

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

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

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

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

8 Overall operation and maintenance

8.1 General

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

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

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

8.2 Requirements on the objectives to be achieved

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

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

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

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

8.3 Output documentation

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

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

Annex A
(informative)

Basic safety issues in the NPP

A.1 General

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

A.2 Plant safety objectives

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

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

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

A.3 Plant safety analysis

A.3.1 General

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

The scope of the safety analysis might include:

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

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

analysis takes proper account of potential human errors in operational states and under accident conditions.

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

A.3.2 Analysis of event sequences

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

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

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

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

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

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

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

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

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

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

A.4 Defence in depth

A major contribution to the safety philosophy is provided by the defence-in-depth concept. This concept should be applied to all safety activities, whether organisational, behavioural or

design related, to ensure that there are overlapping safety provisions so that if a failure does occur, it would be compensated for or corrected (see IAEA NS-R-1; IAEA 75-INSAG-3; IAEA INSAG-10 and IAEA-NS-G-1.3).

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

Examples of the multiple levels of protection:

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

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

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

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

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

Annex B
(informative)

Categorisation of functions and classification of systems

B.1 Background for the categorisation/classification scheme

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

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

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

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

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

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

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

B.2.1 General

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

- Functional point of view

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

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

- Systems point of view

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

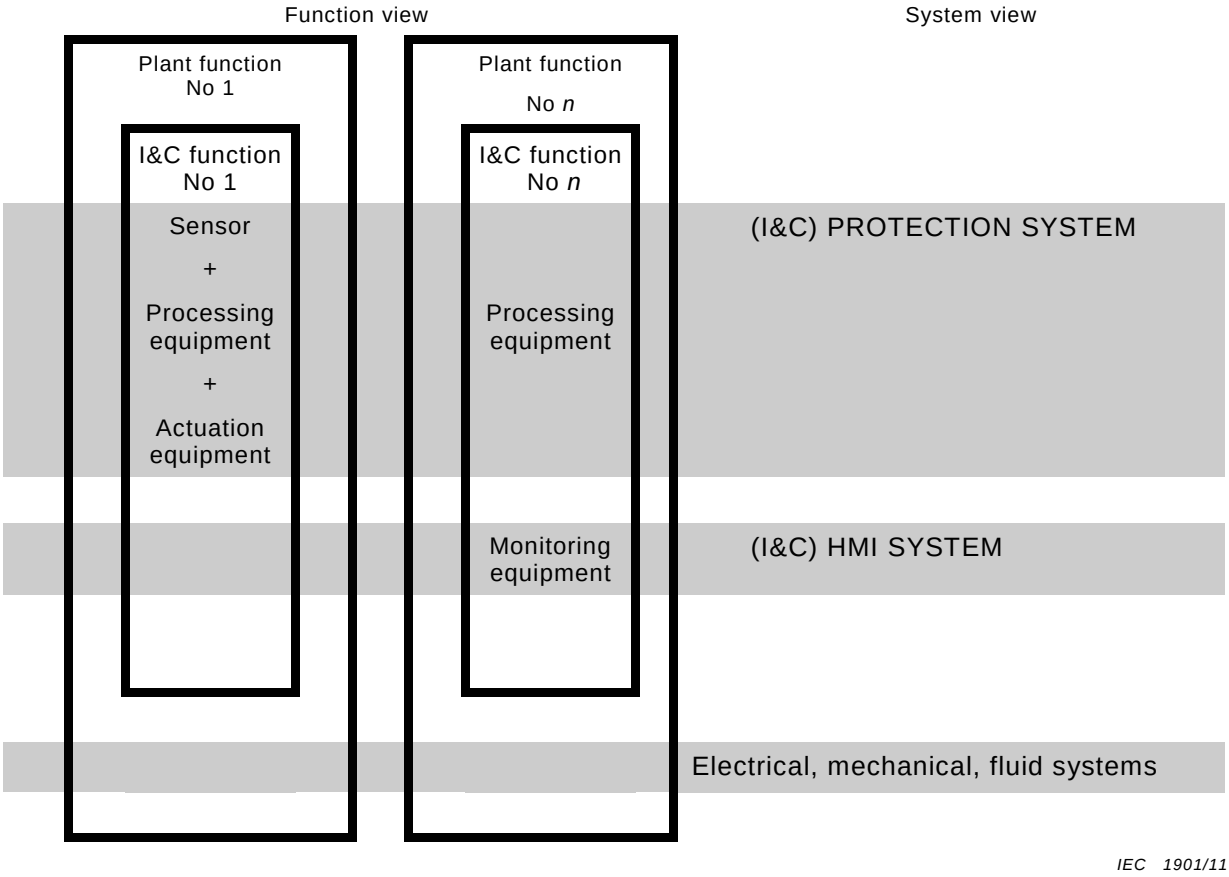


Figure B.1 – Relations between I&C functions and I&C systems

B.2.2 NPP process design phase

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

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

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

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

B.2.3 NPP I&C design phase

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

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

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

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

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

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

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

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

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

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

B.4 Classification of the I&C systems

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

a) Automation and control systems

These systems control plant or equipment parameters to

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

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

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

b) HMI systems

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

Typical functionality of these systems is to

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

c) Protection and safety actuation systems

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

The typical functionality of these systems is as follows:

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

d) Emergency power actuation system

Typical functionality:

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

The I&C systems implementing functions important to safety are assigned to one of three classes which conform to defined design, manufacturing and qualification requirements, which

make these systems suitable for implementing functions of one or more of the categories A, B or C or unclassified (see Clause B.2). A typical classification of I&C systems is given in Table B.1.

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

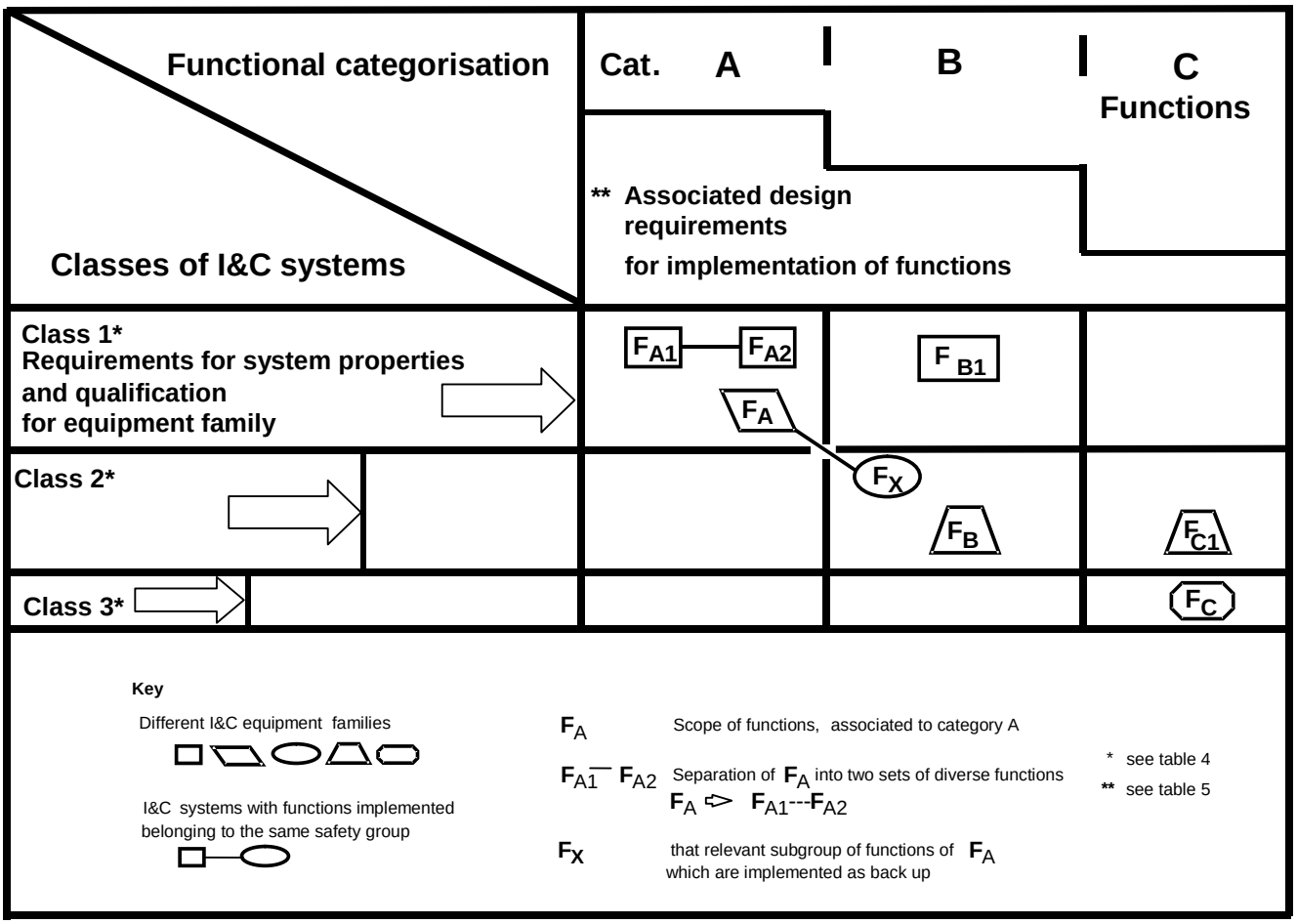
	Class 1	Class 2	Class 3	Not classified
Plant automation and control systems		x	x	x
HMI systems (class 1 HMI may be restricted to a few critical indicators and push-buttons)	x	x	x	x
Protection system and safety actuation system	x			
Emergency power actuation system	x			

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

Annex C
(informative)

Qualitative defence approach against CCF

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



IEC 1902/11

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

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

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

FA1---FA2: The scope of the safety group includes two functional diverse category A functions FA1 and FA2. The assessment of CCF analysis would need to show that for this case the application of functional diversity has given effective protection against CCF. The two

functions are then implemented in independent class 1 systems based on the same equipment family.

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

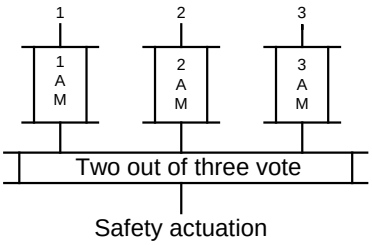
FB1---FB: The scope of the safety group includes two functional diverse category B functions FB1 and FB. The CCF analysis shall show that the application of equipment diversity and functional diversity gives sufficient protection against CCF that are of concern. The FB1 function is assigned to one class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

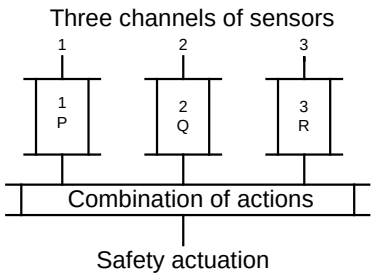
The case of FC1 and FC is similar to the previous one.

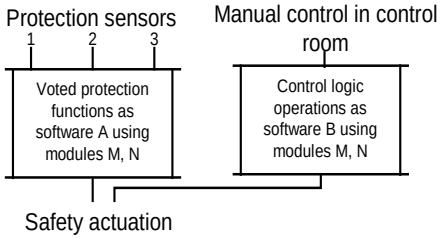
C.2 Examples of CCF sensitivity in safety groups

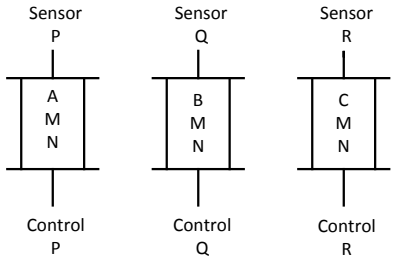
The following typical situations may exist.

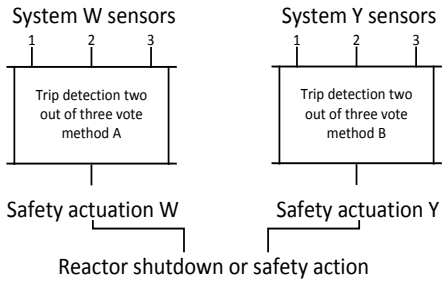
Table C.1 – Examples of CCF sensitive in safety groups

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

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

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

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

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

Annex D
(informative)

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

D.1 General

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

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

This annex includes four clauses:

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

Abbreviations

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

D.2 Comparison of scopes and concepts

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

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

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

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

a) Scope of the overall safety life cycle

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

This standard does not specifically discuss the plant safety analysis nor does it identify the means of assessing the adequacy of the performance and reliability requirements arising from the analysis. The nuclear sector practice is for the plant safety design to be performed according to specific IAEA principles, IEC rules and national regulations that

are outside the scope of this standard. The plant design base defines the PIEs, their sequences, the defence in-depth concept of the plant, the categorisation of functions required to provide the defence. However, this standard does identify the input information required from the plant design base and safety analysis which shall be made available to the I&C developers to guide the subsequent design of the I&C systems.

b) Overall safety validation/assessment

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

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

c) I&C systems and I&C architecture

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

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

d) Safety integrity level and classification

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Annex E
(informative)

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

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

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

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

Bibliography

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

_____

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

CENTRALES NUCLÉAIRES DE PUISSANCE – INSTRUMENTATION ET CONTRÔLE-COMMANDE IMPORTANTS POUR LA SÛRETÉ – EXIGENCES GÉNÉRALES POUR LES SYSTÈMES

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (CEI) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de la CEI). La CEI a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, la CEI – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de la CEI"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec la CEI, participent également aux travaux. La CEI collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de la CEI concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de la CEI intéressés sont représentés dans chaque comité d'études.
3) Les Publications de la CEI se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de la CEI. Tous les efforts raisonnables sont entrepris afin que la CEI s'assure de l'exactitude du contenu technique de ses publications; la CEI ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de la CEI s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de la CEI dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de la CEI et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) La CEI elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de la CEI. La CEI n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à la CEI, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de la CEI, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de la CEI ou de toute autre Publication de la CEI, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de la CEI peuvent faire l'objet de droits de brevet. La CEI ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

La Norme internationale CEI 61513 a été établie par le sous-comité 45A: Instrumentation et contrôle-commande des installations nucléaires, du comité d'études 45 de la CEI: Instrumentation nucléaire.

Cette deuxième édition annule et remplace la première édition publiée en 2001, dont elle constitue une révision technique.

Les principaux changements techniques par rapport à l'édition précédente sont les suivants:

- mettre en cohérence la norme avec les nouvelles révisions des documents de l'AIEA, NS-R-1 et NS-G-1.3; passer en revue les exigences et mettre à jour la terminologie et les définitions;

- prendre en compte, autant que possible, les exigences associées aux normes publiées depuis la parution de la première édition, en particulier les CEI 60880, CEI 61226, CEI 62138, CEI 62340 et CEI 60987;
- prendre en compte le fait que les techniques de génie logiciel ont réalisé des progrès significatifs durant ces années;
- intégrer les exigences relatives à la formation du personnel.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
45A/838/FDIS	45A/848/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation de cette norme.

Cette publication a été rédigée selon les Directives ISO/CEI, Partie 2.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de stabilité indiquée sur le site web de la CEI sous "http://webstore.iec.ch" dans les données relatives à la publication recherchée. A cette date, la publication sera

- reconduite,
- supprimée,
- remplacée par une édition révisée, ou
- amendée.

INTRODUCTION

a) Contexte technique, questions importantes et structure de la présente norme

La présente Norme Internationale établit des exigences applicables aux matériels et systèmes d'instrumentation et de contrôle commande (systèmes d'I&C) utilisés pour réaliser des fonctions importantes pour la sûreté dans les centrales nucléaires de puissance (CNP).

Cette norme met l'accent sur la relation existant entre:

- les objectifs de sûreté de la CNP et les exigences applicables à l'ensemble de l'architecture des systèmes d'I&C importants pour la sûreté.
- l'ensemble de l'architecture des systèmes d'I&C et les exigences relatives aux systèmes individuels importants pour la sûreté.

L'objectif de la présente norme est d'être utilisée par les concepteurs, les exploitants de centrales nucléaires, les évaluateurs de système et par les régulateurs.

b) Position de la présente norme dans la collection de normes du SC 45A de la CEI

La CEI 61513 est le document du SC 45A de la CEI de premier niveau qui traite des exigences générales pour les systèmes. Elle est le point d'entrée de la collection des normes du SC 45A de la CEI.

Pour plus de détails sur la collection de normes du SC 45A de la CEI, voir d) de cette introduction.

c) Recommandations et limites relatives à l'application de présente norme

Il est important de noter que la présente norme n'établit pas d'exigence fonctionnelle supplémentaire pour les systèmes de sûreté.

Afin d'assurer la pertinence de la présente norme pour les années à venir, l'accent est mis sur les questions de principes plutôt que sur les technologies particulières.

d) Description de la structure de la collection des normes du SC 45A de la CEI et relations avec d'autres documents de la CEI, et d'autres organisations (AIEA, ISO)

Le document de niveau supérieur de la collection de normes produites par le SC 45A de la CEI est la norme CEI 61513. Cette norme traite des exigences relatives aux systèmes et équipements d'instrumentation et de contrôle-commande (systèmes d'I&C) utilisés pour accomplir les fonctions importantes pour la sûreté des centrales nucléaires, et structure la collection de normes du SC 45A de la CEI.

La CEI 61513 fait directement référence aux autres normes du SC 45A de la CEI traitant de sujets génériques, tels que la catégorisation des fonctions et le classement des systèmes, la qualification, la séparation des systèmes, les défaillances de cause commune, les aspects logiciels et les aspects matériels relatifs aux systèmes programmés, et la conception des salles de commande. Il convient de considérer que ces normes, de second niveau, forment, avec la norme CEI 61513, un ensemble documentaire cohérent.

Au troisième niveau, les normes du SC 45A de la CEI, qui ne sont généralement pas référencées directement par la norme CEI 61513, sont relatives à des matériels particuliers, à des méthodes ou à des activités spécifiques. Généralement ces documents, qui font référence aux documents de deuxième niveau pour les activités génériques, peuvent être utilisés de façon isolée.

Un quatrième niveau qui est une extension de la collection de normes du SC 45A de la CEI correspond aux rapports techniques qui ne sont pas des documents normatifs.

La CEI 61513 a adopté une présentation similaire à celle de la publication fondamentale de sécurité CEI 61508, avec un cycle de vie de sûreté d'ensemble et un cycle de vie de sûreté des systèmes. Au niveau sûreté nucléaire, elle est l'interprétation des exigences générales de la CEI 61508-1 [1][1], de la CEI 61508-2 et de la CEI 61508-4 pour le secteur nucléaire. Dans ce domaine, la CEI 60880 et la CEI 62138 correspondent à la CEI 61508-3 [2] pour le secteur nucléaire.

La CEI 61513 fait référence aux normes ISO ainsi qu'aux documents AIEA GS-R-3 et AIEA GS-G-3.1 pour ce qui concerne l'assurance qualité.

Les normes produites par le SC 45A de la CEI sont élaborées de façon à être en accord avec les principes de sûreté fondamentaux du Code AIEA sur la sûreté des centrales nucléaires, ainsi qu'avec les guides de sûreté de l'AIEA, en particulier avec le document d'exigences NS-R-1 qui établit les exigences de sûreté relatives à la conception des centrales nucléaires et avec le guide de sûreté NS-G-1.3 qui traite de l'instrumentation et du contrôle commande importants pour la sûreté des centrales nucléaires. La terminologie et les définitions utilisées dans les normes produites par le SC 45A sont conformes à celles utilisées par l'AIEA.

NOTE Il est fait l'hypothèse que pour la conception des systèmes d'I&C dans les CNP qui sont supports de fonctions de sûreté conventionnelle (par exemple pour garantir la sécurité des travailleurs, la protection des biens, la prévention contre les risques chimiques et la prévention contre les risques liés au procédé énergétique) on applique des normes nationales ou internationales, dont les exigences sont comparables à des normes telle que la série CEI 61508.

---

1 Les chiffres entre crochets se réfèrent à la bibliographie.

CENTRALES NUCLÉAIRES DE PUISSANCE – INSTRUMENTATION ET CONTRÔLE-COMMANDE IMPORTANTS POUR LA SÛRETÉ – EXIGENCES GÉNÉRALES POUR LES SYSTÈMES

1 Domaine d'application

1.1 Généralités

Les systèmes d'I&C importants pour la sûreté peuvent être réalisés à l'aide de composants traditionnels câblés, de composants informatiques ou d'une combinaison des deux (voir Note 1). La présente Norme internationale fait état des exigences et des recommandations (voir Note 2) relatives à l'architecture d'ensemble de l'I&C incluant l'une ou l'autre de ces technologies ou les deux.

La présente norme souligne aussi la nécessité d'avoir des exigences complètes et précises, issues des objectifs de sûreté de la centrale, comme condition préalable à l'établissement des exigences relatives à l'architecture d'ensemble de l'I&C, et ensuite à l'établissement de celles portant sur chaque système d'I&C individuel important pour la sûreté.

La présente norme introduit les concepts de cycle de vie de sûreté pour l'ensemble de l'architecture d'I&C, et de cycle de vie de sûreté pour chaque système d'I&C individuel. Ainsi, elle met en exergue les relations existant entre les objectifs de sûreté de la CNP et les exigences relatives à l'architecture d'ensemble des systèmes importants pour la sûreté, et les relations existant entre l'architecture d'ensemble de l'I&C et les exigences relatives aux systèmes individuels importants pour la sûreté.

Les cycles de vie présentés et détaillés dans la présente norme ne sont pas les seuls possibles; d'autres cycles de vie peuvent être adoptés, sous réserve que les objectifs de la présente norme soient atteints.

NOTE 1 Les systèmes d'I&C peuvent aussi utiliser des modules électroniques réalisés à base de composants électroniques complexes tels que des ASICs ou des FPGA. Suivant le domaine d'application et les fonctionnalités de ces composants, ils peuvent être traités conformément aux recommandations relatives aux matériels électroniques conventionnels, ou à des matériels informatiques comparables. Une partie significative des recommandations relatives aux équipements numériques est aussi applicable lors de la conception d'équipements intégrant des composants électroniques complexes, y compris par exemple les concepts liés à réutilisation de conceptions préexistantes, ainsi que l'évaluation des erreurs de conception lors de la conception de logiciels ou de composants matériel complexe.

NOTE 2 Dans la suite de la présente norme, le terme « exigences » est utilisé comme terme général pour les « exigences et recommandations » de la norme. La distinction apparaît au niveau des exigences spécifiques, lorsque les exigences sont exprimées par «doit» et les recommandations par «il est recommander de» ou «il convient que».

1.2 Application: nouvelles centrales et centrales existantes

La présente norme s'applique à l'I&C des nouvelles centrales nucléaires, ainsi qu'à l'amélioration ou à la rénovation de l'I&C des centrales existantes.

Pour les centrales existantes, seul un sous-ensemble des exigences est applicable. Il convient de définir ce sous-ensemble au début de chaque projet.

1.3 Cadre général

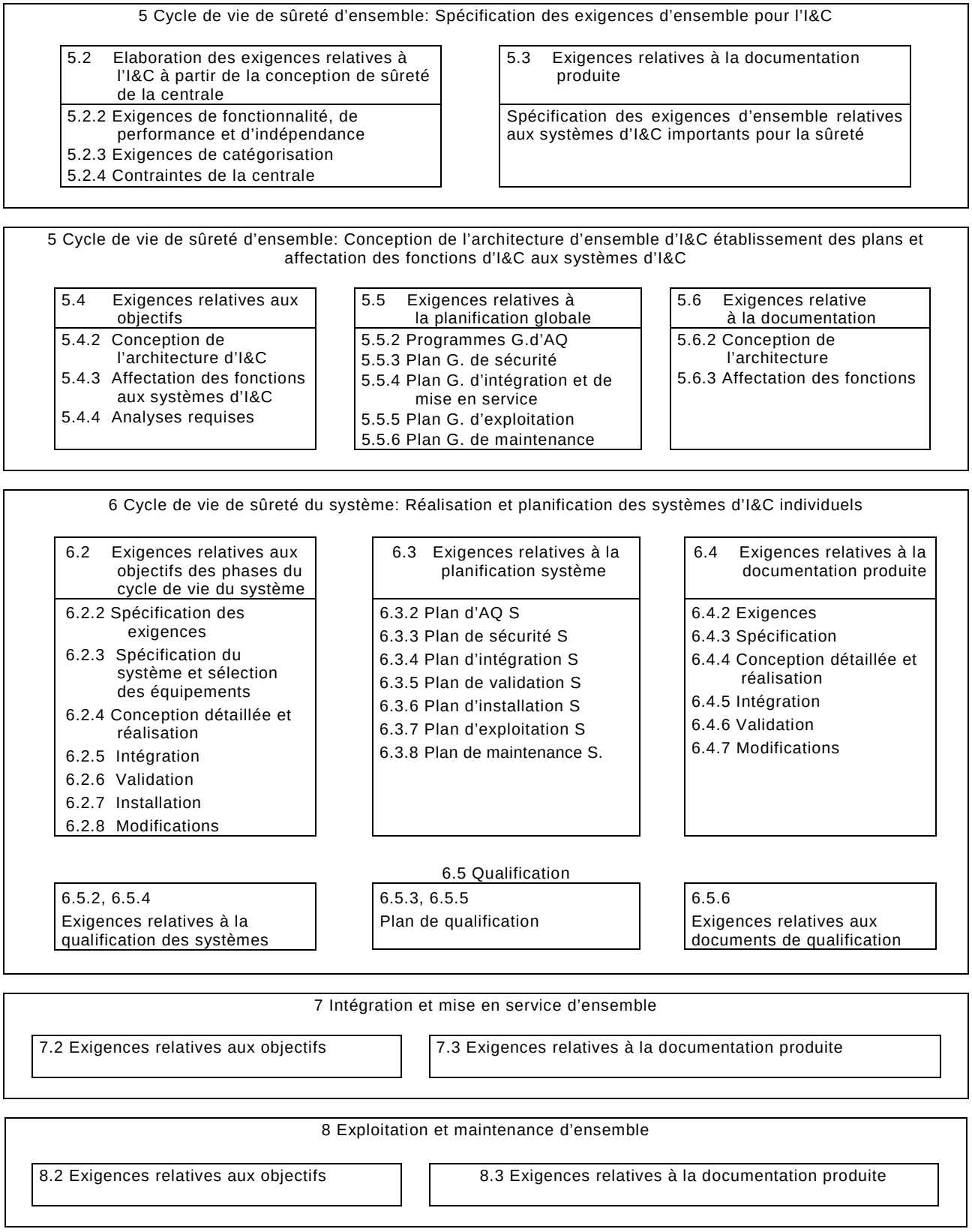
La présente norme comprend quatre articles normatifs (dont la vue d'ensemble est fournie par la Figure 1):

- l'Article 5 traite de l'architecture d'ensemble des systèmes d'I&C importants pour la sûreté:
  - définition des exigences relatives aux fonctions d'I&C et aux systèmes et équipements associés, déduites de l'analyse de sûreté de la centrale, de la catégorisation des fonctions d'I&C, de la disposition de la centrale et du contexte opérationnel,
  - découpage de l'architecture d'ensemble de l'I&C en plusieurs systèmes et affectation des fonctions d'I&C à ces systèmes. Les critères de conception y sont identifiés, y compris ceux nécessaires à la défense en profondeur et à la minimisation du risque de défaillance de cause commune (DCC),
  - établissement des plans relatifs à l'architecture d'ensemble des systèmes d'I&C.
- l'Article 6 traite des exigences relatives à chacun des systèmes d'I&C importants pour la sûreté, en particulier celles relatives aux systèmes programmés. Ceci comprend la différentiation des exigences en fonction des catégories de sûreté des fonctions d'I&C qui sont mises en œuvre;
- les Articles 7 et 8 traitent de l'intégration, de la mise en service, de l'exploitation et la maintenance des systèmes d'I&C;

NOTE La Figure 1 met en exergue la structure de la norme. Elle ne présente pas nécessairement les activités de façon chronologique qui peuvent être en réalité exécutées en parallèle ou comprendre des itérations.

De plus, la présente norme comprend les annexes informatives suivantes:

- l'Annexe A présente les relations entre les concepts de sûreté de base de l'AIEA et ceux utilisés dans la présente norme,
- l'Annexe B fournit des informations sur les principes de catégorisation et de classement,
- l'Annexe C présente des exemples illustrant les niveaux de sensibilité de l'I&C aux DCC,
- l'Annexe D est un guide pour pouvoir comparer la présente norme avec les parties 1, 2 et 4 de la CEI 61508. Elle examine les principales exigences de la CEI 61508 afin de vérifier que les questions liées à la sûreté sont abordées correctement. Elle rappelle les termes communément employés et elle justifie s'il y a lieu l'adoption de techniques ou de termes différents ou complémentaires;
- l'Annexe E indique les modifications qui devront être réalisées lors des futures révisions des normes filles de la CEI 61513 pour que celles ci soient consistantes avec la présente version et que cela minimise les chevauchements entre les contenus de documents.



Légende AQ: Assurance Qualité; G: Global; S: Système

Figure 1 – Cadre général de la présente norme

2 Références normatives

Les documents de référence suivants sont indispensables pour l'application du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

CEI 60671, *Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle-commande importants pour la sûreté – Essais de surveillance*

CEI 60709, *Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle commande importants pour la sûreté – Séparation*

CEI 60780, *Centrales nucléaires – Equipements électriques de sûreté – Qualification*

CEI 60880:2006, *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Aspects logiciels des systèmes programmés réalisant des fonctions de catégorie A*

CEI 60964:2009, *Centrales nucléaires de puissance – Salles de commande – Conception*

CEI 60965, *Centrales nucléaires de puissance – Salles de commande – Points de commande supplémentaires pour l'arrêt des réacteurs sans accès à la salle de commande principale (salle de commande de repli)*

CEI 60980, *Pratiques recommandées pour la qualification sismique du matériel électrique du système de sûreté dans les centrales électronucléaires*

CEI 60987:2007, *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Exigences applicables à la conception du matériel des systèmes informatisés*

CEI 61000-4-1, *Compatibilité électromagnétique (CEM) – Partie 4-1: Techniques d'essai et de mesure – Vue d'ensemble de la série CEI 61000-4*

CEI 61000-4-2, *Compatibilité électromagnétique (CEM) – Partie 4-2: Techniques d'essai et de mesure – Essai d'immunité aux décharges électrostatiques*

CEI 61000-4-3, *Compatibilité électromagnétique (CEM) – Partie 4-3: Techniques d'essai et de mesure – Essai d'immunité aux champs électromagnétiques rayonnés aux fréquences radioélectriques*

CEI 61000-4-4, *Compatibilité électromagnétique (CEM) – Partie 4-4: Techniques d'essai et de mesure – Essais d'immunité aux transitoires électriques rapides en salves*

CEI 61000-4-5, *Compatibilité électromagnétique (CEM) – Partie 4-5: Techniques d'essai et de mesure – Essai d'immunité aux ondes de choc*

CEI 61000-4-6, *Compatibilité électromagnétique (CEM) – Partie 4-6: Techniques d'essai et de mesure – Immunité aux perturbations conduites, induites par les champs radioélectriques*

CEI 61226:2009, *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Classement des fonctions d'instrumentation et de contrôle-commande*

CEI 61500, *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Communication de données dans les systèmes réalisant des fonctions de catégorie A*

CEI 61508-2:2010, *Sécurité fonctionnelle des systèmes électriques/ électroniques/électroniques programmables relatifs à la sécurité – Partie 2: Exigences pour les systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité*

CEI 61508-4:2010, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 4: Définitions et abréviations*

CEI 62138:2004, *Centrales nucléaires – Instrumentation et contrôle-commande importants pour la sûreté – Aspects logiciels des systèmes informatisés réalisant des fonctions de catégorie B ou C*

CEI 62340, *Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle-commande importants pour la sûreté – Exigences permettant de faire face aux défaillances de cause commune (DCC)*

ISO 9001:2008, *Systèmes de management de la qualité – Exigences*

AIEA INSAG N° 10:1997, *La Défense en Profondeur en Sûreté Nucléaire*

AIEA NS-R-1:2000, *Sûreté des Centrales Nucléaires: Conception*

IAEA GS-R-3:2006, *The Management System for Facilities and Activities Safety – Requirements*
(disponible en anglais seulement)

GS-G-3.1:2006, *Application of the Management System for Facilities and Activities – Safety Guide*
(disponible en anglais seulement)

AIEA NS-G-1.3:2005, *Systèmes d'instrumentation et de contrôle-commande importants pour la sûreté des centrales nucléaires*

AIEA 75-INSAG-3, Rev. 1 – INSAG 12:1999, *Principes de sûreté fondamentaux pour les centrales nucléaires*

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions suivants s'appliquent.

3.1
fonction d'application
fonction d'un système d'I&C qui accomplit une tâche relative au processus sous contrôle plutôt qu'au fonctionnement du système lui-même

NOTE 1 Voir également « fonction d'I&C », « système d'I&C », « logiciel d'application ».

NOTE 2 Une fonction d'application est normalement une sous-fonction d'une fonction d'I&C.

3.2
logiciel d'application
partie du logiciel d'un système d'I&C qui exécute les fonctions d'application

NOTE 1 Voir également « fonction d'application », « bibliothèque d'application », « logiciel système ».

NOTE 2 Le logiciel d'application est à mettre en regard avec le « logiciel système ».

NOTE 3 Voir aussi la Figure 2.

NOTE 4 Dans le contexte des composants électroniques complexes, le terme « logique d'application » peut être utilisé plutôt que celui de « logiciel d'application » qui est approprié et utilisé pour l'ensemble de cette norme.

3.3
bibliothèque d'application
ensemble de modules logiciels qui exécutent des fonctions d'application standard

NOTE 1 Si des équipements préexistants sont utilisés, cette bibliothèque est considérée comme faisant partie du logiciel système et est qualifiée comme telle.

NOTE 2 Voir aussi la Figure 2.

3.4
catégorie d'une fonction d'I&C
l'une des trois affectations de sûreté possibles (A, B, C) des fonctions d'I&C résultant de l'évaluation de l'importance pour la sûreté de la fonction exécutée. Une affectation « non classée » peut être délivrée si la fonction n'est pas importante pour la sûreté

NOTE 1 Voir également « classe d'un système d'I&C », « fonction d'I&C ».

NOTE 2 La CEI 61226 définit trois catégories de fonctions d'I&C. A chaque catégorie correspond un ensemble d'exigences relatives à la fois aux fonctions d'I&C (spécification, conception, intégration, vérification et validation) et à l'ensemble des composants nécessaires à la réalisation des fonctions (propriétés et qualification) indépendamment de la manière suivant laquelle ces composants sont distribués dans plusieurs systèmes d'I&C interconnectés. Pour davantage de clarté, la présente norme définit des catégories de fonctions d'I&C et des classes de systèmes d'I&C. Elle établit une relation entre la catégorie d'une fonction et la classe minimale des systèmes et équipements associés.

3.5
circuit
ensemble de composants interconnectés dans un système qui produit un signal de sortie unique. Un circuit perd son identité lorsque les signaux de sortie uniques sont combinés avec ceux d'autres circuits (par exemple un circuit de surveillance ou un circuit actionneur de sûreté)

[Glossaire de Sûreté de l'AIEA, Edition 2007] [3]

3.6
classe d'un système d'I&C
l'une des trois affectations possibles (1,2,3) des systèmes d'I&C importants pour la sûreté, résultant de la nécessité pour ces systèmes d'exécuter des fonctions d'I&C d'importances pour la sûreté différentes. Une affectation « Non Classé » est délivrée si le système d'I&C n'exécute pas de fonction importante pour la sûreté

NOTE Voir également "catégorie d'une fonction d'I&C", "système important pour la sûreté", "systèmes de sûreté".

3.7
mise en service
ensemble des opérations qui consistent à faire fonctionner les systèmes et composants fabriqués des installations et activités et à vérifier qu'ils sont conformes à la conception et satisfont aux critères de performance prescrits

NOTE La mise en service peut comprendre en même temps des essais non liés aux aspects nucléaires/non liés à la radioactivité et des essais liés aux aspects nucléaires/ liés à la radioactivité

[Glossaire de Sûreté de l'AIEA, Edition 2007]

3.8
défaillance de cause commune
DCC
défaillance de plusieurs structures, systèmes ou composants due à un évènement ou à une cause unique

[Glossaire de Sûreté de l'AIEA, Edition 2007, modifiée]

NOTE 1 Les causes communes peuvent être internes ou externes au système d'I&C.

NOTE 2 La définition de la CEI diffère de celle de l'AIEA en deux points:

1) Le terme « spécifique » a été supprimé car autrement la définition de DCC n'aurait pas été consistante avec celle de MDC "Mode de défaillance commun ». De plus, ce terme supplémentaire n'est pas nécessaire pour comprendre la définition.

2) Le mot "et" a été remplacé par "ou" car les experts du SC 45A de la CEI ont pensé qu'il s'agissait d'une erreur typographique. Cette correction est déjà faite sur le dictionnaire de l'AIEA en ligne (NUSAFE).

3.9
complexité
degré de difficulté à comprendre ou vérifier la conception, la mise en œuvre ou le comportement d'un système ou d'un composant

[IEEE 610, modifiée [4]

3.10
composant
l'une des pièces constituant un système. Un composant peut être matériel ou logiciel et peut être subdivisé en plusieurs autres composants

[IEEE 610]

NOTE 1 Voir également « système d'I&C », « équipement »

NOTE 2 Les termes « équipement », « composant » et « module » sont souvent utilisés de manière interchangeable. La relation entre ces termes n'a pas encore été normalisée.

NOTE 3 Cette définition du SC 45A de la CEI est dans le principe compatible avec la sous définition de "Composant" donnée dans la définition de "SCC, Structures, Systèmes et Composants" du Glossaire de Sûreté de l'AIEA Edition 2007. Néanmoins comme il est seulement donné des exemples de composants matériel, ceci peut induire en erreur le lecteur, aussi le SC 45A de la CEI a préféré utiliser une définition qui explicitement couvre les composants logiciel.

3.11
système programmé
système d'I&C dont les fonctions dépendent en grande partie, ou sont totalement effectuées à l'aide de microprocesseurs, d'un matériel électronique programmé ou d'ordinateurs

NOTE Equivalent à système programmé, système informatique.

3.12
gestion de la configuration
processus consistant à identifier et à consigner les caractéristiques des structures, systèmes et composants (y compris des systèmes programmés et des logiciels) d'une installation, et à s'assurer que les modifications de ces caractéristiques sont correctement élaborées, évaluées, approuvées, publiées, mises en œuvre, vérifiées, enregistrées et incorporées dans la documentation relative à cette installation

[Glossaire de sûreté de l'AIEA, Edition 2007]

3.13
données
représentation d'informations ou d'instructions permettant la communication, l'interprétation ou le traitement par ordinateur

[IEEE 610, modifiée]

NOTE Voir Figure 2.

3.14
défense en profondeur
mise en œuvre de mesures de protection multiples pour atteindre un objectif de sûreté donné, de façon que cet objectif soit atteint même en cas de défaillance de l'une des mesures de protection

[Glossaire de sûreté de l'AIEA, Edition 2007]

NOTE Voir aussi l'Article A.4.

3.15
diversité
présence de plusieurs systèmes ou composants redondants pour l'accomplissement d'une fonction déterminée, lorsque ces différents systèmes ou composants possèdent des attributs différents afin de réduire le risque de défaillance de cause commune

[Glossaire de sûreté de l'AIEA, Edition 2007, modifiée]

NOTE 1 Lorsque le terme "Diversité" est utilisé avec un attribut qualificatif, alors ce terme revêt son sens général: " Existence de deux ou plusieurs manières différentes d'atteindre un objectif spécifié. ", et l'attribut qualificatif indique les caractéristiques correspondant aux différentes applications du terme, par exemple diversité fonctionnelle, diversité matériel, diversité des signaux.

NOTE 2 Voir également « diversité fonctionnelle ».

3.16
équipement
une ou plusieurs parties d'un système. Un équipement est une partie déterminée et définissable (et généralement amovible) d'un système

NOTE 1 Voir également « composant », « système d'I&C ».

NOTE 2 Un équipement peut contenir une partie logicielle.

NOTE 3 Les termes « équipement », « composant » et « module » sont souvent utilisés de manière interchangeable. La relation entre ces termes n'a pas encore été normalisée.

NOTE 4 Cette définition dévie de celle donnée dans la CEI 60780. Cet écart est justifié par le fait que la CEI 61513 considère que « l'équipement » fait partie du système alors que la CEI 60780 considère que l'équipement est l'objet de la qualification.

3.17
famille d'équipements
un ensemble de composants matériels et logiciels pouvant travailler de manière complémentaire dans une ou plusieurs architectures définies (configurations). Le développement des configurations spécifiques à la centrale et du logiciel d'application associé peut être réalisé par des outils logiciels. Une famille d'équipements fournit normalement un certain nombre de fonctionnalités standards (bibliothèque des fonctions d'application) qui peuvent être combinées pour générer un logiciel d'application spécifique

NOTE 1 Voir également « fonctionnalité », « logiciel d'application », « bibliothèque d'application ».

NOTE 2 Une famille d'équipements peut être un produit provenant d'un fabricant ou un ensemble de produits interconnectés et adaptés par un fournisseur.

NOTE 3 Le terme « plate-forme de composants » est parfois utilisé comme synonyme de « famille d'équipements »

3.18
erreur
différence entre une valeur ou condition calculée ou mesurée et la valeur ou condition réelle, spécifiée ou théorique

NOTE Voir Figure 3.

3.19
appréciation d'une propriété d'un système
attribution d'une valeur qualitative ou quantitative à cette propriété du système

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

3.20
défaillance
perte de la capacité d'une structure, d'un système ou d'un composant de fonctionner conformément aux critères d'acceptation

[Glossaire de Sûreté de l'AIEA, Edition 2007, modifiée]

NOTE 1 Les équipments sont considérés comme défaillants lorsqu'ils ne fonctionnent plus, que l'on en ait besoin ou non à ce moment-là. Par exemple, la défaillance d'un système de secours peut ne pas être manifeste jusqu'à ce que l'on ait recours à ce système, soit dans le cadre d'essais, soit lorsque le système principal est en panne.

NOTE 2 Une défaillance est le résultat d'un défaut du matériel, d'un défaut du logiciel, d'un défaut du système ou d'une erreur humaine. Elle est engendrée par la trajectoire du signal associé.

NOTE 3 Voir aussi « défaut », « défaillance logicielle ».

NOTE 4 Les experts du SC 45A de la CEI considèrent que la définition de l'AIEA ne reflète pas l'idée que la défaillance est un évènement et n'est pas un état. Les experts du SC 45A de la CEI ont proposé de modifier en conséquence la définition de l'AIEA pour prendre ce point en compte.

3.21
défaut
imperfection dans un composant matériel, logiciel ou système

NOTE 1 Voir Figure 3.

NOTE 2 Les défauts peuvent provenir de défauts aléatoires, par exemple suite au vieillissement du matériel, et peuvent être systématiques, par exemple des défauts logiciels, suite à des erreurs de conception.

NOTE 3 Un défaut (notamment un défaut de conception) peut ne pas être détecté dans le système jusqu'à l'apparition d'une situation pour laquelle le résultat produit n'est pas conforme à ce qui était prévu pour la fonction, c'est à dire qu'une défaillance se produit.

NOTE 4 Voir aussi « défaut logiciel ».

3.22
diversité fonctionnelle
application de la diversité au niveau des fonctions d'application relatives au procédé industriel (par exemple le déclenchement d'une action de protection sur seuil de pression ou sur seuil de température)

[CEI 60880:2006, 3.19 modifiée]

NOTE La Edition 2007 du Glossaire de Sûreté de l'AIEA ne donne pas de définition de la diversité fonctionnelle mais fournit des exemples de moyens qui permettent d'assurer la diversité fonctionnelle. Cette définition du SC 45A de la CEI est compatible avec les moyens qui sont cités dans le Glossaire de Sûreté de l'AIEA comme permettant d'assurer la diversité fonctionnelle.

3.23
validation fonctionnelle
vérification de la conformité des spécifications des fonctions d'application aux exigences fonctionnelles et de performance de haut niveau de la centrale. Elle est complémentaire de la validation du système (qui vérifie la conformité du système à la spécification des fonctions).

3.24
fonctionnalité
attribut d'une fonction définissant les opérations de transformation des informations d'entrée en informations de sortie

NOTE La fonctionnalité des fonctions d'application affecte généralement le fonctionnement de la centrale. Les informations d'entrée peuvent provenir des capteurs, des opérateurs, des autres équipements ou logiciels. Les informations de sortie peuvent être dirigées vers les actionneurs, les opérateurs, les autres équipements ou logiciels (voir la CEI 61508-2).

3.25
événement dangereux
événement ayant le potentiel de provoquer des dommages pour le personnel, les composants, les équipements ou les structures de la centrale. Les événements dangereux sont répartis en événements internes et externes

NOTE 1 Les événements dangereux internes sont, par exemple, les incendies et les inondations. Ils peuvent être aussi la conséquence des EIP (par exemple accident de perte de réfrigérant primaire, rupture de la tuyauterie de vapeur).

NOTE 2 Les phénomènes dangereux externes sont, par exemple, les tremblements de terre et la foudre.

3.26
erreur (ou faute) humaine
action humaine conduisant à un résultat indésirable

[CEI 60880:2006, 3.21]

3.27
architecture d'I&C
structure organisant les systèmes de CC de la centrale importants pour la sûreté

NOTE 1 Voir également « architecture d'un système d'I&C », « système d'I&C ».

NOTE 2 L'architecture définit notamment les principales fonctions, classes et limites de chaque système, les interconnexions et l'indépendance entre les systèmes, les priorités et les votes concernant les signaux agissant simultanément, l'IHM.

NOTE 3 Dans la présente norme, le terme désigne uniquement un sous-ensemble de l'architecture globale de l'I&C de la centrale. Cette dernière inclut également les systèmes et équipements non classés.

NOTE 4 Par soucis de simplicité, l'expression « architecture d'I&C d'ensemble » est utilisé comme un raccourci de l'expression « architecture d'ensemble des systèmes d'I&C importants pour la sûreté".

3.28
fonction d'I&C
fonction permettant de commander, exploiter et/ou surveiller une partie définie du procédé

NOTE 1 Le terme « fonction d'I&C » est utilisé par les ingénieurs automaticiens pour mettre en forme les exigences de fonctionnalité relatives à l'I&C. Une fonction d'I&C est définie de manière à

– donner une représentation complète d'un objectif fonctionnel,
– pouvoir être catégorisée en fonction de son degré d'importance pour la sûreté,
– englober tous les types d'éléments, du capteur jusqu'à l'actionneur, et réaliser ainsi son objectif fonctionnel.

NOTE 2 Une fonction d'I&C peut être subdivisée en plusieurs sous-fonctions (par exemple mesure, commande, mise en marche) pour permettre l'affectation aux systèmes d'I&C.

3.29
système d'I&C
système exécutant des fonctions d'I&C ainsi que des fonctions de service et d'affichage liées au fonctionnement du système lui-même. Sa technologie est électrique et/ou électronique et/ou électronique programmable

Le terme est utilisé comme terme général comprenant tous les éléments du système, tels que les alimentations électriques, les capteurs et autres dispositifs d'entrée, les bus de données et autres chemins de communication, les actionneurs et autres dispositifs de sortie. (voir Note 2). Les différentes fonctions d'un système peuvent utiliser des ressources dédiées ou partagées.

NOTE 1 Voir également « système » et « fonction d'I&C ».

NOTE 2 Les éléments contenus dans un système d'I&C donné sont définis dans la spécification des limites de ce système.

NOTE 3 Selon leur fonctionnalité propre, l'AIEA fait la distinction entre les systèmes de contrôle et de commande, les systèmes d'IHM, les systèmes de verrouillage et les systèmes de protection (voir l'Article B.4).

3.30
architecture d'un système d'I&C
structure organisant un système d'I&C

NOTE Voir également « architecture d'I&C ».

3.31
équipement indépendant
équipement qui possède les deux caractéristiques suivantes:

1) la capacité d'exécuter la fonction demandée n'est pas affectée par le fonctionnement ou la défaillance d'un autre équipement;
2) la capacité d'exécuter la fonction demandée n'est pas affectée par les effets de l'événement initiateur postulé pour lequel il doit fonctionner

[Glossaire de Sûreté de l'AIEA, Edition 2007]

NOTE Les moyens permettant de garantir l'indépendance lors de la conception sont l'isolement électrique (également appelée isolement fonctionnelle dans les documents de l'AIEA), la séparation physique et l'indépendance des communications.

3.32
interruption
suspension d'une opération, par exemple l'exécution d'un programme informatique, provoquée par un événement extérieur à cette opération

[IEEE 610]

3.33
constituant important pour la sûreté
constituant faisant partie d'un groupe de sûreté et/ou dont le mauvais fonctionnement ou la défaillance pourrait entraîner une exposition à des rayonnements du personnel du site ou de personnes du public

Les constituants importants pour la sûreté comprennent:

a) les structures, systèmes et composants dont le mauvais fonctionnement ou la défaillance pourraient entraîner une exposition indue à des rayonnements du personnel du site ou de personnes du public;
b) les structures, systèmes et composants qui empêchent les incidents de fonctionnement prévus d'aboutir à des conditions accidentelles;
c) les dispositifs prévus pour atténuer les conséquences d'un mauvais fonctionnement ou d'une défaillance de structures, systèmes ou composants

[Glossaire de Sûreté de l'AIEA, Edition 2007]

NOTE 1 L'objectif de cette définition est de couvrir tous les aspects relatifs à la sûreté nucléaire.

NOTE 2 Dans la présente norme les constituants principalement pris en compte seront les systèmes d'I&C et les fonctions d'I&C.

NOTE 3 Voir aussi « fonction d'I&C ».

3.34
cycle de vie de sûreté de l'ensemble de l'I&C
activités nécessaires à la mise en œuvre des systèmes et composants de l'architecture d'I&C importants pour la sûreté. Elles ont lieu entre la spécification des exigences d'I&C (lors de la

phase de conception de sûreté de la centrale) et le retrait du service du dernier système d'I&C

[CEI 61508-4:2010, 3.7.1, modifiée] [6]

NOTE 1 Du cycle de vie de sûreté de l'ensemble de l'I&C découlent des exigences sur les cycles de vie de sûreté des systèmes individuels.

NOTE 2 Voir aussi « cycle de vie de sûreté du système ».

3.35
événement initiateur postulé
EIP
évènement dont on détermine au stade de la conception qu'il peut entraîner des incidents de fonctionnement prévus ou des conditions accidentelles

[Glossaire de Sûreté de l'AIEA, Edition 2007]

3.36
constituant prédéveloppé
constituant matériel ou logiciel ou programmé qui existe déjà, qui est disponible comme produit commercial ou propriétaire, et dont l'utilisation est envisagée

NOTE Cette définition est plus large que celle de logiciel prédéveloppé, voir 3.28 de la CEI 60880:2006.

3.37
organisation en charge du projet
organisation(s) ou personnes responsables, pendant les phases du cycle de vie de sûreté de l'ensemble de l'I&C et/ou pendant les phases des cycles de vie de sûreté des systèmes d'I&C, de la définition et de la mise en place de toutes les activités ayant trait à la gestion et aux aspects techniques concernant les fonctions, systèmes et équipements d'I&C importants pour la sûreté

NOTE Ce terme est à mettre en regard de celui d'« organisation en charge de l'exploitation ».

3.38
qualification
processus déterminant si un système ou composant est apte à l'utilisation opérationnelle. La qualification est effectuée dans le contexte de la classe de sûreté particulière du système d'I&C et d'un ensemble particulier d'exigences de qualification

NOTE 1 Les exigences de qualification dérivent de la classe particulière du système d'I&C et du contexte particulier de l'application.

NOTE 2 Les systèmes d'I&C sont généralement mis en œuvre à partir d'un ensemble d'équipement interagissant. De tels équipements peuvent être développés comme une partie de projet, ou ils peuvent être des équipements préexistant (par exemple développés dans le cadre d'un projet antérieur, pour des produits commercialement disponibles). Généralement, la qualification d'un système d'I&C est réalisée par étapes: d'abord la qualification de l'équipement individuel pré existant (habituellement tôt dans le processus de réalisation du système); et plus tard la qualification du système intégré (par exemple sur la conception finale).

NOTE 3 La qualification des systèmes d'I&C est toujours une activité particulière à la centrale et à l'application. Cependant, ceci peut reposer dans une grande mesure sur des activités de qualification réalisées hors du contexte particulier à la conception d'une centrale (celles ci sont appelées « qualification générique » ou « pré qualification »). Une pré qualification peut réduire l'effort de qualification propre à la centrale, néanmoins, il convient que la démonstration de la satisfaction aux exigences de qualification particulière à l'application soit quand même faite.

3.39
qualité
niveau de satisfaction d'exigence atteint par un ensemble inhérent de caractéristiques

[ISO 9000: 2005] [6]

3.40
assurance qualité
fonction d'un système de gestion qui garantit que des prescriptions spécifiques seront respectées

[Glossaire de Sûreté de l'AIEA, Edition 2007]

NOTE Cette définition est compatible avec celle de l'ISO 8402:1994, 3.5 [7].

3.41
plan qualité
document établissant les pratiques en matière de qualité, les ressources et les séquences d'activités pertinentes à un produit, projet ou contrat particulier

3.42
redondance
mise en place de structures, systèmes ou composants (identiques ou différents) supplémentaires, afin qu'un élément quelconque puisse remplir la fonction requise indépendamment de l'état de fonctionnement ou de défaillance d'un autre élément

[Glossaire de Sûreté de l'AIEA, Edition 2007]

3.43
fiabilité
probabilité qu'un composant, un système ou une installation satisfasse aux exigences minimales de performance lorsqu'il est sollicité pour une période de temps spécifié et dans des conditions de fonctionnement données

[Glossaire de Sûreté de l'AIEA, Edition 2007, modifiée]

NOTE 1 La fiabilité d'un système programmé comprend la fiabilité de son matériel qui est généralement quantifiée et la fiabilité de son logiciel qui est généralement une mesure qualitative car il n'y a pas de moyens communément reconnus pour quantifier la fiabilité du logiciel.

NOTE 2 Cette définition diffère de celle fournit dans la Edition 2007 du Glossaire de Sûreté de l'AIEA qui est «Probabilité qu'un système ou un composant satisfasse aux exigences minimales de performance lorsqu'il est sollicité ». Les experts du SC 45A de la CEI ont indiqué que cette définition de l'AIEA n'est pas cohérente avec la pratique courante car elle ne fait pas état du concept de temps de mission.

3.44
exigence
expression dans le contenu d'un document formulant les critères à respecter afin de prétendre à la conformité avec le document, et avec lesquels aucun écart n'est permis

[Directive ISO/CEI, Partie 2, 2004, 3.12.1] [8]

NOTE 1 Dans les documents du SC 45A de la CEI on distingue les types d'exigences suivant:

Exigences de sûreté – Exigences imposées par les autorités (judiciaires, administratives ou les organisations de normalisation) et les autorités de conception en matière de sûreté de la centrale nucléaire, en ce qui concerne l'impact sur les personnes, la société et l'environnement pendant le cycle de vie de la centrale nucléaire.

Exigences fonctionnelles et de performances – Les exigences fonctionnelles indiquent les réactions du système par rapport à des conditions ou des signaux particuliers, et les exigences de performances définissent des caractéristiques telles que le temps de réponse et la précision.

Exigences opérationnelles – Exigences concernant l'aptitude et la capacité opérationnelles de la centrale imposées par le propriétaire.

Exigences de conception de la centrale – Exigences techniques portant sur la conception globale de la centrale afin de garantir le respect des exigences en matière de sûreté et les exigences opérationnelles de la centrale.

Exigences de conception du système – Exigences de conception de systèmes individuels permettant que la conception de la centrale complète satisfasse aux exigences de conception de la centrale.

Exigences de conception d'équipement – Exigences concernant un équipement individuel qui lui permettent de respecter les exigences de conception du système.

NOTE 2 Le Glossaire de Sûreté de l'AIEA, Edition 2007 contient la définition suivante:

Prescrit, prescription – Prescrit par une législation ou une réglementation (nationale ou internationale) ou par des fondements ou des prescriptions de sûreté de l'AIEA.

Cette définition AIEA utile dans le cadre des publications de l'AIEA est trop limitée pour être utilisée dans le cadre des normes techniques. Elle correspond à la définition « Exigence de sûreté » telle que fournit dans la Note 1.

NOTE 3 Il est bien entendu que tout écart par rapport à une exigence est à justifier.

3.45
logiciel réutilisable
module de logiciel pouvant être utilisé dans plusieurs programmes informatiques ou systèmes de logiciels

[IEEE 610], modifiée

3.46
groupe de sûreté
ensemble d'équipements prévus pour accomplir toutes les actions requises si un événement initiateur postulé particulier se produit afin que les limites spécifiées dans la base de conception pour les incidents de fonctionnement prévus et les accidents de dimensionnement ne soient pas dépassées

[Glossaire de Sûreté de l'AIEA, Edition 2007]

3.47
systèmes de sûreté
systèmes important pour la sûreté destinés à garantir la mise à l'arrêt sûre du réacteur ou l'évacuation de la chaleur résiduelle du cœur, ou à limiter les conséquences des incidents de fonctionnement prévus et des accidents de dimensionnement

[Glossaire de sûreté de l'AIEA, Edition 2007]

3.48
sécurité
capacité d'un système informatique à protéger les informations et les données afin que les personnes ou systèmes non autorisés ne puissent ni les lire, ni les modifier, ni qu'ils puissent passer ou inhiber des commandes et que les personnes ou systèmes autorisés puissent y accéder

[ISO 12207:2008, 4.39, modifiée] [9]

3.49
défaillance unique
perte de la capacité d'un composant à remplir sa (ses) fonction(s) de sûreté prévue(s) et toute autre défaillance qui peut en résulter

[Glossaire de sûreté de l'AIEA, Edition 2007, modifiée]

NOTE Cette définition diffère de celle fournit dans le Glossaire de Sûreté de l'AIEA édition 2007 et qui est «Défaillance qui rend un système ou un composant impropre à remplir sa (ses) fonction(s) de sûreté prévue(s) et toute autre défaillance qui peut en résulter ». Le mot « système » à été supprimé de la définition originale de l'AIEA car sa présence a été jugée inappropriée par les experts du SC 45A de la CEI du fait que cela suppose la perte de fonction système. Les systèmes qui satisferait au critère de défaillance unique ne devraient ainsi pas pouvoir présenter de défaillances uniques. Il semble que cela puisse amener à entrer dans des discussions sans fin concernant la conformité au critère de défaillance unique. De plus cette définition modifiée de l'AIEA est cohérente avec la définition de « défaillance » du SC 45A de la CEI.

3.50
critère de défaillance unique
critère (ou contrainte) appliqué à un système, en vertu duquel ce dernier doit être capable de remplir sa (ses) fonctions en cas de défaillance unique

[Glossaire de Sûreté de l'AIEA, Edition 2007]

NOTE Voir l'article 5.37 du document AIEA NS-R-1:2000, comme recommandation sur la façon de satisfaire au critère de défaillance unique et sur son application à un groupe de sûreté.

3.51
logiciel
programmes (ensembles ordonnés d'instructions), données, règles et toute documentation associée relatifs au fonctionnement d'un système d'I&C programmé

3.52
défaillance logicielle
défaillance du système due à l'activation d'un défaut de conception dans un composant logiciel

NOTE 1 Toutes les défaillances logicielles sont dues à des défauts de conception, dans la mesure où un logiciel n'est défini que par sa conception et ne fait l'objet d'aucune usure, ni ne souffre d'aucune défaillance physique. Les commandes qui activent les défauts du logiciel se présentant d'une manière aléatoire pendant le fonctionnement du système, les défaillances du logiciel se produisent également d'une manière aléatoire.

NOTE 2 Voir aussi « défaillance », « défaut », « défaut logiciel ».

3.53
défaut logiciel
défaut de conception situé dans un composant logiciel

NOTE Voir aussi « défaut ».

3.54
fiabilité logicielle
composante de la fiabilité du système qui dépend des défaillances logicielles

3.55
spécification
document qui spécifie de manière complète, précise et vérifiable les exigences, le comportement de la conception ou autres caractéristiques d'un système ou composant et, souvent, les procédures permettant de déterminer si ces dispositions ont été satisfaites

[CEI 60880:2006, 3.39]

3.56
système
ensemble de composants qui interagissent conformément à une conception donnée, un élément d'un système pouvant être un autre système, appelé sous-système

[CEI 61508-4:2010, 3.3.1, modifiée]

NOTE 1 Voir également « système d'I&C ».

NOTE 2 Les systèmes d'I&C se distinguent des systèmes mécaniques et électriques d'une centrale nucléaire.

NOTE 3 Cette définition du SC 45A de la CEI est totalement compatible avec la sous-définition de « système » donnée dans la définition de « SCC Systèmes, Structures et Composants » de la Edition 2007 du Glossaire de Sûreté de l'AIEA.

3.57
cycle de vie de sûreté du système
activités nécessaires à la mise en œuvre d'un système d'I&C important pour la sûreté. Elles ont lieu entre la spécification des exigences du système (lors de la phase de conception) et le retrait du service du système d'I&C

NOTE 1 Le cycle de sûreté du système fait référence aux activités du cycle de sûreté global d'I&C.

NOTE 2 Voir aussi "cycle de vie de sûreté de l'ensemble de l'I&C".

3.58
logiciel système
logiciel conçu pour un système programmé particulier ou pour une famille de systèmes programmés afin de faciliter le développement, le fonctionnement et la maintenance de ces systèmes et des programmes connexes. Le logiciel système est généralement composé de logiciels opérationnels et de logiciels de soutien

NOTE 1 Logiciels opérationnels: logiciels fonctionnant sur le processeur cible pendant le fonctionnement du système. Par exemple:le système d'exploitation, les gestionnaires d'entrée/sortie, gestion des interruptions, programmateur, gestionnaires de communication, bibliothèques d'application, diagnostic en ligne, gestion de la redondance et de la dégradation progressive.

NOTE 2 Logiciels de soutien: logiciels d'aide au développement, aux essais ou à la maintenance des autres logiciels tels que les compilateurs, les générateurs de codes, les simulateurs, le diagnostic hors-ligne, les programmes d'initialisation, les outils, etc.

NOTE 3 Voir également « logiciel d'application ».

NOTE 4 Voir aussi la Figure 2.

3.59
validation système
confirmation par examen et apport d'autres éléments justificatifs qu'un système satisfait à la totalité des exigences spécifiées (fonctionnalités, temps de réponse, tolérance aux fautes, robustesse)

[CEI 60880:2006, 3.42]

NOTE L'édition 2007 du Glossaire de Sûreté de l'AIEA donne les deux définitions suivantes:

> *Validation*: Processus visant à déterminer si un produit ou un service est capable de remplir sa fonction prévue de façon satisfaisante. Validation est d'application plus large que vérification et peut impliquer un élément d'appréciation plus important.
>
> *Validation du système informatique*: Processus consistant à tester et évaluer le système informatique intégré (matériel et logiciel) afin de garantir sa conformité par rapport aux exigences fonctionnelles, aux exigences relatives aux performances et à celles concernant les interfaces.

Tout d'abord cette définition de « validation système » est un cas particulier de validation. Il fait référence à un produit particulier, à savoir un système d'I&C, ce qui est cohérent avec la définition de l'AIEA. Ensuite, la définition CEI précise la référence de validation, à savoir les spécifications d'exigences alors que la définition de l'AIEA ne fait que référence à « la fonction prévue ».

3.60
défaut systématique
défaut relié de façon déterministe à une certaine cause, ne pouvant être éliminé que par une modification de la conception, du processus de fabrication, des procédures d'exploitation, de la documentation ou d'autres facteurs appropriés

[CEI 61508-4:2010, 3.3.6, modifiée]

3.61
essai de type
essai de conformité effectué sur une ou plusieurs entités représentatives de la production

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

3.62
vérification
confirmation par examen et apport d'éléments objectifs que les résultats d'une activité sont conformes aux objectifs et exigences établis pour cette activité

[CEI 62138:2004, 3.35]

NOTE L'édition 2007 du Glossaire de Sûreté de l'AIEA donne les deux définitions suivantes:

Validation: Processus visant à déterminer si un produit ou un service est capable de remplir sa fonction prévue de façon satisfaisante. Validation est d'application plus large que vérification et peut impliquer un élément d'appréciation plus important.

Vérification: Processus visant à déterminer si la qualité ou les performances d'un produit ou d'un service sont conformes à celles indiquées, voulues ou nécessaires.

La définition de l'AIEA pour la « vérification » est très proche de celle de la « validation », et les deux s'intéressent au produit final ou au service.

Dans les normes du SC 45A de la CEI, les termes « vérification » et « validation » font référence à des résultats provenant du cycle de vie de produits particuliers, à savoir les équipements et les systèmes d'I&C, mais en général pas à des services.

D'autre part, les termes «vérification » et « validation » sont utilisés pour identifier deux types d'évaluations différentes et complémentaires:

« *Vérification* » fait référence à une évaluation d'une activité individuelle par rapport à ses entrées.

« *Validation* » fait référence à une évaluation du produit final par rapport à ses objectifs et ses exigences documentés.

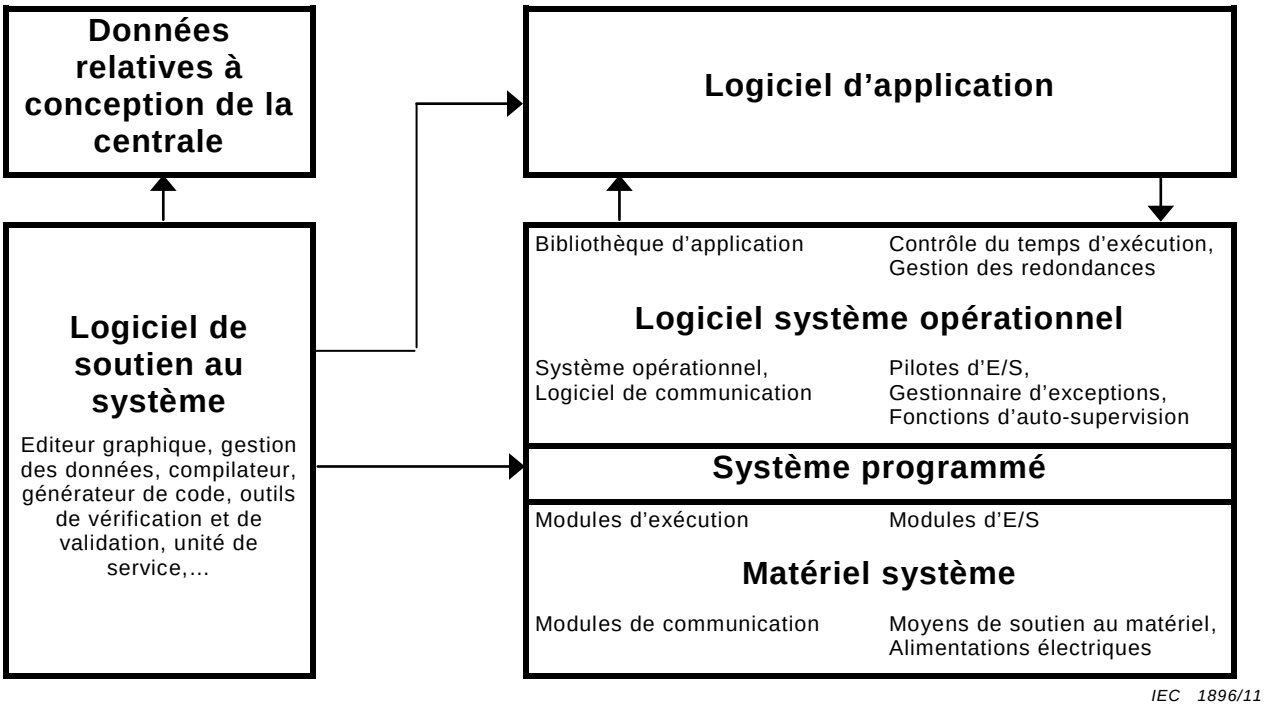


Figure 2 – Relations types entre logiciel et matériel d'un système programmé

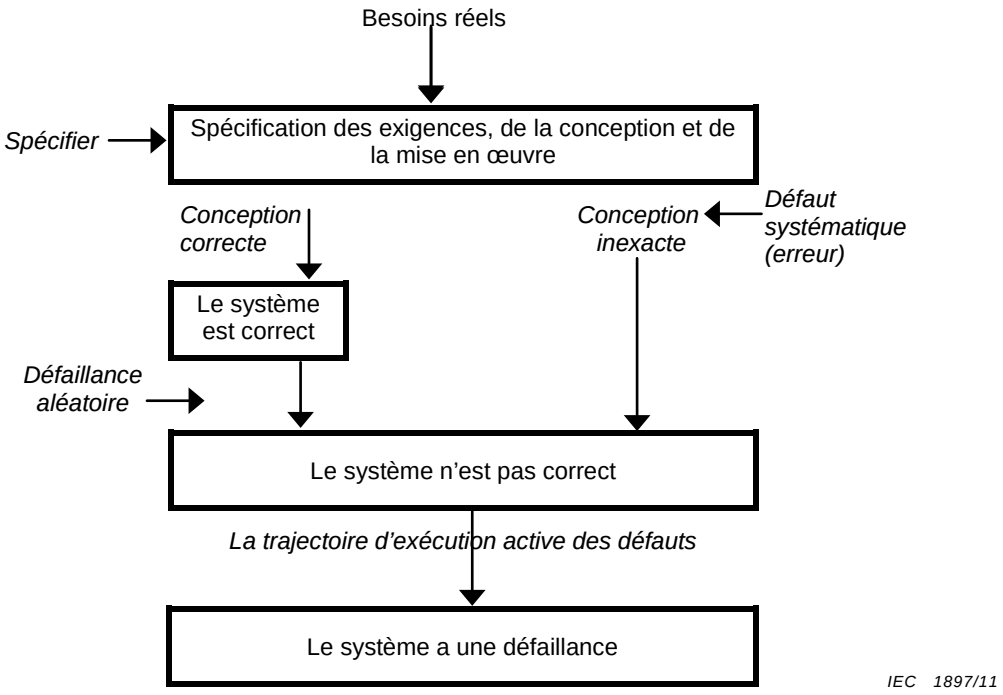


Figure 3 – Relations entre défaillance, défaillance aléatoire et défaut systématique

4 Symboles et abréviations

ASIC	Application-specific integrated circuit
CB	Programmé
DCC	Défaillance de cause commune
GC	Gestion des configurations
COTS	Composants sur étagère du commerce
IEM	Interférence electro magnétique
FPGA	Field-programmable gate array
IHM	Interface homme – machine
I&C	Instrumentation et contrôle commande
E/S	Entrée/sortie
CNP	Centrale nucléaire de puissance
LPD	Logiciel prédéveloppé
EIP	Evénement initiateur postulé
AQ	Assurance qualité

5 Cycle de vie de sûreté de l'ensemble de l'I&C

5.1 Généralités

L'objectif de cet article est de définir la manière permettant de

- déduire les exigences relatives à l'architecture des systèmes I&C importants pour la sûreté à partir de la conception de sûreté du CNP (voir Articles A.2 et A.3), et
- déduire les exigences relatives aux systèmes individuels d'I&C importants pour la sûreté de ces exigences d'ensemble.

Afin d'assurer que toutes les exigences relatives à la sûreté de la centrale et concernant l'I&C sont prises en compte, mises en œuvre et maintenues, une approche systématique est nécessaire. A cet effet, les activités liées au développement, à la mise en œuvre et au fonctionnement de l'I&C sont introduites dans un cycle de vie de sûreté de l'ensemble de l'I&C. Ce cycle de vie fait référence, à son tour, aux cycles de vie de sûreté des systèmes individuels d'I&C (voir l'Article 6).

Les phases du cycle de vie de sûreté de l'ensemble de l'I&C comprennent généralement

a) la revue de la conception de sûreté de la centrale, et en particulier (5.2):
   - les exigences de fonctionnalité, de performance et d'indépendance;
   - les exigences relatives à la catégorisation;
   - les contraintes issues du cadre général de conception de la centrale;
b) la définition de la spécification des exigences globales relatives aux fonctions, systèmes et équipements d'I&C importants pour la sûreté (5.3);
c) la conception de l'architecture d'ensemble de l'I&C et l'affectation des fonctions d'I&C aux systèmes et équipements (5.4);
d) la définition de la planification globale (5.5);
e) la réalisation des systèmes individuels (Article 6);
f) lintégration et la mise en service de l'ensemble des systèmes (Article 7);
g) l'exploitation et la maintenance d'ensemble (Article 8);

Les chiffres entre parenthèses identifient les paragraphes ou articles de la présente norme dans lesquels les phases sont traitées. L'objectif, les entrées, sorties et domaines d'application de chaque phase sont développés dans le Tableau 1.

Les liens entre ce cycle de vie de sûreté de l'ensemble de l'I&C et les cycles de vie de sûreté des systèmes d'I&C sont représentés de manière simplifiée sur la Figure 4.

a) le cycle de vie de sûreté de l'ensemble de l'I&C est un processus itératif. Les sorties de chaque phase doivent être vérifiées comme étant cohérentes avec les entrées issues des activités précédentes. Une phase peut débuter même si les activités de la précédente ne sont pas terminées, sous réserve de la mise en place de moyens de contrôle adéquats pour conserver la cohérence du déroulement du cycle;

b) une phase ne peut être terminée qu'après l'achèvement des phases précédentes.

Tableau 1 – Vue d'ensemble du cycle de vie de sûreté de l'ensemble de l'I&C

Article ou paragraphe	Entrées	Objectifs de l'activité	Domaine d'application	Sorties
5 Exigences relatives au cycle de vie de sûreté de l'ensemble de l'I&C et relations avec les cycles de vie sûreté des systèmes				
5.2	*Elaboration des exigences relatives à l'I&C à partir de la conception de sûreté de la centrale*			
5.2.2 Revue des exigences de fonctionnalité, de performance et d'indépendance	Documents de conception de sûreté de la centrale Principes d'exploitation de la centrale	Identifier: – les exigences de fonctionnalité et de performance des systèmes d'I&C importants pour la sûreté, – les concepts de défense en profondeur de la centrale et les exigences d'indépendance imposées aux fonctions d'I&C, – les fonctions automatiques et les tâches de l'opérateur	Systèmes de la centrale et systèmes d'I&C associés importants pour la sûreté	Identification des exigences relatives aux entrées de 5.3
5.2.3 Revue des exigences de catégorisation	Catégorisation de sûreté de la centrale	Identifier la catégorisation des fonctions d'I&C Vérifier leur exhaustivité Vérifier la faisabilité des exigences complexes	Fonctions d'I&C importantes pour la sûreté	Identification des exigences relatives aux entrées de 5.3
5.2.4 Revues des contraintes de la centrale	Documents relatifs aux plans et schémas de la centrale et base de données de conception de la centrale	Identifier: – les limites des systèmes d'I&C par rapport au reste de la centrale, – les contraintes provenant des systèmes de soutien, de la disposition des composants de la centrale et de l'environnement, – les sources potentielles de phénomènes internes et externes dangereux, – les modalités d'exploitation et de maintenance de la centrale	Implantation dans la centrale Systèmes de la centrale Systèmes d'I&C	Identification des contraintes pour la conception de l'architecture (5.4) et pour la spécification des exigences relatives aux systèmes individuels d'I&C (6.2)
5.3 Documentation produite	Sorties de 5.2	Développer la spécification des exigences globales relatives aux systèmes I&C importants pour la sûreté en termes d'exigences de fonctionnalité, performance, indépendance et catégorisation	Systèmes d'I&C	Spécification des exigences relatives à l'ensemble de l'I&C pour 5.4
5.4 *Conception de l'architecture d'ensemble de l'I&C et affectation des fonctions d'I&C*				
5.4.2 Conception de l'architecture d'I&C	Sorties de 5.3	Concevoir une architecture d'ensemble de l'I&C convenable afin de mettre en œuvre les spécifications des exigences relatives aux systèmes I&C importants pour la sûreté Concevoir des mesures adéquates contre les DCC potentielles	Fonctions d'I&C et systèmes d'I&C	Conception détaillée de l'architecture d'I&C en termes de systèmes automatiques, IHM et interconnexions (voir 5.6.2)
5.4.3 Affectation des fonctions	Sorties de 5.4.2 et 5.5 (Itération avec les sorties de 6.4)	Affecter les fonctions d'I&C aux systèmes et équipements d'I&C individuels Concevoir des exigences (limites, classement, fonctionnalité, fiabilité et autres propriétés requises) pour les systèmes individuels d'I&C	Fonctions d'I&C et systèmes d'I&C	Exigences relatives aux fonctions d'application des systèmes et de l'IHM, à la conception des systèmes d'I&C et aux outils (voir 5.6.3)

Article ou paragraphe	Entrées	Objectifs de l'activité	Domaine d'application	Sorties
5.4.4 Analyses requises	Sorties de 5.4.2 et 5.4.3	Evaluer la défense contre les DCC Evaluer les facteurs humains.	Fonctions d'I&C et systèmes d'I&C	Evaluation de la fiabilité et de la défense contre les DCC (voir 5.4.4.2) Evaluation des facteurs humains (voir 5.4.4.3)
5.5 Planification globale	Sortie de 5.4	Développer des plans d'AQ, de sécurité, d'intégration, de mise en service, d'exploitation et de maintenance	Systèmes d'I&C reliés dans leur fonctionnement	Plans pour les activités désignées
6 Réalisation des systèmes	Sorties de 5.6	Spécifier et créer des systèmes d'I&C conformes à la spécification de l'architecture de l'&C (voir Article 6)	Systèmes individuels d'I&C	Les sorties sont décrites dans le Tableau 3
7 Intégration et mise en service globales	Sortie de 5.5.4 et 6.3.6	Tester et mettre en service les systèmes interconnectés de l'architecture d'I&C	Systèmes d'I&C de l'architecture d'I&C	Systèmes intégrés et mis en service Rapport de mise en service (voir 7.3)
8 Exploitation et maintenance globales	Sortie de 5.5.5, 5.5.6 et 7.2	Exploiter, entretenir et réparer les systèmes afin de maintenir le niveau de sûreté	Systèmes d'I&C de l'architecture d'I&C	Exécution des fonctions Registres de fonctionnement et de maintenance (voir 8.3)
NOTE Pour une comparaison de cette définition des phases avec celle de la CEI 61508-1, voir l'Annexe D.				

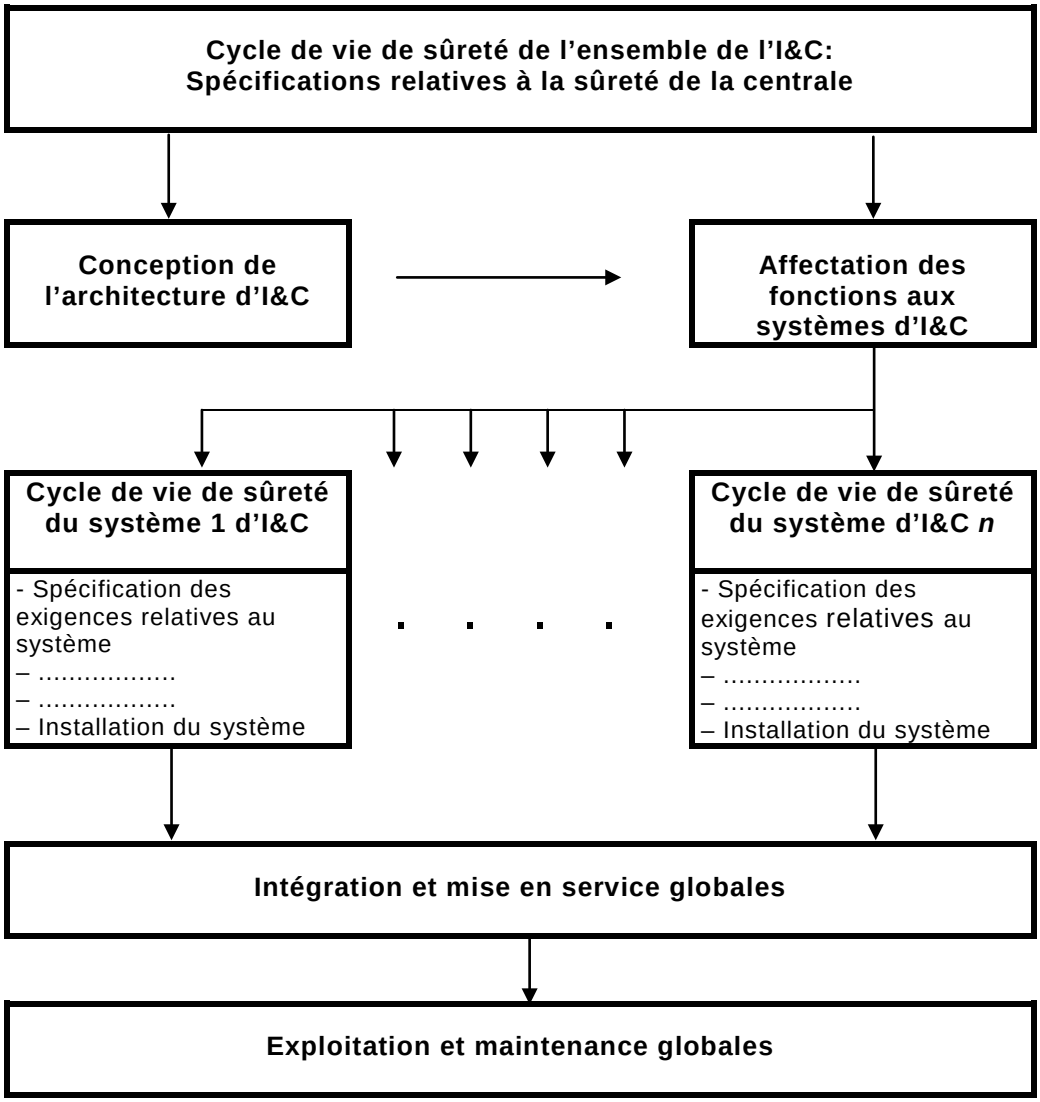


Figure 4 – Liens entre le cycle de vie de sûreté de l'ensemble de l'I&C et les cycles de vie de sûreté des systèmes individuels d'I&C

5.2 Elaboration des exigences portant sur l'I&C à partir de la base de conception de sûreté de la centrale

5.2.1 Généralités

L'objectif des exigences du présent paragraphe est d'identifier les exigences devant être prises en compte lors de la spécification des systèmes d'I&C, et les contraintes d'architecture d'I&C, à partir des bases de conception de sûreté de la centrale et du cadre général de conception de la centrale.

Le document AIEA 75-INSAG-3 définit un certain nombre de « principes de sûreté » qui forment une «approche intégrée de la sûreté» garantissant la sûreté d'une centrale nucléaire. Ces principes seront utilisés dans la conception (voir AIEA NS-R-1), en tenant compte de tous les «événements initiateurs postulés» (EIP) pertinents et de toutes les barrières physiques successives, afin de maintenir l'exposition aux rayonnements des employés, du public et de l'environnement dans certaines limites (voir Articles A.2, A.3 et A.4). Dans cette approche, la conception de la centrale spécifie le niveau de qualité requis pour les fonctions et systèmes de la centrale nécessaires pour le maintien de celle-ci dans un état opérationnel

normal, pour garantir une réponse correcte à tous les EIP et pour faciliter la gestion à long terme de la centrale suite à un accident.

5.2.2 Revue des exigences de fonctionnalité, de performance et d'indépendance

Les exigences de fonctionnalité, de performance et d'indépendance relatives aux fonctions d'I&C importantes pour la sûreté ainsi que les principes d'exploitation de la centrale sont définis dans la base de conception de sûreté de la centrale. Cette base de conception est un élément fondamental de la conception d'ensemble de l'I&C. Les exigences relatives aux interactions homme–machine prennent en compte les principes d'exploitation et des considérations ergonomiques, afin de minimiser les défaillances dues aux facteurs humains.

Le processus de conception de l'I&C a besoin des données d'entrée suivantes qui proviennent de la base de conception de sûreté de la centrale:

- les principes de défense en profondeur de la centrale (voir Article A.4) et les groupes de fonctions prévus pour faire face aux séquences d'EIP et remplir les objectifs de sûreté (voir Article A.3),

  NOTE 1 Si la fiabilité d'une fonction doit être d'un niveau très élevé, la spécification des exigences portant sur la centrale et sur l'I&C stipule différentes lignes de défense pour le même EIP, par exemple au moins deux critères de déclenchement indépendants et fonctionnellement différents et, si nécessaire, un second système mécanique redondant, indépendant et fonctionnellement différent, pour le contrôle des accidents.

  NOTE 2 Les échelons de défense en profondeur peuvent contenir les fonctions importantes pour la sûreté ainsi que d'autres fonctions. Les exigences de la présente norme ne concernent que les fonctions importantes pour la sûreté.

- les exigences de fonctionnalité et de performance relatives aux fonctions de la centrale importantes pour la sûreté et nécessaires pour répondre aux exigences de sûreté globale (voir Article A.4);

  NOTE 3 Lorsqu'une validation fonctionnelle est requise (voir 6.2.4.2), la conception de la centrale fournit les conditions initiales, les limites admissibles et le taux admissible de variation des variables de la centrale devant être contrôlées par les systèmes d'I&C importants pour la sûreté.

- le rôle des automatismes et les actions requises de l'opérateur pour gérer les incidents opérationnels hypothétiques et les situations accidentelles (voir Article A.4);
- une analyse des tâches conformément au 6.3 de la CEI 60964:2009 définissant les fonctions qu'il convient d'affecter à l'opérateur et celles qu'il convient d'affecter aux machines;
- les variables à afficher pour l'opérateur en cas d'actions de contrôle-commande manuelles;
- les principes de priorité entre actions automatiques et manuelles, en tenant compte des catégories des fonctions, des salles de commande ou des lieux où elles se trouvent.

5.2.3 Revue des exigences de catégorisation

5.2.3.1 Hypothèses de la présente norme concernant la catégorisation des fonctions et le classement des systèmes

Les fonctions, systèmes et équipements de la centrale sont classés selon leur degré d'importance pour la sûreté. La présente norme fait la distinction entre la catégorisation des fonctions d'I&C et le classement des systèmes d'I&C, conformément à la CEI 61226.

NOTE 1 Les termes « catégorisation » et « classement » sont parfois confondus, et ceci même dans la CEI 61226. Dans un but de clarté dans la présente norme, le terme « catégorisation » est réservé aux fonctions et celui de « classement » aux systèmes.

Une fonction d'I&C est affectée par le processus de catégorisation à une catégorie selon son degré d'importance pour la sûreté.

Les catégories sont définies par un ensemble d'exigences relatives à la spécification, à la conception, à l'intégration, à la vérification et à la validation de la fonction d'I&C, ainsi que par

des exigences portant sur les propriétés devant être satisfaites par les systèmes adaptés pour les catégories, leur qualification, les fonctions d'application, les fonctions de service et les fonctions logiciel système du système, telles qu'appropriées. Des exigences consistantes s'appliquent à l'ensemble des éléments nécessaires à la réalisation de la fonction d'une catégorie donnée, indépendamment de la façon suivant laquelle elle est répartie dans un réseau de systèmes d'I&C interconnectés. Ainsi, il est pratique de définir des classes de systèmes d'I&C qui sont appropriées pour supporter des fonctions d'I&C jusqu'à une certaine catégorie.

La catégorisation des fonctions d'I&C fait partie de la base de conception de sûreté de la centrale et sort du cadre de la présente norme. La présente norme suppose que la base de conception de sûreté de la centrale a réparti les fonctions d'I&C individuelles importantes pour la sûreté dans une des trois catégories, A, B et C et que les principales exigences de conception pour les systèmes et équipements associés à ces catégories sont conformes à celles de l'Article 7 de la CEI 61226:2009. De plus, les exigences relatives à la catégorie A sont conformes à celles requises par l'AIEA pour les systèmes de sûreté.

NOTE 2 Les références normatives de catégorisation peuvent varier selon les pays et s'écarter de la référence utilisée dans la présente norme (CEI 61226). Une situation particulière peut aussi survenir lorsqu'on applique une norme à une centrale existante pour laquelle les nouvelles exigences de catégorisation ne sont valables que pour une partie de l'étendue du projet de modernisation. Dans un tel cas, une analyse particulière peut être nécessaire pour identifier les exigences minimums devant être satisfaites par les classes de système.

Le classement des systèmes d'I&C est défini par l'organisation en charge du projet de l'I&C pendant la phase de conception de l'architecture d'I&C, avant l'affectation des fonctions d'I&C aux systèmes (voir 5.4.2 et 5.4.3).

5.2.3.2 Exigences

a) La catégorisation des fonctions d'I&C doit être indiquée dans la base de conception de sûreté de la centrale et doit servir de référence pour la spécification des exigences d'ensemble de I&C (voir 5.3).

b) L'organisation en charge du projet d'I&C doit effectuer une revue de la catégorisation et la vérifier au niveau exhaustivité et faisabilité. En cas de non faisabilité (par exemple affectation de la catégorie maximale à une fonction qui ne satisfait pas au critère de défaillance unique du fait de la conception de la centrale) la définition ou la catégorisation des fonctions d'I&C doit être revue par rapport aux exigences fonctionnelles de l'I&C de la centrale. Les exigences fonctionnelles et leur catégorisation associée doivent être l'objet d'itérations jusqu'à ce qu'une solution réalisable soit trouvée.

5.2.4 Revue des contraintes de la centrale

La conception de l'architecture d'I&C (voir 5.4) est sujette à des contraintes imposées par le cadre général de conception de la centrale.

a) L'organisation en charge du projet d'I&C doit identifier les contraintes imposées aux équipements d'I&C par l'organisation de la centrale, les interfaces avec les équipements de la centrale et les événements externes à l'I&C, en particulier

- les limites entre les systèmes et équipements d'I&C d'une part et les systèmes de la centrale d'autre part, y compris les interfaces avec les systèmes de mise en marche électriques/mécaniques et les systèmes auxiliaires tels que les alimentations électriques et les systèmes de conditionnement de l'air;
- les plages d'évolution des régimes transitoires et permanents des paramètres environnementaux, dans les situations normales, anormales et accidentelles pour lesquelles le fonctionnement des systèmes d'I&C est requis;
- les plages d'évolution des régimes transitoires et permanents des alimentations de motricité et de commande, dans les situations normales, anormales et accidentelles de pour lesquelles le fonctionnement des systèmes d'I&C est requis;
- les contraintes générales portant sur l'installation et le cheminement des câbles;

- les contraintes spécifiques portant sur l'installation et le cheminement des câbles vers les points de convergence, tels que la salle de commande et les salles de regroupement de câbles;
- les contraintes portant sur la mise à la terre et sur la distribution de l'alimentation électrique;
- les événements dangereux internes et externes à prendre en considération en fonction des hypothèses prises au niveau de la centrale; ce qui comprend, les incendies, les inondations, le gel, la foudre, la surtension, l'interférence électromagnétique, les tremblements de terre, les explosions ou les effets chimiques.

b) L'organisation en charge du projet d'I&C doit identifier les contraintes imposées aux équipements d'I&C issues des principes d'exploitation, c'est-à-dire les contraintes résultant de

- la sécurité;
- l'exploitation et de la maintenance (voir 5.6 de CEI 60964:2009);
- « la maintenance en service » des systèmes d'I&C.

Généralement, cela amène des exigences complémentaires qui vont structurer la division de l'architecture d'I&C en sous-systèmes séparés. Les points les suivants sont à prendre en compte:

- la centrale est généralement divisée en systèmes de tranche distincts, qui sont groupés en lots de façon à organiser les activités d'ingénierie, d'installation, de mise en service et d'essais. Il convient que la division des systèmes d'I&C prenne en compte ce découpage;
- il convient que la planification optimale des travaux de maintenance, des essais périodiques et des activités relatives aux modifications soit possible pour un ensemble de sous-systèmes d'I&C et de la centrale choisi, tandis que les autres sous-systèmes restent pleinement opérationnels;
- il convient que l'impact du partage et de la répartition des responsabilités des personnels d'exploitation soit pris en compte lors de la division des systèmes d'I&C;
- il convient d'identifier les exigences portant sur les outils et stations de travail de service destinés à la maintenance et aux activités de diagnostique; ce qui couvre les interfaces avec les systèmes d'ingénierie. Ceci peut comprendre des exigences portant sur les interfaces homme-machine pour le personnel de maintenance, sur les interfaces avec les moyens de gestion centralisés de la tranche, etc.

5.3 Documentation produite

Les documents produits par l'activité décrite en 5.2 sont les spécifications d'exigences de chaque système d'I&C important pour la sûreté.

NOTE 1 Les spécifications d'exigences couvrent la fonction d'I&C dans sa totalité, c'est-à-dire depuis les entrées (capteurs, opérateurs et autres équipements) jusqu'aux sorties (dirigées vers les actionneurs, opérateurs ou autres équipements). Une répartition ultérieure plus fine de ces exigences permettra de spécifier les exigences relatives aux sous-fonctions associées aux systèmes individuels d'I&C. Ceci dépendra de l'architecture d'I&C choisie (voir 5.4) et de la manière dont les fonctions sont réparties sur les équipements (instrumentation, automates et actionneurs).

a) Une spécification des exigences doit être établie pour chaque fonction d'I&C. Elle doit contenir:

1) une spécification des exigences de fonctionnalité définissant la manière dont la fonction transforme les informations d'entrée en informations de sortie afin d'exploiter et de surveiller la centrale;
2) une spécification des exigences de performance définissant le domaine de valeur, la précision et la performance dynamique de la fonction;

NOTE 2 Ceci comprend les exigences relatives au comportement temporel qui peuvent avoir été omises dans le passé pour les systèmes traditionnels câblés.

3) la spécification de la catégorie de la fonction.

NOTE 3 La catégorie de la fonction définit implicitement le classement minimal des systèmes d'I&C réalisant la fonction (voir Tableau 2).

b) La spécification des exigences d'ensemble doit définir toutes les relations de dépendances entre fonctions qui induisent les contraintes relatives à l'affectation des fonctions aux systèmes d'I&C. Ceci inclut:

1) les associations de fonctions à surveiller pour commander les mesures de protection,

2) les associations de fonctions assurant la défense en profondeur,

3) l'association de fonctions qui constituent un groupe de sûreté.

c) Les spécification des exigences relatives à toutes les fonctions d'I&C doivent être vérifiées afin de s'assurer qu'un ensemble de contraintes et de fonctions complet et consistant est défini pour permettre l'affectation des fonctions aux systèmes et la production de la spécification de ces systèmes (voir 6.2).

NOTE 4 En débutant la préparation de la spécification des exigences pour une fonction d'I&C, il peut arriver que l'ensemble des capteurs ou des actionneurs liés à la fonction n'ait pas été encore complètement déterminé. Il sera alors nécessaire de compléter ultérieurement la spécification pour que tous les capteurs et les actionneurs soient pris en compte. De la même façon le contrôle commande associé à n'importe quel actionneur supplémentaire qui n'aurait pas été initialement pris en compte, a besoin d'être évalué et correctement catégorisé. Il est possible de réaliser cela au niveau d'itérations associées à la spécification des exigences.

5.4 Conception de l'architecture d'ensemble d'I&C et affectation des fonctions d'I&C

5.4.1 Généralités

Le présent paragraphe décrit la manière dont

- les contraintes de 5.2.4 et les exigences de 5.3 s'appliquent à la conception de l'architecture d'ensemble des systèmes d'I&C importants pour la sûreté (en abrégé architecture d'I&C);
- les fonctions d'I&C sont affectées aux systèmes individuels d'I&C.

5.4.2 Conception de l'architecture d'I&C

5.4.2.1 Généralités

La conception de l'architecture d'I&C fournit une description de haut niveau des systèmes d'I&C de la centrale nucléaire, de la communication entre ces systèmes et des outils nécessaires pour assurer une interface consistante entre ces systèmes.

5.4.2.2 Exigences générales

a) La conception de l'architecture d'I&C doit englober la totalité de l'I&C nécessaire à la mise en œuvre des fonctions d'I&C importantes pour la sûreté spécifiées en 5.3.

b) La conception de l'architecture d'I&C doit décomposer la totalité de l'I&C en systèmes et composants avec une granularité suffisante pour garantir le respect des exigences relatives

- à l'indépendance des fonctions réparties dans les différentes lignes de défense,
- à la séparation appropriée des systèmes de classes différentes,
- à la satisfaction des contraintes portant sur la séparation physique et l'isolement électrique résultant des contraintes d'environnement et d'implantation de la centrale, de l'analyse des risques et des contraintes relatives aux activités de démarrage, d'essais, de maintenance et d'exploitation (voir 5.2.4).

c) La conception de l'architecture d'I&C doit garantir qu'on dispose d'un nombre suffisant de systèmes et sous-système pour que le critère de défaillance unique soit vérifié pour les fonctions de catégorie A, dans toutes les configurations possibles des systèmes et de la centrale (voir 4.17 – 4.21 de l'AIEA NS-G-1.3:2005).

d) Chaque système d'I&C doit être classé en fonction de sa capacité à réaliser des fonctions d'I&C jusqu'à une certaine catégorie.

Tableau 2 – Corrélation entre les classes des systèmes d'I&C et les catégories des fonctions d'I&C

Catégories de fonctions d'I&C importantes pour la sûreté			Classes correspondantes des systèmes d'I&C importants pour la sûreté
A	(B)	(C)	1
	B	(C)	2
		C	*3*
NOTE Un cas particulier est discuté au niveau du 7.3.2.1 de la CEI 61226:2009.			

e) Les interfaces avec la centrale et les interconnexions entre les systèmes d'I&C doivent être définies dans le cadre de la conception de l'architecture afin d'identifier

- le partage de signaux (de mesure) par différentes fonctions importantes pour la sûreté,
- le vote entre les signaux de commande provenant de différents systèmes, et les priorités entre ces signaux,
- les chemins des signaux et les équipements communs aux fonctions d'activation manuelles ou automatiques dans les différentes lignes de défense.

f) La description des systèmes, équipements et de leurs interconnexions dans la conception de l'architecture d'I&C doit être suffisamment détaillée pour permettre l'analyse des questions de sûreté relatives à l'I&C

5.4.2.3 Interfaces homme–machine

a) La conception de l'architecture d'I&C doit structurer les systèmes d'IHM des diverses zones de commande et de surveillance de la centrale, en particulier la salle de commande principale, les salles de commande complémentaires, les panneaux de commande locale et le centre de crise, avec le degré de redondance et l'ergonomie nécessaire pour prendre en compte les contraintes liées à l'exploitation et à la maintenance de la centrale (voir 5.2.4).

b) La conception de l'architecture d'I&C doit répondre aux principes d'exploitation de la centrale définis au niveau de la conception de la centrale (voir 5.2.2) et en particulier aux:

- principes de priorité entre les signaux automatiques et les signaux de commande manuels;
- principes de priorité entre les différents systèmes d'IHM pendant l'exploitation normale accidentelle et post accidentelle;
- principes de priorité entre les systèmes d'IHM normaux et de secours;
- principes relatifs aux conditions de basculement entre les systèmes d'IHM normaux et de secours.

c) La conception de l'architecture doit définir la manière dont les défauts ou défaillances détectées par les outils de diagnostique des systèmes sont présentés à l'opérateur de la centrale. La forme de la présentation doit être telle que l'opérateur puisse:

- immédiatement reconnaître la signalisation d'une défaillance et la distinguer des autres signalisations opérationnelles,
- décider de l'opportunité d'intervenir manuellement au niveau contrôle-commande afin de restaurer l'état sûr de la centrale,
- identifier les systèmes cause pour le personnel de maintenance concerné.

NOTE 1 Les interventions manuelles au niveau contrôle-commande sont supposées être réalisées à partir des moyens de commande et d'affichage d'information prévus. Les interventions directes dans les équipements d'I&C, par exemple par injection sur les broches de signaux simulés ou par débranchement de câbles ne sont pas considérées ici.

d) On doit démontrer la cohérence de la conception de l'architecture d'I&C avec les principales décisions concernant la technologie des systèmes d'IHM (par exemple informatisée ou traditionnelle). Il convient que des systèmes plus complexes soient utilisés pour la présentation des informations aux opérateurs de la centrale si cela réduit la contribution des facteurs humains aux défaillances à la demande et si cela peut être réduit par une amélioration des informations. Il convient de considérer la possibilité de DCC d'un système d'information de technologie informatique par rapport aux possibilités de défaillances dues aux facteurs humains.

e) La conception de l'architecture d'I&C doit

- affecter les fonctions à un contrôle automatique ou humain, en accord avec l'analyse des tâches de la conception de la centrale (voir 5.2.2),
- déterminer les capacités de traitement des systèmes d'I&C nécessaires au traitement des informations ainsi que leurs capacités nécessaires à la réalisation des tâches prévues pour les interactions avec l'opérateur (voir 6.3.3 de la CEI 60964:2009),
- assurer que les informations, les caractéristiques de l'IHM et le temps dont dispose l'opérateur pour une action manuelle s'accordent avec les exigences de conception de la centrale (voir 5.2.2).

f) Les techniques relatives aux facteurs humains basées sur la CEI 60964 et CEI 60965 doivent être utilisées pour garantir l'efficacité des IHM dans la conception de la salle de commande principale et des autres zones de commande de la centrale.

NOTE 2 Les tâches opérateurs associées et leurs performances sont des points de départ pour les analyses orientées facteurs humains, permettant d'intégrer correctement les affichages et les commandes, et ceci en particulier pour les tâches devant être réalisées fréquemment, avec une contrainte de temps ou avec une augmentation des risques en cas d'erreur humaine.

g) Les tâches de l'opérateur et l'optimisation des exigences relatives aux IHM, pour les tâches importantes et non importantes pour la sûreté, doivent être prises en compte dans l'analyse de la conception.

5.4.2.4 Communication de données

Les communications de données entre les systèmes constituant l'architecture d'I&C incluent toutes les liaisons prévues pour transmettre, un ou plusieurs signaux ou messages, via un ou plusieurs chemins utilisant les techniques de communication de données en série.

a) Les liaisons de communications doivent être capables de satisfaire aux spécifications des exigences de performance d'ensemble (voir 5.3) dans toutes les conditions d'exploitation de la centrale.

b) L'architecture et la technologie des liaisons de communications doivent assurer que les exigences relatives à l'indépendance entre les systèmes sont satisfaites. En plus de la séparation physique et de l'isolement électrique, il convient que la conception présente des dispositions pour garantir que les défauts et les dérangements affectant les moyens de communication n'ont pas pour conséquence la production par les modules de traitement de résultats non sûrs.

c) Les liaisons de communications doivent comprendre des dispositifs permettant la vérification du fonctionnement des équipements de communication et de l'intégrité des données transmises.

d) Il convient qu'une redondance des liaisons communications soit prévue afin de pallier aux défaillances.

e) Les liaisons de communications doivent être conçues de telle manière que la communication de données et le comportement des fonctions appartenant à une plus haute catégorie de sûreté ne soient pas perturbés par les communications de données avec des systèmes de classes inférieures.

Voir la CEI 61500 et la CEI 60709 pour plus de détails.

5.4.2.5 Outils

a) La conception de l'architecture d'I&C doit contenir la définition des outils, généralement logiciels (voir l'Article 14 de la CEI 60880:2006 et 5.1.4 et 6.1.4 de la CEI 62138:2004), utilisés pour assurer la cohérence des données échangées entre les systèmes d'I&C travaillant ensemble et pour assurer la cohérence des données avec la base de données de la centrale.

NOTE Les outils spécifiques aux systèmes individuels sont définis pendant la phase de spécification du système (voir 6.2.3.2).

b) Il convient que des outils soient utilisés dans toutes les phases du cycle de vie de sûreté de l'ensemble de l'I&C lorsqu'ils permettent l'amélioration de l'assurance qualité et de la fiabilité des fonctions importantes pour la sûreté, par exemple pour aider

- tous les aspects liés à la conception des interfaces entre les systèmes d'I&C,
- à l'intégration globale et à la mise en service d'ensemble des fonctions réparties.

c) Les outils doivent être choisis et les méthodes pour obtenir une qualité suffisante des résultats doivent être définies conformément aux exigences de la CEI 60880 (pour les systèmes de classe 1) et à celles de la CEI 62138 (pour les systèmes de classe 2 et 3).

5.4.2.6 Défense contre les DCC

Les systèmes d'I&C présentant une architecture redondante peuvent faire l'objet de défaillance, si deux de leurs circuits redondants ou plus font l'objet de défaillances simultanées (DCC), (par exemple, défaillance d'une logique de vote majoritaire sur sollicitation). De telles manifestations peuvent survenir, si un ou plusieurs défauts latents sont systématiquement présents dans certains ou dans tous les circuits redondants et qu'un mécanisme, pouvant solliciter de tels défauts latents, existe dans deux circuits redondants ou plus, pour qu'ils soient sujets à des défaillances corrélées dans le temps (voir la CEI 62340).

L'origine des défauts latents systématiques est principalement liée aux erreurs humaines. Ils peuvent être introduits dans n'importe quelle phase du cycle de vie d'un système d'I&C. L'utilisation d'ordinateur permet de mettre en œuvre des algorithmes et des processus plus complexes que ceux que l'on pouvait mettre en œuvre avec la seule technologie câblée. De plus, l'effort de conception à fournir pour un système d'I&C informatisé, y compris les activités liées à la conception de la plate-forme d'I&C support, est plus important que celui associé à un système d'I&C câblé et la conception peut être plus complexe.

Il convient d'évaluer les choix de conception avec pour objectif de minimiser l'introduction d'une complexité qui aurait pu être évitée.

La défense contre les DCC dans les systèmes d'I&C comprend les niveaux suivants:

a) Il convient de réaliser une validation fonctionnelle de la spécification des exigences des fonctions d'application pour les systèmes de classe 1 (voir le paragraphe 6.2.4.2.1) pour réduire la probabilité de présence de défauts latents dans la spécification d'exigences.

b) Un processus d'ingénierie clairement organisé doit être suivi avec la plus haute attention portée à toutes les activités de vérification et de validation, ceci pour réduire la probabilité de présence de défauts latents dans la conception. Il convient de graduer les efforts entre les systèmes de classe 1, 2 et 3.

c) Il convient de concevoir les systèmes d'I&C de classe 1 et leurs systèmes supports de façon à ce qu'ils fonctionnent indépendamment de facteurs d'influence associés au procédé de la centrale, ceci pour minimiser la probabilité que les éventuels défauts latents ne soient sollicités (par exemple il convient que les composants matériels supportant des fonctions d'atténuation des EIP ne soient pas affectés par le changement des conditions d'ambiance liées à l'apparition des EIP; il convient que l'ordonnancement de l'exécution du logiciel ne dépendent pas des signaux relatifs à la centrale).

NOTE 1 Cette recommandation correspond à l'exigence de la CEI 62340 qui indique qu'il convient que les systèmes d'I&C fonctionnent indépendamment du « profil de d'exploitation de la centrale".

d) Pour les systèmes de classe 1, une analyse doit être réalisée pour identifier les sources de DCC et les mécanismes qui pourraient solliciter les défauts latents entraînant des défaillances. Dans cette analyse, il convient de porter une attention particulière aux liaisons et aux dispositifs associés à la communication des données et aux composants dont la charge est liée à la demande. Il convient d'évaluer les modes de défaillance possibles et les séquences de défaillance de tels composants par rapport aux sources et aux effets possibles des DCC. Il convient de prévoir cette analyse pour les systèmes des groupes de sûreté auxquels il est fait appel pour compenser les effets des DCC postulées pour les systèmes de classe 1.

Une conception tolérante aux DCC est nécessaire si la défaillance postulée des fonctions importantes pour la sûreté peut entraîner des conséquences inacceptables. Ce qui est en général le cas pour les fonctions de catégorie A et pour un sous ensemble des fonctions de catégorie B (voir 5.3.2 et 5.3.3 dans la CEI 61226:2009).

e) Il convient que la conception de l'architecture d'I&C mette en œuvre les principes de diversité lorsqu'un niveau de fiabilité élevé est requis pour un groupe de sûreté, et en conséquence les causes et conséquences des DCC sont à prendre en compte. Il convient de prendre en compte la diversité fonctionnelle, matériel et des signaux. Si la diversité est utilisée pour lutter contre les DCC, la conception doit comprendre une analyse de l'efficacité des mesures diversifiées auxquelles il est fait appel pour réduire la possibilité de DCC.

f) Lorsqu'on fait appel à des systèmes d'I&C de classe 1 et de classes inférieures dans une analyse de sûreté déterministe en tant que lignes de défense différentes pour des accidents de dimensionnement, ces systèmes doivent être indépendants. Des systèmes d'I&C réalisent leurs fonctions de sûreté de façon indépendante si la défaillance postulée d'un de ces systèmes n'empêche pas les autres systèmes de réaliser leurs fonctions comme prévu. Des systèmes d'I&C indépendants doivent fonctionner avec des trajectoires de signal différentes. Ceci peut être garanti par la diversité (par exemple la diversité matérielle ou la diversité fonctionnelle).

On peut trouver des exigences supplémentaires concernant les mesures pour lutter contre les DCC dans les systèmes réalisant des fonctions de catégorie A dans la CEI 62340.

NOTE 2 Il convient de prévoir une activité au niveau de l'analyse de sûreté de la centrale pour vérifier que les mesures prises pour gérer/contrer les défaillances d'I&C seront réalisées par les fonctions de catégories A/B/C spécifiées. Ce ne sera pas une activité limitée à l'I&C, car elle se situe au niveau analyse de sûreté, elle est donc hors du domaine de la présente norme.

5.4.3 Affectation des fonctions aux systèmes

Le processus d'affectation des fonctions attribue les exigences d'ensemble relatives aux fonctions d'I&C importantes pour la sûreté établies en 5.3 aux systèmes individuels de l'architecture I&C. Il peut décomposer, si nécessaire, une fonction en plusieurs sous-fonctions réparties sur plusieurs systèmes. Toutes les fonctions ou sous-fonctions sont appelées fonctions d'application des systèmes d'I&C (voir 6.2.2.2).

a) La spécifications des exigences de fonctionnalité et de performance relatives aux fonctions d'application doivent être compatibles avec celles relatives aux fonctions d'I&C. Si une fonction est répartie sur plusieurs systèmes d'I&C, ces systèmes interconnectés doivent ensemble présenter des caractéristiques telles que les exigences qui sont l'objet du 5.3 soient respectées.

   NOTE 1 Ceci comprend une évaluation de l'atteinte des objectifs probabilistes tels que définis.

b) Les spécifications des exigences de fonctionnalité et de performance relatives aux fonctions d'application doivent inclure les fonctions auxiliaires de validation, de verrouillage et de surveillance qui ont été identifiées lors de la conception de l'architecture d'I&C, par exemple: état et mode de fonctionnement des systèmes interconnectés, validation des signaux en provenance d'autres systèmes.

c) L'affectation des fonctions d'application aux systèmes doit être conforme aux principes définis dans le Tableau 2 sur la classe des systèmes et la catégorie des fonctions.

d) Les fonctions de catégorie A doivent être attribuées à des systèmes de telle façon que le critère de défaillance unique soit satisfait.

NOTE 2 Pour s'aligner sur le NS-R-1, c'est au groupe de sûreté de satisfaire au critère de défaillance unique et non pas au système individuel d'I&C lui-même.

e) L'affectation à des systèmes des fonctions de catégorie A d'un même groupe de sûreté doit prendre en compte les mesures de défense contre les DCC prescrites en 5.4.2.6. Des exemples d'affectation de fonctions de catégories différentes sont donnés Figure C.1.

f) L'affectation des fonctions d'application aux systèmes doit viser à minimiser la complexité des systèmes de classe 1.

NOTE 3 Ceci est en particulier valable pour les nouvelles centrales. En cas de remplacement de systèmes câblés par des systèmes programmés, les exigences pour les fonctions d'application du système câblé remplacé sont normalement reportées pour le système programmé.

NOTE 4 La complexité système peut être réduite en considérant lors de la conception des approches telles que

- l'évitement des algorithmes et des traitements complexes qui ne peuvent pas être clairement définis et validés,
- la réduction du nombre de fonctions différentes qui sont mises en œuvre dans un système,
- l'utilisation de principes de conception simples afin de limiter les conséquences de défaillances complexes liées à d'éventuels défauts.

Néanmoins, il convient que la réduction de la complexité n'ait pas un impact négatif trop important au niveau de la conception, tel qu'une augmentation de la complexité de l'architecture d'ensemble de l'I&C ou tel que la réduction de fonctionnalités liées à la sûreté telles que l'étendue de couverture des autotests.

g) La fiabilité requise de chaque fonction d'application doit être compatible avec des limites que l'on peut estimer pouvoir atteindre, ceci comprenant les DCC.

NOTE 5 L'évaluation des limites peut dépendre des recommandations établies par les normes, des analyses préliminaires réalisées et du retour d'expérience acquis au niveau de précédents processus réglementaires d'autorisation et d'évaluation des risques.

h) Les rapports produits lors du processus d'affectation des fonctions aux systèmes doivent clairement faire apparaître quels systèmes réalisent quelles fonctions, c'est-à-dire que la capacité à pouvoir tracer doit être assurée.

5.4.4 Analyses requises

5.4.4.1 Généralités

Des analyses sont requises pour vérifier l'architecture d'I&C et l'affectation des fonctions aux systèmes d'I&C. De telles analyses correspondent une démarche itérative qui doit être effectuée avec le processus de conception (voir Article 6).

5.4.4.2 Estimation de la fiabilité et des défenses contre les DCC

a) Il convient qu'une évaluation de la fiabilité des systèmes d'I&C importants pour la sûreté soit réalisée. Il convient qu'elle prenne en compte les dépendances dues à des services communs, tels que la fourniture d'énergies électrique et pneumatique, et les moyens de ventilation et de chauffage.

b) Cette évaluation peut être initialement basée sur la fiabilité estimée qui peut être atteinte pour les fonctions des différents systèmes. Il convient qu'elle soit vérifiée à la fin du processus de conception, en se basant sur l'estimation de la fiabilité des systèmes (voir 6.2.4.2.2).

c) Une évaluation de la vulnérabilité aux DCC, des groupes de sûreté réalisant des fonctions de catégorie A doit être effectuée pour évaluer l'efficacité des mesures mises en place contre les DCC et pour identifier d'éventuels points faibles dans l'architecture d'ensemble.

d) La documentation de conception des systèmes (voir 6.4.4) doit être analysée afin d'identifier les composants matériels ou logiciels, communs ou identiques, impliqués dans différentes fonctions d'un groupe de sûreté contenant des fonctions de catégorie A. Si des éléments communs ou identiques sont détectés dans différentes lignes de défense, une

justification doit être fournie pour montrer que la probabilité de DCC est suffisamment faible et est compatible avec le rôle de sûreté du groupe de sûreté.

e) Il n'existe aucune méthode unanimement reconnue pour procéder à une estimation quantitative de la probabilité des DCC, aussi les méthodes à utiliser pour cette estimation sont essentiellement qualitatives (voir Annexe C). Il convient que les méthodes à utiliser soient définies au début de la conception.

NOTE 1 Un objectif de ces recommandations et de ces exigences est d'éviter des changements tardifs dans la planification et la conception d'un système en réponse à des modifications d'exigences, des DCC potentielles pouvant résulter d'erreurs faites lors de la réponse à ces modifications.

NOTE 2 Le niveau de détail de l'analyse des DCC peut dépendre de la catégorie des fonctions mises en œuvre par les systèmes et sera justifié.

NOTE 3 Les exigences relatives à l'analyse des DCC logicielles dans les systèmes de classe 1 sont données en 13.3 de la CEI 60880:2006.

5.4.4.3 Estimation des facteurs humains

Il convient que la vérification de la conception de l'architecture contienne une analyse des exigences relatives aux facteurs humains afin de permettre l'optimisation de la conception des systèmes d'IHM.

5.5 Planification globale

5.5.1 Généralités

Le présent paragraphe impose des exigences sur le développement des plans d'ensemble qui garantissent la prise en compte des exigences communes issues du cycle de vie de sûreté de l'ensemble de l'I&C par tous les systèmes d'I&C individuels et qui d'assurent que les exigences relatives aux fonctions d'I&C importantes pour la sûreté réparties sur les systèmes d'I&C seront respectées et maintenues pendant la durée de vie des systèmes.

Les exigences du présent article coordonnent et complètent les plans établis en 6.3 pour les systèmes individuels d'I&C.

NOTE Les exigences suivantes portant sur ces plans n'empêchent pas d'organiser ceux-ci avec un nombre de documents différents.

Les plans globaux doivent être établis avant que les activités qu'ils concernent ne débutent.

5.5.2 Plan global d'assurance qualité

La présente norme suppose qu'un programme d'assurance qualité, ou mieux un système de gestion de la qualité intégré, en accord avec les exigences des documents AIEA GS-R-3 et GS-G-3.1 existe en tant que partie intégrante du projet de centrale nucléaire et qu'il prévoit le contrôle des diverses activités.

a) Des programmes d'assurance qualité doivent être établis et mis en œuvre pour chaque activité ayant trait au cycle de vie de sûreté de l'ensemble de l'I&C.

b) Les programmes d'assurance qualité doivent comprendre toutes les activités nécessaires pour atteindre la qualité ainsi que les activités vérifiant que la qualité demandée a bien été atteinte.

c) Les activités de vérification doivent être définies dans les plans de vérification. Ceux-ci couvrent les moyens, le processus et les informations de sortie des phases du cycle de vie de sûreté de l'ensemble de l'I&C et définissent:

- les procédures et les outils relatifs aux activités de vérification,
- les enregistrements qu'il convient de faire et de vérifier,
- les aspects pertinents relatifs à la sûreté qu'il convient de vérifier,
- les procédures de résolution des défaillances et des incompatibilités,

- les critères permettant de déclarer la fin de chaque phase,
- les rapports finals à établir, montrant la conformité des résultats de la phase aux exigences en entrée et la résolution des anomalies.

d) Les programmes d'assurance qualité doivent être prévus et intégré dans le cadre du programme général d'assurance qualité du projet de la centrale nucléaire et ses activités doivent être incluses dans le calendrier général des activités du projet de centrale nucléaire.

5.5.3 Plan global de sécurité

Des mesures de sécurité sont requises pour protéger les informations traitées dans les systèmes importants pour la sûreté contre les modifications non autorisées, y compris le contrôle des actions non autorisées, (intégrité), les blocages d'accès (disponibilité) et la divulgation non autorisée (confidentialité).

NOTE 1 Pour les systèmes d'I&C des centrales nucléaires, les exigences relatives à l'intégrité et à la disponibilité ont priorité sur celles relatives à la confidentialité.

Les logiciels (codes ainsi que paramètres et données) peuvent être particulièrement vulnérables pendant la conception et la maintenance. Les menaces qu'il faut prendre en compte comprennent les modifications malintentionnées provoquant un comportement erroné des logiciels, soit d'une manière générale, soit déclenché par des contraintes de temps ou de données.

NOTE 2 Les menaces résultant de modifications non intentionnelles sont traitées dans la spécification des exigences relatives aux systèmes (voir 6.2.2.5).

Le plan global de sécurité spécifie les procédures et les mesures techniques à prendre pour protéger l'architecture des systèmes d'I&C contre les attaques intentionnelles et intelligentes pouvant compromettre des fonctions importantes pour la sûreté. Les dispositions du plan global de sécurité peuvent faire la différence entre les exigences portant sur les systèmes de classes 1, 2 et 3.

a) Les exigences de sécurité relatives aux fonctions et systèmes importants pour la sûreté doivent être identifiées dans le plan de sécurité des systèmes (voir 6.3.3).

b) Le risque résultant d'un accès ou modification non autorisés doit être géré de manière systématique pendant toutes les phases du cycle de vie d'un système, du début, au démantèlement. Ceci couvre le développement et la réalisation des systèmes, comme les systèmes d'I&C à installer sur la tranche. Les accès physiques comme les accès à distance doivent pris en compte.

c) Les mesures de sécurité dans un système doivent être telles qu'elles n'ont pas d'influence significative sur sa fiabilité ou sa disponibilité.

d) Afin de maintenir en permanence la sécurité des systèmes à un niveau élevé, une politique de sécurité spécifique au site doit être établie. Elle doit contenir des procédures relatives à l'interface entre la sécurité administrative et technique, l'accès aux systèmes, la sécurité de la gestion des données, la sécurité des modifications et de la maintenance, l'audit et les rapports sur l'état de la sécurité et sur la formation à la sécurité.

e) Les systèmes réalisant des fonctions importantes pour la sûreté doivent être physiquement protégés contre les accès non autorisés (voir 4.51 de l'AIEA NS-G-1.3:2005). Le contrôle des accès doit permettre une identification et une authentification du personnel accédant aux systèmes supportant des fonctions de catégorie A ainsi qu'une identification fiable du personnel accédant aux systèmes supportant des fonctions de catégorie B et C.

f) L'accès à distance (depuis l'extérieur de la centrale) aux systèmes supportant des fonctions de catégorie A ou B ne doit pas être possible, et il convient qu'il ne soit pas non plus possible pour les systèmes supportant des fonctions de catégorie C. Si l'accès par liaison de communication (à l'intérieur ou à l'extérieur de la centrale) est prévu, il doit être analysé et il doit être démontré qu'il n'engendre pas de risque non acceptable d'accès non

autorisé aux systèmes, et qu'il ne représente pas un risque non acceptable de défaillances pour les systèmes.

NOTE 3 La restriction des accès n'empêche pas de transmettre des données à partir d'un système.

g) Il convient que l'accès (y compris les tentatives d'accès) aux systèmes soit enregistré. Ceci comprend: l'identification de la personne, le type d'accès, l'heure et les actions effectuées.

h) Les registres de sécurité doivent être formellement inspectés à intervalles de temps définis pour les systèmes réalisant des fonctions de catégorie A. Il convient qu'ils soient vérifiés périodiquement pour les systèmes réalisant des fonctions de catégorie B et C.

5.5.4 Plans d'intégration et de mise en service globaux de l'I&C

5.5.4.1 Généralités

L'intégration d'ensemble de l'I&C regroupe toutes les mesures techniques et administratives réalisées sur site permettant aux systèmes d'I&C d'être installés sur site, interconnectés, testés, étalonnés et préparés pour une utilisation opérationnelle.

La mise en service d'ensemble regroupe toutes les mesures techniques et administratives réalisées sur site nécessaires pour garantir que les systèmes installés et la centrale dans sa totalité sont aptes à fonctionner, avant leur mise en exploitation (voir 4.4 de l' AIEA 75-INSAG-3:1999).

NOTE 1 La mise en service globale fait référence à la mise en service de l'ensemble de la centrale et comprend tous les systèmes de la centrale, et pas seulement les systèmes d'I&C (voir 3.7).

L'intégration d'ensemble de l'I&C et la mise en service globale complètent la validation et l'installation effectuées sur les systèmes individuels (voir 6.2.6 et 6.2.7). Les exigences suivantes doivent être satisfaites:

a) Après l'intégration des systèmes d'I&C sur site, la conformité des fonctions d'I&C importantes pour la sûreté à leurs exigences de fonctionnalité et de performance doit être établie pour tous les modes d'exploitation spécifiés de la centrale.

b) L'étendue des activités d'intégration et de mise en service à réaliser au niveau de la centrale peut être définie en prenant en compte l'étendue des essais réalisés lors d'autres phases de conception, par exemple les essais des fonctions et d'intégration réalisés en usine ou sur site, ou les essais réalisés pour des centrales de même type, si la centrale nucléaire n'est pas une première réalisation. Ces réductions doivent être justifiées et documentées.

NOTE 2 La minimisation du volume des essais à réaliser sur site sur le système intégré d'I&C en faisant une partie importante des essais d'intégration au préalable en usine, est une bonne pratique. Il convient de développer très tôt au niveau du projet une stratégie globale concernant la répartition des essais dans différents environnements (essais réalisés en utilisant une simulation ou une émulation, essais utilisant un banc d'intégration d'essai en usine, essais réalisés sur site), voir pour exemple 7.18 de l' AIEA NS-G-1.3:2005.

Généralement, ces essais forment une partie du processus de recette des systèmes d'I&C réalisé par le propriétaire de la centrale. La CEI 62381 [11] fournit des détails pratiques pour réaliser et documenter les recettes usine, les recettes site et les essais d'intégration sur site.

5.5.4.2 Plan d'intégration global de l'I&C

Un plan d'intégration global de l'I&C doit être établi dans le cadre du programme d'assurance qualité. En complément des exigences génériques du 5.5.2 sur l'assurance qualité et la vérification, les exigences techniques suivantes s'appliquent:

a) Les systèmes interconnectés doivent être testés pour confirmer que

- toutes les interfaces des systèmes interconnectés fonctionnent correctement,
- la détection des défaillances, les actions correctives et l'affichage des données associées sont conformes aux exigences des fonctions d'I&C.

b) La vérification de l'immunité aux interférences électromagnétiques des systèmes interconnectés doit être effectuée conformément aux exigences de la CEI 61000-4-1 à la CEI 61000-4-6.

NOTE La vérification de l'immunité nécessite généralement de mettre en œuvre une combinaison de mesures (par exemple pour définir les conditions sur site), d'essais (par exemple des sous-systèmes) et d'analyses. De plus, d'autres sections de la série CEI 61000-4 fournissent des recommandations applicables aux mesures et aux essais.

c) La mise à la terre de tous les équipements et écrans de câble doit être vérifiée pour quelle soit correcte.

d) La réponse des systèmes lors de la perte et de la restauration des alimentations électriques externes, ainsi que lors de l'apparition de surintensités telles que spécifiées, doit être testée afin de vérifier le comportement et la disponibilité des systèmes en cas de coupure et de restauration des alimentations électriques.

e) La conformité des conditions environnementales par rapport à celles spécifiées doit être vérifiée sur le lieu d'utilisation des systèmes d'I&C.

f) Les signaux logiques et analogiques échangés entre les systèmes doivent être testés pour montrer que des valeurs et états corrects sont fournis aux différentes fonctions importantes pour la sûreté. Lorsque des fonctions d'affichage, d'alarme, d'enregistrement et de calcul sont exécutées dans un système non important pour la sûreté, il convient que ces tests soient effectués conjointement avec ce système, à moins qu'une méthode plus simple démontre l'exactitude des données qui lui sont transmises.

g) Les fonctions de commande logique et de commande en boucle fermée doivent être testées, depuis les entrées jusqu'aux sorties et en tenant compte des interfaces avec l'opérateur, les actionneurs et les basculements de commande (par exemple manuel/automatique).

h) Les tests doivent confirmer que des informations exactes sont fournies à chaque système en cas de défaillance d'équipements redondés, de liaisons de communication, de capteurs ou d'organes réglant d'actionneur. Il convient que ces tests confirment que les temps de réponse et le bon fonctionnement des commandes de commutation sont corrects.

i) Le système de communication de données doit être testé pour garantir la bonne transmission des données ainsi qu'un temps de réponse acceptable, depuis l'émission de la commande jusqu'à la réception de l'indication correcte de l'état de l'actionneur. Il convient que les tests soient effectués en simulant des conditions opérationnelles normales, des conditions accidentelles pertinentes, les conditions les plus pénalisantes, et aussi en simulant des défaillances matérielles.

5.5.4.3 Plan de mise en service global

Un plan de mise en service global complétant la validation des systèmes d'I&C doit être établie dans le cadre du programme de mise en service des systèmes de la centrale (voir 4.4. 253 de l'AIEA 75-INSAG-3:1999). Les exigences suivantes traitent des aspects spécifiques à l'I&C et doivent être intégrées au programme de mise en service global:

a) Le réglage des points de consigne, des seuils, des paramètres et des valeurs d'étalonnage doit être vérifié et les valeurs doivent être ajustées pendant la mise en service des systèmes de la centrale pour confirmer que l'utilisation et la performance des systèmes satisfont à leurs exigences.

b) Les procédures d'exploitation et d'essais des systèmes d'I&C doivent être vérifiées et mises à jour pendant la mise en service de la centrale.

5.5.5 Plan d'exploitation global

Le plan d'exploitation global traite du fonctionnement des systèmes d'I&C interconnectés. Ce plan global est un complément des plans d'exploitation des systèmes individuels d'I&C (voir 6.3.7).

Un plan d'exploitation global doit être établi dans le cadre du programme d'assurance qualité. En complément des exigences génériques de 5.5.2 sur l'assurance qualité et la vérification, les exigences suivantes s'appliquent:

a) Le plan doit décrire

- les moyens permettant le démarrage, l'initialisation et le maintien dans un état opérationnel des systèmes interconnectés;
- les moyens permettant de vérifier la capacité des systèmes à réaliser les fonctions importantes pour la sûreté;
- les actions de routine, par exemple les tests périodiques, qui doivent être effectuées pendant le fonctionnement de la centrale afin de maintenir la fiabilité requise des fonctions importantes pour la sûreté.

b) Le plan doit spécifier les conditions sous lesquelles la modification des paramètres ou commandes des systèmes peut être effectuée ainsi que les effets de ces modifications sur le fonctionnement des systèmes et sur l'exploitation et la sûreté de la centrale. Il doit également indiquer les modifications qu'il est possible d'apporter:

- sous seul contrôle administratif;
- sous contrôle administratif après approbation du concepteur et réalisation de tests et vérifications appropriés.

NOTE Le processus de mise en œuvre de modifications et les autorités autorisant ces modifications peuvent dépendre de l'exploitant et des réglementations nationales.

c) Le plan doit identifier tous les modes de fonctionnement des systèmes interconnectés et spécifier la façon dont les systèmes doivent être exploités dans chaque mode, y compris:

- les mesures à prendre et les contraintes d'exploitation des systèmes et de la centrale, en cas de défaillance des systèmes ou d'événement dangereux externe aux systèmes;
- les contraintes d'exploitation des systèmes et de la centrale pendant les essais périodiques, la maintenance et/ou la mise en place de modifications;
- lorsque les contraintes précédentes peuvent être levées, les procédures permettant de revenir à un fonctionnement normal et de confirmer que le fonctionnement normal est bien rétabli.

5.5.6 Plan de maintenance global

Le plan de maintenance global traite de la maintenance au niveau des systèmes interconnectés de l'architecture d'I&C. Il complète et coordonne les plans de maintenance des systèmes individuels (voir 6.3.8).

Un plan de maintenance global doit être établi dans le cadre du programme d'assurance qualité. En complément des exigences génériques de 5.5.2 sur l'assurance qualité et la vérification, les exigences suivantes s'appliquent :

a) Des contraintes doivent porter sur les activités de maintenance des systèmes individuels d'I&C afin d'assurer que tout effet sur la sûreté de la centrale est acceptable. En particulier, lorsque cela est exigé, les systèmes doivent continuer à satisfaire au critère de défaillance unique pendant la maintenance. Le plan doit identifier les équipements devant être retirés du service, les conséquences de ces retraits et les moyens pour remettre en état ces équipements et pour vérifier une remise en service correcte.

b) Une approche systématique d'essai et de remplacement doit être mise en œuvre afin de rendre les DCC improbables dans les parties de l'architecture d'I&C soumises à des variations des conditions d'ambiance lorsque un accident survient. Il convient que l'approche garantisse que les parties du système soumises aux rayonnements, et de ce fait à un possible vieillissement rapide, à des modifications de leurs propriétés physiques (câbles, capteurs) ou dont la charge est modifiée en réponse à une sollicitation (par exemple commutation des amplificateurs de puissance, relais), soient remplacées avant que la dégradation de leur aptitude à réaliser leurs fonctions de sûreté soit inacceptable.

NOTE 1 Les intervalles de remplacement peuvent être déterminés par vieillissement accéléré sur un équipement représentatif.

NOTE 2 Voir la CEI 62342 [12] pour les recommandations portant sur la gestion du vieillissement.

c) Les activités de maintenance nécessitant l'ajustement de données de configuration ou d'étalonnage doivent être contrôlées par des procédures documentées assurant que

- les ajustements se font dans les limites définies (ces limites peuvent être imposées par la conception des systèmes et le dimensionnement de conception de la centrale, auquel cas il n'est pas nécessaire d'imposer de restrictions formelles au personnel de maintenance),
- lorsque les ajustements sont effectués pendant le fonctionnement d'un système, les exigences du 5.5.5 ci-dessus s'appliquent,
- un enregistrement relatif à tous les ajustements faits en maintenance est conservé.

5.5.7 Plan de formation

5.5.7.1 Programme de formation

Le présent paragraphe traite des exigences permettant de s'assurer que le personnel travaillant à la centrale sur les systèmes d'I&C a reçu une formation appropriée.

a) Un programme de formation des personnels de maintenance et de conduite doit être mis en place pour les opérateurs de conduite et les spécialistes d'instrumentation et de contrôle commande.

NOTE La formation des opérateurs de conduite sera centrée sur les interfaces opérateur, et comprendra une connaissance de base pour ce qui est des aspects relatifs aux systèmes d'I&C, à la technologie, à la maintenance et au diagnostique, alors que la formation des spécialistes d'instrumentation et de contrôle commande sera centrée sur les modifications, le diagnostique et la maintenance, conformément à la définition des tâches à accomplir.

b) Il convient d'établir un programme de formation en se basant sur une approche de formation systématique. Ce programme doit comprendre

1) une analyse des tâches de la responsabilité des catégories de personnel, qui doit établir les objectifs de formation, un calendrier prévisionnel d'ensemble et une définition d'ensemble des cours de formation,
2) la garantie que les formateurs qualifiés sont disponibles ainsi que les moyens matériels de formation pour les formateurs comme pour les personnes formées,
3) une évaluation de la formation entreprise,
4) le programme d'amélioration de formation prenant en compte le retour d'expérience.

c) La formation des opérateurs de conduite doit traiter du fonctionnement en conditions normales et anormales de la centrale en utilisant les dispositifs d'interface opérateur et les fonctions d'I&C pertinents.

d) Il convient de prévoir dans le programme une formation particulière pour reconnaître les défaillances matériel et les anomalies logicielles.

5.5.7.2 Documentation utilisateur

a) La documentation utilisateur du système d'I&C doit être mis à disposition des personnels de conduite et de maintenance.

b) Il convient que la documentation utilisateur définisse chaque dispositif d'interface opérateur. Chaque fonction de chaque dispositif doit être expliquée et faire l'objet d'illustration en tenant compte de sa complexité.

c) La formation doit permettre aux personnels de conduite et de maintenance de se familiariser avec la documentation utilisateur pertinente pour leur tâche.

5.5.7.3 Systèmes de formation

En plus des activités en salle de cours, il convient que la formation repose sur l'utilisation de systèmes de formation. Pour la formation des opérateurs de conduite il convient d'utiliser des simulateurs de fonction ou pleine échelle.

a) La formation des personnels de conduite et de maintenance doit être réalisée sur des systèmes de formation qui sont pleinement représentatifs des caractéristiques des

systèmes et des matériels objets de la formation. Les limitations présentées par les systèmes de formation doivent être connues et documentées.

b) Les simulateurs employés pour la formation des opérateurs de conduite doivent comprendre des interfaces de salle de commande réalistes et offrir des possibilités de simulation temps réel du comportement de la centrale y compris des systèmes d'I&C. Les simulateurs doivent être capables de simuler les conditions réacteur normales et anormales, en comprenant des combinaisons de défaillances et de disfonctionnement d'équipement.

5.6 Documentation produite

5.6.1 Généralités

La documentation produite pour la conception de l'architecture d'I&C et le processus d'affectation des fonctions fournit les informations nécessaires à la spécification des exigences portant sur les systèmes individuels de l'architecture d'I&C (voir 6.2.2).

5.6.2 Documentation de conception de l'architecture

a) La documentation produite doit définir, pour les systèmes d'I&C individuels:

- les contraintes de conception provenant du cadre général de conception de la centrale (voir 5.2.4);
- les contraintes de conception provenant de la conception de l'architecture d'I&C (voir 5.4.2);
- les limites physiques et fonctionnelles des systèmes.

b) Il convient que les outils d'ingénierie utilisés soient documentés afin de préciser comment chaque outil est utilisé pour supporter les activités de conception dans le cycle de vie du système.

NOTE Pour les exigences relatives aux méthodes et outils logiciels utilisable pour les systèmes de classe 1, voir les Articles 7, 14 et 15 de la CEI 60880:2006 et pour les systèmes de classes 2 et 3, voir 5.1.1 et 6.1.1 de la CEI 62138:2004.

5.6.3 Documentation de l'affectation des fonctions

a) La documentation produite doit définir les exigences de fonctionnalité, performance et fiabilité relatives aux fonctions d'application (voir 5.4.3) affectées à chaque système. Les exigences peuvent être représentées sous forme de texte, schéma mécanique, matrices, schéma logique, etc., pourvu que les fonctions soient clairement explicitées.

b) Il convient que les spécifications des exigences relatives aux fonctions d'application soient définies de telle façon qu'elles soient autant que possible indépendantes de la technologie qui peut être utilisée pour mettre en œuvre les fonctions, par exemple calculateurs, relais.

c) Les principaux utilisateurs des documents d'exigence sont les auteurs de spécifications d'exigences des systèmes individuels et des opérateurs de conduite. Il convient que des méthodes et outils soient choisis de façon judicieuse pour ces personnels.

6 Cycle de vie de sûreté du système

6.1 Généralités

L'architecture d'I&C identifie les systèmes d'I&C supportant les fonctions importantes pour la sûreté (voir 5.4.2). Le présent article développe les objectifs et exigences relatifs à des systèmes programmés. Les exigences du présent article adressent les systèmes informatiques.

NOTE La plupart de ces exigences peuvent aussi s'appliquer aux systèmes d'I&C non numériques.

Afin d'assurer que toutes les exigences ayant trait à la sûreté et devant être respectées par le système sont bien prises en compte, mises en œuvre et maintenues, une approche systématique est nécessaire. A cet effet, les activités liées au développement, à la réalisation

et à l'exploitation des systèmes sont introduites dans un cycle de vie de sûreté du système. Ce cycle de vie fait référence, à son tour, aux activités du cycle de vie de sûreté de l'ensemble de l'I&C (voir l'Article 5 et la Figure 4).

L'ensemble des phases du cycle de vie de sûreté d'un système comprend généralement:

- la spécification des exigences du système,
- la spécification du système,
- la conception détaillée et la réalisation du système,
- l'intégration du système,
- la validation du système,
- l'installation du système,
- les modifications apportées à la conception du système (le cas échéant).

La qualification du système est prise en compte séparément car elle peut être réalisée en partie indépendamment du cycle de vie du développement du système. Cette approche correspond à la pratique actuelle qui consiste à utiliser de plus en plus des composants préexistants.

La Figure 5 donne un aperçu classique du cycle de vie de sûreté du système et indique les liens avec les cycles de vie du logiciel et du matériel prescrits dans la CEI 60880, la CEI 62138 et la CEI 60987.

Le Tableau 3 présente une vue d'ensemble des objectifs, entrées et sorties des différentes activités pendant le cycle de vie d'un système classique et fait référence aux paragraphes pertinents correspondants.

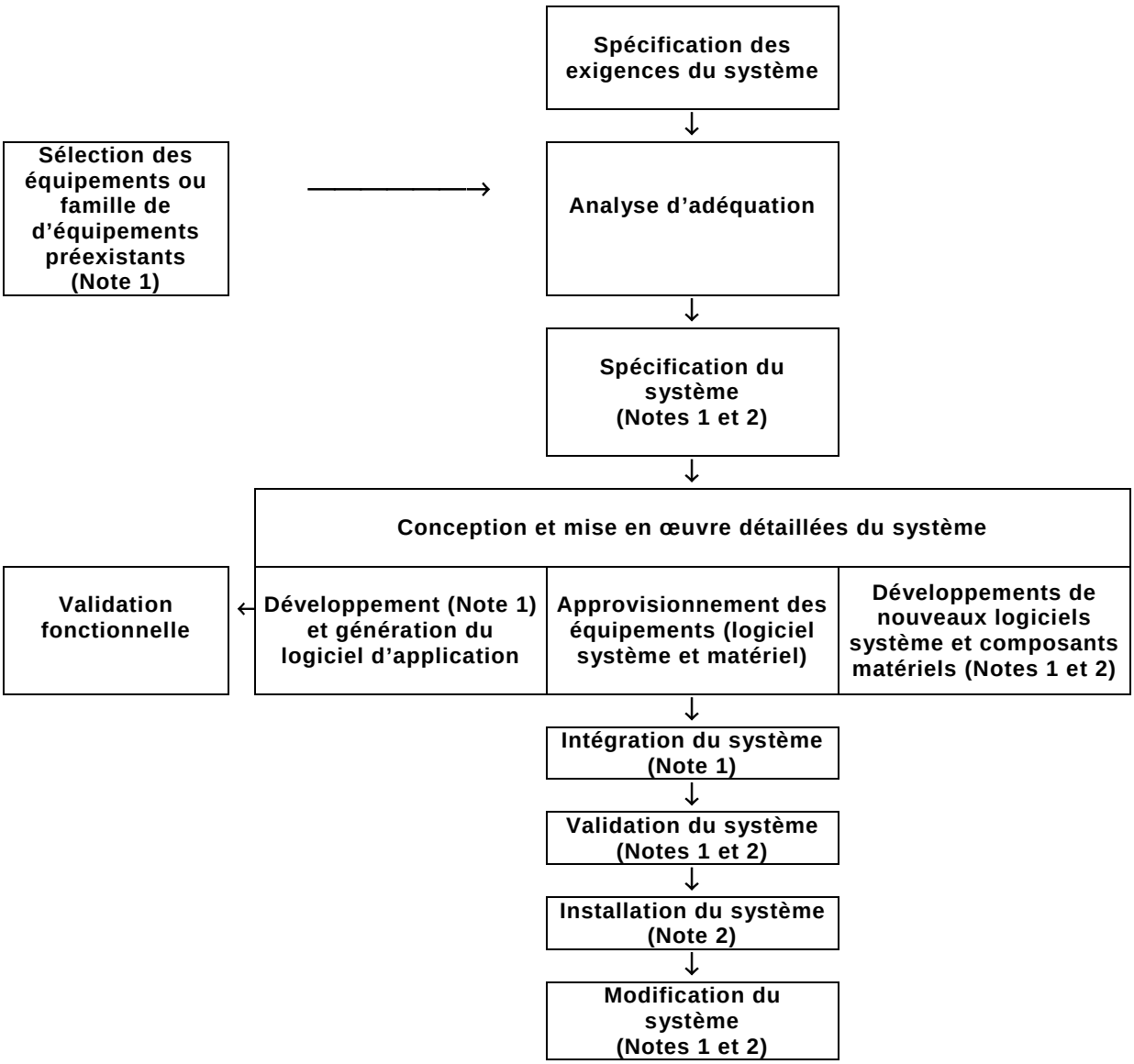
Le présent article inclut

- des exigences génériques qui s'appliquent de la même façon à tous les systèmes importants pour la sûreté,
- des exigences qui s'appliquent, en complément des précédentes, à des classes de systèmes et catégories de fonctions particulières.

Le cycle de vie du système est un processus itératif. Une phase peut débuter avant l'achèvement de la précédente, mais ne peut se terminer que si les phases précédentes sont achevées et si ses sorties sont consistantes avec les entrées fournies par ces phases précédentes.

Tableau 3 – Vue d'ensemble du cycle de vie de sûreté du système

Article ou paragraphe	Entrées	Objectifs de l'activité	Sorties
6 Exigences relatives au cycle de vie du système et relation de ce cycle avec le cycle de vie de sûreté d'ensemble			
6.2.2 Spécification des exigences portant sur le système	Sorties de 5.6, 5.5 Sorties de 6.3.2, 6.3.3	Spécifier les exigences portant sur le système pour – les fonctions, – les contraintes de conception, – les limites et interfaces avec les autres systèmes et outils, – les interfaces avec les personnels, – les conditions environnementales	Spécification des exigences du système Spécification des exigences des fonctions d'application
6.2.3 Spécification du système	Sorties de 6.2.2 Documentation des composants candidats préexistants Sorties de 6.3.2, 6.3.3	Evaluer et déterminer la faisabilité de l'intégration des composants candidats préexistants dans la conception du système Concevoir l'architecture du système conformément aux spécifications d'exigences système Affecter les fonctions d'application aux sous-systèmes	Document de spécification du système (voir 6.4.3) incluant: – l'identification des équipements choisis et les analyses de faisabilité, – l'architecture du système, – la spécification du logiciel
6.2.4 Conception détaillée et réalisation du système	Sorties de 6.2.3 Sorties de 5.2.2 Sorties de 6.3.2, 6.3.3	Elargir et améliorer la conception de l'architecture Développer le matériel et le logiciel (système ou d'application) Valider les exigences relatives aux fonctions d'application	Documentation de la conception détaillée du système (voir 6.4.4) Validation fonctionnelle et estimation de la fiabilité (voir 6.2.4.2) Composants et sous-systèmes matériels et logiciels
6.2.5 Intégration du système	Sorties de 6.2.4 Sorties de 6.3.2, 6.3.3, 6.3.4	Intégrer les composants individuels matériels et logiciels qui forment ensemble le système	Rapports d'intégration Système intégré
6.2.6 Validation du système	Sorties de 6.2.3, 6.2.5 Sorties de 6.3.2, 6.3.3, 6.3.5	Valider le système (voir Note 1)	Rapport de validation du système
6.2.7 Installation du système	Sorties de 6.2.6 Sorties de 6.3.2, 6.3.3, 6.3.6	Installer et tester le système sur site	Rapport d'installation Système installé et testé sur site
6.2.8 Modifications de la conception du système	Demande de modification (le cas échéant) Sorties de 6.3.2, 6.3.3, 6.3.8	Apporter les corrections, les améliorations ou les adaptations au système	Rapport sur les modifications Système modifié
6.3 Planification système	Sorties de 5.5, 6.2	Développer les plans de validation, d'installation, d'exploitation, de maintenance, de sécurité	Plans du système
6.5 Qualification du système	Sorties de 6.3.2, 6.3.3	Développer le plan de qualification et l'exécuter.	Documentation concernant la qualification
NOTE 1 La validation des systèmes d'I&C individuels est complétée dans le cadre de l'intégration d'ensemble de l'I&C et de la mise en service d'ensemble de la centrale (voir 5.5.4). La mise en service de la centrale en tant que telle est hors du domaine de la présente norme. NOTE 2 Pour une comparaison de cette définition des phases avec celle de la CEI 61508-2, voir Annexe D.			



NOTE 1 Les exigences relatives au logiciel portant sur cette activité sont définies dans la CEI 60880 et la CEI 62138, y compris en cas d'utilisation de logiciel préexistant.

NOTE 2 Pour les systèmes de classe 1 et 2, les exigences relatives au matériel portant sur cette activité sont définies dans la CEI 60987.

Figure 5 – Cycle de vie de sûreté du système

6.2 Exigences

6.2.1 Généralités

Le présent paragraphe définit les exigences portant sur le cycle de vie de sûreté du système.

Ces exigences couvrent également les aspects liés aux

- fonctions spécifiques affectées au système par le processus d'affectation des fonctions,
- caractéristiques génériques qui, selon le classement du système, rendent celui-ci apte à réaliser les fonctions importantes pour la sûreté des catégories spécifiées.

NOTE L'Article 7 de la CEI 61226:2009 spécifie les exigences relatives aux fonctions d'I&C et les exigences spécifiques aux différentes classes de systèmes et d'équipements d'I&C. Ces exigences sont prises en compte de manière appropriée dans la présente norme lors du développement des exigences relatives aux systèmes et fonctions respectivement.

6.2.2 Spécifications des exigences portant sur le système

6.2.2.1 Généralités

L'objectif de cette phase est de fournir une description de haut niveau des exigences relatives au système, indépendamment du choix d'une solution technique particulière. Cependant, des exigences particulières définies au niveau de l'architecture d'ensemble de l'I&C peuvent imposer des contraintes sur la technologie à utiliser, par exemple prise en compte des DCC.

La documentation produite de l'architecture d'I&C et de l'affectation des fonctions (voir 5.6) est une des entrées de la spécification des exigences système.

La documentation de sortie de cette phase est le document de référence utilisé pour communiquer entre ceux qui définissent le problème (« spécifieur ») et ceux qui apporteront une solution technique (« concepteur »).

La spécification des exigences du système doit indiquer:

- les fonctions du système,
- les exigences de performance globale,
- les contraintes portant sur la conception du système,
- les limites du système et les interfaces avec les autres systèmes,
- les interfaces avec les utilisateurs du système,
- les conditions d'environnement applicables au système,
- la qualification requise.

6.2.2.2 Fonctions

6.2.2.2.1 Généralités

Les exigences à prendre en compte sont celles relatives aux fonctions d'application et aux fonctions de service du système. Les exigences suivantes sont applicables.

6.2.2.2.2 Fonctions d'application

Les spécifications d'exigences relatives aux fonctions d'application importantes pour la sûreté sont définies par le processus d'affectation des fonctions (voir 5.4.3).

a) Les spécifications d'exigences relatives à chaque fonction d'application doivent établir
   1) la fonctionnalité, y compris les domaines de variation des entrées/sorties et des points de consigne (respectivement les gammes permises). Pour les fonctions d'arrêt d'urgence, les spécifications définissent les marges entre les points de consigne et les valeurs admissibles (c'est-à-dire celles incluant toutes les incertitudes dues aux erreurs d'étalonnage ou aux dérives de l'instrumentation);
   2) la performance, y compris la précision et les temps de réponse. Si nécessaire, les exigences de performance sont définies pour différentes conditions d'exploitation de la centrale et différents EIP,
   3) le filtrage adapté des signaux, la validation des signaux et les verrouillages doivent être spécifiés pour mettre en œuvre les modes de fonctionnement de repli et pour minimiser la probabilité d'actions intempestives.
b) La spécification d'exigences relative à chaque fonction d'application doit déterminer sa catégorie ainsi que l'existence éventuelle de contraintes d'indépendance vis à vis d'autres fonctions du même groupe de sûreté.

Les règles d'affectation des fonctions définissent pour chaque catégorie de fonction une classe minimale de système d'I&C. Ces règles, ainsi que les exigences relatives à l'indépendance entre les fonctions d'un même groupe de sûreté (critère de défaillance unique, défense contre les DCC), permettent une estimation qualitative de la fiabilité de la fonction ou du groupe de fonctions dans un groupe de sûreté.

Un objectif quantitatif de la fiabilité peut être associé à chacune des fonctions d'application de façon à compléter le processus de conception déterministe et pour aider à la vérification de la conception des systèmes et du dimensionnement de conception de la centrale. L'aptitude des matériels à satisfaire ces objectifs peut être évaluée en utilisant des techniques pertinentes pour les composants matériels, mais aucune méthode unanimement reconnue n'existe pour l'évaluation quantitative de la fiabilité du logiciel (voir 6.2.4.2.2).

6.2.2.2.3 Fonctions de service

Ces fonctions, à la différence des fonctions d'application, ne sont pas directement liées au procédé mais sont liées à des activités particulières du système. Elles incluent les fonctions nécessaires à la configuration, à la validation, à la qualification, à l'installation, à la mise en service, à l'exploitation, aux essais périodiques, à la maintenance, à l'incorporation de modifications et à la sécurité.

Les spécifications des exigences relatives aux fonctions de service sont finalisées par le rédacteur de la spécification du système. La précision des exigences de ces fonctions est déterminée au cas par cas. Dans certains cas, elle peut être finalisée dans la spécification du système et durant la phase de conception de l'architecture, après sélection d'une solution technique appropriée pour le matériel et le logiciel.

Il convient que les exigences relatives aux fonctions de service prennent en compte les contraintes pouvant provenir des plans du système (voir 6.3).

NOTE Par exemple, il convient que les commandes permettant la modification des paramètres soient consistantes avec les dispositions spécifiées par le plan de sécurité du système (voir 6.3.3), le plan d'exploitation du système (voir 6.3.7) et le plan de maintenance du système (voir 6.3.8).

6.2.2.3 Contraintes portant sur la conception

6.2.2.3.1 Généralités

Les exigences suivantes définissent les contraintes qui limitent le choix de solutions potentielles pour la conception du système et l'affectation des fonctions dans le système. Ces contraintes dépendent de la classe du système et des catégories des fonctions; elles doivent être prises en compte pendant la spécification et la conception de l'architecture du système afin de

- satisfaire aux exigences relatives à la catégorisation des fonctions d'application,
- assurer que le système fonctionnera comme il a été spécifié,
- permettre ou faciliter la démonstration du bon fonctionnement du système.

6.2.2.3.2 Architecture du système

L'architecture du système dépend de la catégorie des fonctions à réaliser au sein du système (voir 5.4.3) et du concept de défense en profondeur (voir 2.9 de l'AIEA NS-R-1:2000 et 3.8 et 4.23 de l'AIEA NS-G-1.3:2005).

a) Le système peut réaliser des fonctions de la catégorie la plus élevée permise pour sa classe (voir 5.4.3) et des fonctions de catégories inférieures. Le système peut contenir des sous-systèmes appartenant à des classes inférieures, à condition que les exigences suivantes soient respectées:

1) les exigences relatives à la conception de chaque sous-système ne doivent pas être plus faibles que celles requises pour la fonction de la catégorie la plus élevée supportée par le sous-système;

2) la conception du système doit garantir que les exigences des sous-systèmes ou équipements des classes supérieures sont satisfaites, même en cas de défaillance d'équipements de classes inférieures.

b) La conception du système doit intégrer la redondance et les caractéristiques nécessaires pour assurer la tolérance à la défaillance (voir 6.2.3.3.4) et prendre en compte l'affectation des fonctions d'application importantes pour la sûreté (voir 6.2.3.5).

NOTE 1 Le système peut également présenter un niveau de redondance pour satisfaire aux exigences de disponibilité. Le besoin pour de telles redondances est défini au niveau de la conception du système.

c) La conception du système doit satisfaire toutes les exigences d'indépendance (voir la CEI 60709 et 6.2.3.3.3)

- afin d'éviter la propagation de défaillances provenant de systèmes moins importants pour la sûreté,
- afin d'éviter la propagation de défaillances entre les voies redondantes réalisant des fonctions de catégorie A.

d) La conception des systèmes appartenant à des groupes de sûreté réalisant des fonctions de catégorie A doit présenter un niveau de redondance suffisant pour satisfaire au critère de défaillance unique pendant l'exploitation et la maintenance (voir e de 6.2.3.5).

NOTE 2 Les défaillances dues au logiciel sont des défaillances systématiques et non aléatoires. Ainsi, le critère de défaillance unique ne peut pas être appliqué à la conception du logiciel comme il l'est pour la conception du matériel. Les effets possibles de DCC dues au logiciel à l'intérieur de chaque ligne de défense et entre des sous-systèmes redondants sont pris en compte au niveau de chaque système et de l'architecture d'I&C (voir la CEI 62340).

6.2.2.3.3 Comportement interne du système

a) Il convient que la conception d'un système programmé assure un comportement prédictible en accord avec les exigences de performance des fonctions mises en œuvre.

NOTE 1 Un système programmé peut être déclaré avoir un comportement prédictible si la période de temps entre le stimulus et la réponse a un maximum et un minimum garantis dans toutes les conditions d'utilisation prévues.

b) Les technologies de communication doivent être choisies et dimensionnées afin de satisfaire aux exigences de performance dans toutes les conditions de charge de données générées par les régimes transitoires prévisibles de la centrale (y compris changements d'état très nombreux en cas de perte générale des alimentations électriques).

c) Afin de garantir avec un haut degré de confiance le comportement déterministe, il convient que les systèmes de classe 1 soient développés avec des techniques telles que celles mentionnées à l'Annexe B de la CEI 60880:2006 (voir notamment B2.d « Temps d'exécution » et B2.e « Interruptions »). Les techniques utilisant un séquencement statique des instructions (voir Note 2) sont préférables à celles utilisant des interruptions.

NOTE 2 « Statique » se définit comme permanent durant l'exécution du programme informatique (des exemples en sont les structures de données qui ne sont ni détruites, ni créées durant le fonctionnement après démarrage ou les paramètres de séquencement qui sont fixés au démarrage). Ainsi, en séquencement statique, la séquence des instructions ou des tâches ne dépend pas de la séquence d'évènements externes survenant, ce qui n'entraine pas de variation au niveau des ressources consommées par le calculateur, bien qu'il puisse y avoir un nombre fini de séquences différentes dépendant du chemin d'exécution.

NOTE 3 Voir 5.5.3 de la CEI 60880:2006 concernant le rôle des annexes à la norme et les exigences applicables si les pratiques diffèrent de celles mentionnées dans les annexes.

d) Les systèmes de classe 2 peuvent être développés avec des techniques autres que celles définies en c). Dans ce cas, il convient que la conception du système garantisse un comportement adéquat dans toutes les conditions d'exploitation prévues de la centrale (voir la CEI 62138 pour les détails).

e) Pour augmenter l'aptitude des systèmes de classe 1 et 2, à supporter des situations imprévues:

- l'adéquation des marges de conception fixées pour l'utilisation des ressources (du type puissance de l'unité centrale, mémoire, largeur de la bande de communication, ressources des systèmes opérationnels), ainsi que les temporisations internes au sein du système doivent être justifiées en conséquence;
- il convient que des dispositifs soient prévus pour surveiller tout écart au comportement déterministe et pour reconstituer l'état réel de la centrale en cas de pertes temporaires des informations d'entrée, par exemple: chiens de garde, rafraîchissement cyclique en parallèle à la détection des événements sur changement d'état.

6.2.2.3.4 Auto-supervision et tolérance aux défaillances

a) Il convient que les systèmes soient conçus de telle manière que les erreurs et défaillances sont détectées suffisamment tôt pour assurer la disponibilité requise pour le système, et que la détection des défaillances par les dispositifs d'autocontrôle soit mise en regard de la complexité supplémentaire qui est introduite. Il convient que les exigences des paragraphes 6.2 et A.2.2 de la CEI 60880:2006 relatives à l'auto-surveillance soient satisfaites autant que possible, pour chaque classe de système.

b) Il convient que des informations adéquates, opportunes et correctement mises en valeur concernant les défaillances soient transmises aux opérateurs de la centrale afin qu'ils puissent prendre les mesures correctives appropriées.

c) Il convient que la conception du système garantisse l'établissement d'un mode de fonctionnement approprié en cas de détection de défaillances (dégradation progressive, position de replis sûre, invalidation des sorties en cas de défaillance).

d) Pour les systèmes de classe 1, les installations d'autocontrôle doivent être conformes aux exigences de la CEI 60880 et de la CEI 60987.

6.2.2.3.5 Testabilité

a) Les systèmes doivent être munis de dispositifs permettant de vérifier qu'ils sont en mesure d'accomplir leurs fonctions importantes pour la sûreté.

NOTE Conformément au 4.83 de l'AIEA NS-G-1.3:2005, les essais sont de préférence des vérifications d'ensemble depuis les capteurs en entrée jusqu'aux actionneurs en sortie, mais les essais de chevauchement sont acceptables. Les essais incluent notamment:

a) la modification de l'état ou de la valeur de tout signal d'entrée et la surveillance des modifications au niveau de l'équipement récepteur;

b) l'interruption de la transmission, et la confirmation que l'équipement récepteur détecte cette interruption et effectue une action appropriée;

c) le contrôle et l'étalonnage des capteurs;

d) le contrôle de la mise en marche des actionneurs en sortie.

b) Les principes fournis par la CEI 60671 doivent être appliqués.

6.2.2.3.6 Maintenabilité

a) Le système doit être conçu de telle manière qu'il facilite la maintenance et, en cas de défaillance, un diagnostic aisé, une réparation ou remplacement sûr et le réétalonnage (voir 4.97 à 4.100 de l'AIEA NS-G-1.3:2005).

b) Il convient de concevoir les moyens de maintenance pour que leur influence sur la sûreté de la centrale durant la maintenance soit acceptable.

c) Les capacités et limites humaines et les facteurs environnementaux (température, humidité, espace, accessibilité, etc.) doivent être pris en compte afin de minimiser le risque et la charge de travail pour le personnel durant la maintenance.

d) Le système doit être conçu de manière à permettre que suite à sa réparation ou suite à son réétalonnage, l'aptitude opérationnelle de celui puisse être confirmée. Ceci doit inclure la vérification de:

- la restauration correcte de la continuité des circuits,
- l'étalonnage correct des mesures analogiques et de tout seuil d'alarme associé,

- l'aptitude du système à effectuer ses fonctions importantes pour la sûreté comme prévu dans les spécifications.

NOTE Les exigences relatives à la maintenance et aux essais de l'Article 11 de la CEI 60987:2007 s'appliquent aux systèmes programmés importants pour la sûreté de classes 1 et 2.

e) Il convient de prendre des mesures particulières lors de la conception des équipements à installer dans des zones normalement non accessibles (par exemple l'enceinte réacteur). Ceci peut entraîner l'ajout de redondance, ou la redondance de liaisons de communication.

6.2.2.4 Limites et interfaces avec les autres systèmes et outils

Afin d'assurer l'intégration du système dans l'architecture d'I&C, les aspects suivants doivent être spécifiés conformément aux exigences correspondantes de l'Article 5:

- l'emplacement prévu et les contraintes physiques relatives à l'installation du système dans la centrale (voir 5.2.4);
- les interfaces physiques et fonctionnelles du système avec les systèmes et équipements de soutien (voir 5.2.4);

NOTE Les exigences relatives aux sources électriques des systèmes d'I&C importants pour la sûreté sont définies dans à la CEI 61225 [16].

- les interfaces physiques et fonctionnelles du système avec les autres systèmes et équipements avec lesquels il échange des informations (voir 5.4.2.4);
- les interfaces avec les outils logiciels utilisés pour définir les échanges de données entre systèmes et pour vérifier la cohérence de ces données (voir 5.4.2.5).

6.2.2.5 Interfaces avec les utilisateurs

Les exigences relatives à l'IHM doivent minimiser le risque d'erreur humaine, par exemple les erreurs d'inadvertance, oublis et omissions, pendant l'installation, l'exploitation, les essais et la maintenance du système et de la centrale, ou lors de l'introduction de modifications.

NOTE La protection contre les modifications malintentionnées est traitée dans le plan de sécurité (voir 6.3.3).

6.2.2.6 Conditions liées à l'environnement

Les plages de variation normale et extrême des conditions environnementales auxquelles le système est tenu de résister doivent être spécifiées en fonction des contraintes imposées par le cadre général de conception de la centrale (voir 5.2.4). Les conditions à spécifier incluent:

- les conditions d'ambiance, comprenant: la température, l'humidité, la pression, le rayonnement et les interférences électromagnétiques pendant le fonctionnement normal et les situations accidentelles;

NOTE 1 Les normes suivantes fournissent des recommandations détaillées pour les IME: la CEI 61000-6-2 [13] et la CEI 61000-6-4 [14] spécifient les niveaux minimums d'immunité et les limites d'émission. La série de normes CEI 61000-4 indique les méthodes applicables pour réaliser les essais de qualification. La CEI 62003 [15] fournit des éclaircissements en ce qui concerne les critères et les paramètres de qualification indiqués par normes de la série CEI 61000 pour garantir que les exigences de sûreté nucléaires sont satisfaites, par exemple pour les systèmes de classe 1 et/ou de classe 2.

- les conditions d'ambiance imposées par les événements dangereux potentiels externes au système, ceux ci comprenant les séismes ou les inondations;
- les conditions relatives à l'alimentation électrique et à l'évacuation de la chaleur.

NOTE 2 Les conditions d'ambiance peuvent aussi traiter de questions telles que les rayonnements ultraviolet (par exemple la dégradation des gaînes de câbles, l'éffacement des EEPROMS), les poussières, les particules, les IEM produites par les arcs de soudage.

6.2.2.7 Qualification

Les systèmes importants pour la sûreté doivent être qualifiés. Pour les systèmes programmés, cette qualification couvre le matériel (ce qui comprend la tolérance aux conditions environnementales applicables), le logiciel système et le logiciel d'application tous deux intégrés dans le matériel (voir 6.5).

NOTE 1 Il peut être nécessaire de considérer aussi la qualification des outils. L'approche choisie dépend de la fiabilité requise ainsi que du risque associé aux erreurs et défauts qui peuvent être introduits par les outils, et l'étendue de la vérification des sorties résultats produits par les outils. Les CEI 60880 et CEI 62138 fournissent des recommandations sur le sujet.

La qualification confirme que la conception et l'équipement satisfont aux exigences. Elle couvre tous les aspects apparaissant dans la spécification système, par exemple la conformité des caractéristiques système aux exigences système telle que définie de 6.2.2.2 à 6.2.2.6.

C'est une bonne pratique que de diviser les exigences en exigences portant sur le système et en exigences portant sur les logiciels et matériels préexistants employés dans le système. Cette approche facilite la qualification en utilisant une approche par étape, par exemple en prenant en compte des preuves de qualification existante relatives à des équipements préexistant (préqualification, qualification générique), en qualifiant le matériel et le logiciel de façon séparée et en concluant par la prise en compte des aspects intégration matériel/logiciel.

La spécification système doit identifier les méthodes qui doivent être appliquées durant la conception de façon à garantir que la qualification du matériel, du logiciel support de l'équipement et de l'ensemble du système soit réalisable. Des détails sont fournis par 6.5.

NOTE 2 La façon la plus efficace de réussir la qualification est d'avoir une conception matériel et logiciel reposant sur les exigences et des processus conformes aux normes CEI applicables. Voir aussi la Note 1 en 1.1 de cette norme.

6.2.3 Spécification du système

6.2.3.1 Généralités

L'objectif de cette phase est de fournir une description de haut niveau de l'architecture du matériel et du logiciel du système, de spécifier les équipements à utiliser ou à développer pour sa mise en œuvre et d'affecter les fonctions d'application.

Les exigences relatives au système et la documentation relative aux composants candidats préexistants font partie des informations d'entrée nécessaires à la spécification du système.

La documentation produite résultant de cette phase (voir 6.4.3) constitue une donnée d'entrée pour la réalisation du système (matériel et logiciel) au cours des phases ultérieures du cycle de vie du système.

Cette phase inclut les activités nécessaires à la définition des exigences relatives au logiciel, au matériel et à l'intégration du système.

La spécification du système doit définir

- les composants à utiliser,
- l'architecture du système d'I&C individuel,
- les exigences relatives au logiciel,
- l'affectation des fonctions d'application dans les sous-systèmes.

6.2.3.2 Sélection des composants préexistants

Il n'est pas rare d'utiliser des composants préexistants (composants matériels ou logiciels spécifiques ou composants d'une famille d'équipements) pour réaliser tout ou partie d'un « nouveau » système.

NOTE 1 Les composants préexistants peuvent être des composants sur étagère du commerce (également appelés « COTS ») ou des produits utilisés en interne par des fabricants.

NOTE 2 L'Article 15 de la CEI 60880:2006 traite des critères d'acceptation de logiciels préexistants réutilisables pour les fonctions de catégorie A; 5.2 et 6.2 de la CEI 62138:2004 en font de même pour respectivement les fonctions de catégories B et C. La CEI 60987 fournit des recommandations pour l'utilisation du matériel préexistant.

a) L'aptitude à l'emploi des composants candidats doit être évaluée et estimée afin de démontrer que leurs caractéristiques sont conformes aux exigences du système.

b) Il convient que l'évaluation et l'estimation des composants candidats reposent sur la comparaison de deux ensembles documentaires: la spécification des exigences système et la documentation relative aux composants préexistants. Cette dernière inclut les spécifications produit et (si disponible) la documentation de pré-qualification.

c) Les exigences suivantes s'appliquent:

- on doit analyser si la documentation fournie définie explicitement les fonctionnalités et les propriétés de tous les composants,

  NOTE 3 Généralement les éléments dont les définitions sont attendues sont: les temps d'exécution et les besoins en mémoire des composants logiciels, les taux de défaillance des composants matériels, les modes de défaillance et les caractéristiques des positions de repli de l'équipement sur défaillance matériel et erreur logiciel, les conditions d'ambiance supportées par le système et les exigences relatives au montage des armoires, au câblage et aux connexions à l'alimentation électrique, à la consommation électrique et aux outils de service.

- les propriétés qui, initialement, ne sont pas définies explicitement doivent le devenir après détermination par analyses ou par essais,
- la documentation doit permettre de déterminer la fiabilité et la performance des fonctions d'application de la centrale dans la ou les configurations prévues des composants,
- la documentation doit définir la fonctionnalité et les propriétés des méthodes et outils d'ingénierie logicielle associés,
- les fonctions non utilisées (c'est-à-dire celles contenues dans des équipements mais qui ne seront pas utilisées) doivent être identifiées. Il doit être démontré que ces fonctions ne peuvent compromettre la réalisation des fonctions demandées.

  NOTE 4 S'il existe des propriétés et des caractéristiques de composants préexistants, qui n'ont pas été explicitement identifiées dans la documentation fournie pour l'équipement, ou si l'utilisation des propriétés, caractéristiques ou des fonctions est limitée de façon à satisfaire la spécification d'exigence système, alors la production d'une version spéciale sur mesure de la documentation du composant peut être nécessaire pour pouvoir être la base d'une qualification particulière à l'application (voir 6.5.2). La documentation sur mesure centrée sur l'utilisation sûre du composant est parfois appelée « documentation pour la sûreté ».

d) Si des différences sont identifiées entre les exigences du système et la spécification des composants candidats et que celles-ci rendent les composants inadaptés à la classe du système, ceux-ci doivent être rejetés. L'estimation de l'aptitude à l'emploi doit établir que la spécification des composants candidats est conforme avec l'utilisation qu'il est prévue d'en faire et qui est définie par les spécifications des exigences système (voir 6.4.3.2).

  NOTE 5 Les caractéristiques des produits et familles d'équipements disponibles telles que mises en évidence durant l'évaluation peuvent avoir une influence sur la conception ultérieure des systèmes et entraîner des itérations au niveau de la conception de l'architecture d'ensemble de l'I&C.

e) Pour les systèmes de classe 1 et 2, la faisabilité de la qualification conformément aux exigences de 6.5 doit être vérifiée.

  NOTE 6 L'évaluation de la faisabilité de la qualification fait intervenir non seulement les propriétés techniques du composant candidat mais aussi des questions organisationnelles et contractuelles, par exemple l'accessibilité à la documentation de la conception détaillée, et la disponibilité d'un temps suffisant, et ceci en supposant que les activités de qualification puissent débuter au plus tard au début de la spécification du système.

f) Si les résultats d'une pré-qualification sont utilisés (par exemple des résultats génériques, un programme de qualification indépendant de la centrale, ou les résultats d'un autre projet), les propriétés démontrées doivent être identifiées explicitement. On doit garantir qu'on peut accéder à ces justifications dans la documentation. Les contraintes additionnelles et le supplément de travail nécessaire pour la qualification spécifique à la centrale doivent également être identifiés.

6.2.3.3 Architecture du système

6.2.3.3.1 Généralités

L'architecture divise le système en sous-systèmes et composants interconnectés assurant le niveau de redondance requis et permettant les reconfigurations définies. L'objectif de cette partition est de parvenir à une configuration optimale simple du matériel et du logiciel qui satisfasse aux exigences de fonctionnalité et de performance et qui soit conforme aux exigences de fiabilité et de maintenance.

L'organisation des sous-systèmes doit

- satisfaire aux exigences du 6.2.2.3,
- permettre de satisfaire aux exigences relatives à l'affectation des fonctions d'application (voir 6.2.3.5),
- être en accord avec les exigences de fiabilité des fonctions d'application importantes pour la sûreté (voir 6.2.2.2.2).

6.2.3.3.2 Répartition géographique des sous-systèmes (centralisés/décentralisés)

Lors de la définition des emplacements géographiques des sous-systèmes dans la centrale et des chemins de transmission de données entre ces sous-systèmes, il convient que les facteurs suivants soient pris en compte:

- la séparation des voies redondantes d'un équipement dont le vote est majoritaire peut être nécessaire afin de réduire les conséquences d'événements dangereux localisés, tels que les incendies, et de respecter le critère de défaillance unique lorsqu'il est requis (voir 6.2.2.3.2);
- la centralisation des fonctions importantes pour la sécurité peut être nécessaire pour respecter l'exigence relative au contrôle des accès non autorisés (voir 5.5.3);
- la centralisation des composants complexes peut faciliter l'exploitation, les essais périodiques, la maintenance et la maîtrise des conditions d'environnement;
- l'utilisation de transmissions de données en série ou multiplexées peut réduire le volume du câblage nécessaire et faciliter la mise en œuvre du principe de séparation physique.

6.2.3.3.3 Indépendance

Le principe d'indépendance prévoit des dispositions pour éviter les interactions néfastes entre les sous-systèmes du système, ou avec d'autres systèmes, dues à un fonctionnement anormal ou à la défaillance de composants du système ou de sous-systèmes, y compris les défaillances de cause commune. Ces interactions peuvent aussi être causées par un phénomène d'induction électromagnétique, des courts-circuits, des défauts de mise à la terre, des incendies, des explosions chimiques, des chutes d'avion et la propagation de données altérées.

a) Lorsque l'indépendance est requise (voir 6.2.2.3.2), il convient que cette exigence soit satisfaite en appliquant les principes
   - d'isolement électrique, ce qui peut être réalisé en utilisant des fibres optiques, des isolateurs optiques et le blindage des câbles;
   - de séparation physique, ce qui peut être réalisé par éloignement, mise en place de barrières ou bien combinaison des deux;

- de l'indépendance des communications pour les systèmes programmés, ce qui peut être réalisé en sélectionnant des architectures et protocoles de communication appropriés (voir également 5.4.2.4).

NOTE 1 Les exigences relatives à l'isolement électrique et à la séparation physique figurent en 4.36 à 4.48 de l'AIEA NS-G-1.3:2005.

b) Dans un système de classe 1, la séparation physique et l'isolement électrique entre sous-systèmes redondants doivent être conformes aux exigences de la CEI 60709.

c) La séparation et l'isolement entre un système important pour la sûreté et les systèmes et composants non importants pour la sûreté doivent être conformes aux exigences de la CEI 60709.

NOTE 2 La méthode privilégiée pour la séparation physique et la protection des câbles d'un système de sûreté, véhiculant des signaux électriques ou optiques, est l'utilisation de boîtiers ou de goulottes de câbles particuliers garantissant une protection totale contre les événements dangereux.

6.2.3.3.4 Défense contre la propagation des défaillances et leurs effets secondaires

Du fait du haut niveau de concentration des fonctions dans les systèmes informatisés, il convient, dans le cadre des bonnes pratiques de conception, que des mesures soient prises pour limiter les effets secondaires des défaillances survenant à l'intérieur d'un seul sous-système, en plus des mesures mises en œuvre contre la propagation des défaillances entre les systèmes indépendants.

Il convient qu'une défaillance d'un matériel ne requiert pas trop d'actions de commande manuelles de la part du personnel de conduire pour contrôler les conséquences de cet événement. Il convient en particulier de prendre ceci en compte lors de la conception des boucles de régulation fermées dans les systèmes de classes 2 ou 3 pour lesquels on considère fréquemment que l'opérateur est le moyen de contrôle de secours.

Les techniques suivantes peuvent être considérées pour minimiser les risques et les conséquences relatifs à la propagation d'une défaillance ainsi que les effets de bord liés à une défaillance au niveau de l'architecture:

- l'isolement interne, qui bloque la propagation des défaillances du fait de l'absence de chemins de propagation et de ressources partagées;
- la surveillance du système par des moyens internes (c'est-à-dire l'auto-supervision) ou externes (c'est-à-dire par d'autres systèmes ou par l'opérateur), permettant une détection rapide des données altérées et/ou des ressources détériorées;
- les interfaces défensives, permettant au système et à ses sous-systèmes d'identifier les informations d'entrée altérées et/ou les interactions erronées;
- la validation en ligne des signaux d'entrée redondants utilisés comme informations d'entrée pour les traitements postérieurs;
- les modes de comportement bien définis qu'il convient d'adopter lorsque des défaillances sont détectées, permettant au système de réduire le potentiel de propagation des défaillances et/ou de leurs effets secondaires.

NOTE 1 Pour les systèmes de classe 1, les exigences détaillées pour éviter les structures logicielles prédisposées aux erreurs et pour vérifier et contrôler les modules logiciels figurent dans la CEI 60880.

NOTE 2 Les exigences détaillées concernant la défense contre la propagation et les effets de bord liés aux défaillances sont fournies par la CEI 62340.

6.2.3.4 Spécification du logiciel

La spécification du logiciel contient:

- la spécification des fonctions d'application (spécifications du logiciel d'application);
- la spécification de l'architecture du logiciel;

NOTE 1 L'architecture du logiciel définit les principaux composants et sous-systèmes du logiciel, leur interconnexion et la manière dont les caractéristiques exigées seront atteintes. Les exigences relatives à l'architecture du logiciel sortent du domaine de la présente norme. (Pour les systèmes de classe 1, se référer à la CEI 60880, pour les systèmes de classe 2 ou 3 se référer à la CEI 62138.)

- la spécification des fonctions de service et des fonctions du logiciel système.

NOTE 2 Lorsque des familles d'équipements préexistants sont utilisées, les spécifications du logiciel système font essentiellement partie de la documentation des équipements.

Les exigences applicables à la spécification logiciel sont fournies par la CEI 60880 (pour les systèmes de classe 1) et par la CEI 62138 (pour les systèmes de classes 2 et de classe 3).

6.2.3.5 Affectation des fonctions d'application dans le système

Ceci inclut l'affectation

- des signaux d'entrée aux fonctions et des fonctions à des processeurs spécifiques,
- du processus de vote, de la gestion des priorités, des fonctions de protection des composants,
- des liens entre les actions de commande des sorties et les actionneurs.

Les exigences suivantes sont applicables:

a) L'affectation des fonctions d'application importantes pour la sûreté au système et aux sous-systèmes doit respecter la spécification des exigences fonctionnelles, de performance et de catégorisation des fonctions (voir 6.2.2.2.2).

b) L'affectation doit tenir compte du confinement des défaillances.

c) Le traitement des fonctions redondantes et les signaux importants pour la sûreté doivent être affectés à des sous-systèmes séparés, afin qu'en cas de survenance d'une défaillance ou d'un événement dangereux localisé dans un sous-système, le système puisse encore accomplir ses fonctions.

d) Les fonctions de différentes catégories affectées au même système ou sous-système doivent toutes être considérées comme appartenant de la catégorie de sûreté la plus élevée, sauf s'il est démontré que des données et fonctions de catégories inférieures ne peuvent compromettre les fonctions des catégories supérieures, par exemple arrêter ou déclencher de manière intempestive l'une de ces dernières. Ceci peut conduire à répartir les fonctions dans différents sous-systèmes, ou à affecter les fonctions de catégories inférieures à d'autres systèmes (itération du processus avec affectation d'ensemble - voir 5.4).

e) Pour les fonctions de catégorie A, le critère de défaillance unique doit être satisfait au cours de l'exploitation, même lorsqu'une voie redondante est isolée pour cause de maintenance.

6.2.4 Conception détaillée et réalisation du système

6.2.4.1 Généralités

L'objectif de cette phase est de

- développer et obtenir la conception détaillée du matériel du système,
- développer (conception et codage), respectivement et obtenir, les programmes informatiques qui constituent le logiciel système opérationnel et de soutien,

NOTE 1 La situation normale (voir 6.2.3.3) veut que les nouveaux développements soient limités, par exemple, interfaces avec les autres systèmes.

- développer (conception et codage) respectivement et produire automatiquement le logiciel d'application du système.

NOTE 2 En utilisant des familles d'équipements préexistants, le code du logiciel d'application est bien souvent généré automatiquement à partir de la spécification du logiciel d'application (voir 6.2.3.4).

La documentation de spécification du système et le plan d'intégration du système sont les principales informations d'entrée pour la phase de conception détaillée et de réalisation.

Les résultats de cette phase sont

- les sous-systèmes et composants matériels et logiciels pour la phase suivante d'intégration du système,
- les programmes informatiques exécutables sur le système.

Le développement et l'obtention du matériel et du logiciel font partie des cycles de vie du matériel et du logiciel et sortent ainsi du cadre de la présente norme.

Pour les systèmes de classe 1, les exigences relatives au développement du logiciel sont fournies par la CEI 60880 et pour les systèmes de classe 2 ou 3 elles sont fournies par la CEI 62138, enfin les exigences relatives au matériel sont fournies par la CEI 60987.

6.2.4.2 Analyses requises

6.2.4.2.1 Validation fonctionnelle de la spécification des exigences relatives aux fonctions d'application

La validation fonctionnelle a pour objectif de détecter les erreurs ou omissions concernant la spécification des fonctions d'application et qui peuvent ne pas être détectées par la validation du système (voir 6.2.6). La validation fonctionnelle implique la modélisation de la dynamique des actionneurs et de l'exploitation de la centrale nucléaire. Un émulateur de l'I&C, un simulateur d'ingénierie ou même un simulateur pleine-échelle de formation peuvent être utilisé comme environnement d'essai.

a) La conformité de la spécification des fonctions d'application aux exigences de fonctionnalité et de performance des fonctions la centrale (voir 5.2.2) doit être validée pour les fonctions de catégorie A.

b) Il convient de réaliser la validation fonctionnelle des fonctions d'application avant de développer le logiciel d'application, sur la base d'analyses et de simulation. La validation fonctionnelle peut être aussi réalisée au cours de la phase de conception détaillée, par exemple lors de l'exécution finale du logiciel couplé à la simulation de la centrale.

NOTE La validité de cette validation dépend de la qualité du simulateur.

6.2.4.2.2 Estimation de la fiabilité

a) Il doit être justifiée que le niveau de fiabilité atteint par les fonctions d'application supportées par le système est approprié. Il convient que la rigueur de la démonstration soit plus forte pour les fonctions de la catégorie la plus élevée:

   - la démonstration doit reposer sur des critères déterministes et être complétée, lorsque cela est approprié, par une analyse quantitative de la fiabilité;
   - l'effet d'éventuelles défaillances du matériel sur la fiabilité de la fonction doit être déterminé par une analyse probabiliste quantitative reposant sur le taux de défaillances des composants. L'analyse englobe l'architecture du système et les composants, et il convient qu'elle prenne en compte les défaillances permanentes et transitoires;
   - il convient que l'estimation des effets des erreurs de conception potentielles du logiciel sur la fiabilité de la fonction repose sur une évaluation qualitative, tenant compte de la complexité de la conception, de la qualité du processus de développement et du retour d'informations sur l'expérience opérationnelle. Il convient que l'évaluation repose sur une méthode préalablement convenue et démontre que la qualité du logiciel correspond à la fiabilité voulue.

     NOTE Les résultats de l'analyse et des essais de simulation pourraient être utilisés pour une évaluation quantitative, mais il n'existe aucune méthode reconnue qui puisse être utilisée. Pour les systèmes câblés, aucune quantification des défaillances provenant de défauts de conception n'a généralement été donnée.

b) La capacité des fonctions de service du système à perturber les fonctions d'application doit être analysée avec une rigueur adaptée à l'importance pour la sûreté des fonctions d'application.

c) Si la fonction réalisée par le système fait partie d'un groupe de sûreté et que des exigences de fiabilité, liées à l'architecture d'I&C, portent sur ce groupe (voir 5.4.4.2), l'analyse de fiabilité doit prendre en compte les effets des défaillances uniques, des DCC et de la propagation des défaillances au sein de tous les systèmes contribuant à ce groupe.

d) Pour les systèmes de classe 1, l'analyse de fiabilité doit également estimer la conformité des dispositifs de test du système aux exigences du 6.2.2.3.5.

6.2.5 Intégration du système

L'objectif de cette phase est d'assembler les modules matériels et logiciels et pour vérifier la compatibilité du logiciel chargé dans le matériel.

NOTE 1 Pour l'application de 6.2 et 6.3 aux composants matériels programmables complexes tels que des PLD ou des FPGA, les exigences relatives au logiciel sont aussi applicables aux données de configuration et de programmation de tels matériels.

L'intégration système comprend les étapes suivantes:

- assemblage et branchement des modules matériel et des sous-systèmes tels que définis dans les documents de conception;
- réalisation du logiciel cible à partir des modules logiciel;
- chargement du logiciel cible sur le matériel cible;
- vérification
  - que le logiciel satisfait aux spécifications de conception,
  - que les exigences relatives à l'interface logiciel/matériel sont satisfaites,
  - que le logiciel est capable de fonctionner dans cet environnement matériel particulier;
- documentation de la configuration et mise à disposition formelle pour les essais de validation.

Les sous-systèmes et composants du système, la documentation de conception détaillée et le plan d'intégration du système constituent les principales informations d'entrée pour la phase l'intégration du système. Les exigences suivantes sont applicables:

a) L'intégration doit être réalisée conformément au plan d'intégration et au plan de gestion de configuration défini en 6.3, avec les supports matériel ayant satisfait aux essais usine.

b) Les exigences de performance doivent être vérifiées lorsque l'ensemble du logiciel d'application (développés en utilisant les outils de la famille d'équipements ou spécifiquement développés) est intégré dans le système.

c) Le système doit être aussi complet que possible pour cet essai.

d) Les cas d'essai choisis pour les essais d'intégration système doivent solliciter les caractéristiques d'interface des modules logiciel et des sous-systèmes et les caractéristiques de base de fonctionnement des modules et des sous-systèmes eux-mêmes, ces caractéristiques étant tirées de la spécifications des exigences (par exemple la synchronisation, les protocoles particuliers à l'application). Les essais doivent montrer que les performances de tous les équipements mis en jeu sont correctes.

e) On doit avoir des cas d'essai qui montrent que chaque fonction d'application choisie réalise sa tâche.

NOTE 2 Suivant les techniques de conception utilisées pour garantir un comportement prédictible du système (voir le paragraphe 6.2.2.3.3), des cas d'essai comprenant des données aléatoires entraînant de hauts niveaux de variations en entrée d'autres fonctions à l'intérieur d'un même système programmé, peuvent être nécessaires.

f) Les équipements utilisés pour la vérification système doivent être étalonnés comme requis.

g) Les mesures d'assurance qualité doivent être établies pour les outils logiciel utilisés pour la vérification en fonction de l'importance de ces outils pour la vérification.

h) Le rapport d'essai du système intégré doit faire l'objet d'une revue et les résultats des essais doivent être évalués par une équipe de vérification possédant une bonne connaissance des spécifications système.

i) Si la résolution des défauts nécessite une modification de n'importe lequel des composants matériel ou logiciel vérifié ou de n'importe quel document de conception, ce défaut doit faire l'objet d'un compte rendu conformément aux procédures établies (voir 6.3.2.4). Tout défaut détecté durant l'intégration système qui correspond strictement à des erreurs du processus d'intégration lui-même, et qui n'a de conséquence sur aucun document projet, peut être corrigé sans compte rendu formel de défaut.

6.2.6 Validation du système

L'objectif de cette phase est de tester le système intégré afin de démontrer la conformité aux spécifications de fonctionnalité, de performance et d'interface.

Des essais doivent être réalisés pour valider le système et son logiciel, les données de programmation et de configuration doivent être conformes aux exigences système.

La validation doit comprendre des essais réalisés sur le système dans la configuration d'assemblage finale comprenant la version finale du logiciel et les autres données de programmation.

Le système intégré, la spécification du système et le plan de validation du système constituent les principales informations d'entrée pour la phase de validation du système.

a) La validation doit être réalisée conformément au plan de validation défini en 6.3.5.

b) Le système doit être sollicité par une simulation statique et dynamique des signaux d'entrée normalement présents en fonctionnement normal, en conditions de fonctionnement incidentel et accidentel nécessitant une réaction des systèmes en essai.

c) Chaque fonction du système doit être évaluée par des essais représentatifs, pour ce qui concerne les exigences relatives à la fonctionnalité, aux performances et pour ce qui est des interfaces. On doit fournir des justifications pour les exigences non couvertes.

d) Pour des fonctions de catégorie A et B, chaque paramètre d'arrêt d'urgence ou de protection doit être considéré de façon isolée et par une combinaison pertinente. Les essais doivent:

- couvrir toutes les gammes de signaux, et les gammes de paramètres calculés d'une façon pleinement représentative;
- couvrir les logiques de vote et autres logiques et les combinaisons de logique de façon exhaustive;
- être faits pour tous les signaux d'arrêt d'urgence ou de protection de la configuration d'assemblage final;
- garantir que la précision et les temps de réponse sont corrects et que les bonnes actions sont mises en œuvre en cas de défaillance ou de combinaison de défaillances d'équipements pertinentes;
- être faits pour toutes les autres fonctions qui ont une influence directe sur la sûreté du réacteur (par exemples permissifs, verrous).

e) Pour les fonctions de catégories C:

- Chaque fonction doit être couverte par un ensemble d'essais approprié et justifié, reposant sur des gammes représentatives de signaux, de paramètres ou de combinaisons de logique. Chaque signal individuel doit être vérifié.

- Il convient de vérifier à l'aide d'essais la satisfaction des exigences critiques en matière de précision ou de temps de réponse dont font l'objet les signaux.

f) Pour les systèmes de classe 2 et de classe 3, il peut y avoir besoin d'essais particuliers, par exemple les essais des fonctionnalités de reprise sur défaillance, ou les essais liés à un changement de charge système (si le système n'est pas programmé pour être indépendant des demandes de la centrale).

g) Il doit être vérifié que le système présente des moyens de défense contre les erreurs opérateur et les défaillances des autres systèmes et équipements, tels que définis dans les spécifications d'exigences système.

h) Les équipements utilisés pour la validation doivent être étalonnés et configurés (paramètres matériel et logiciel) de façon appropriée.

i) Il convient de montrer que les équipements utilisés pour la validation sont appropriés à la validation du système.

Le rapport de validation système doit documenter les résultats de la validation du système.

a) Le rapport doit identifier le matériel, le logiciel et la configuration du système utilisée, l'équipement utilisé et ses paramètres d'étalonnage et les modèles de simulation utilisés.

b) Ce rapport doit aussi identifier toutes les discordances.

6.2.7 Installation du système

L'objectif de cette phase est d'installer, d'interconnecter et de tester le système sur site.

Les activités suivantes, relatives à l'intégration globale du système aux autres systèmes et à la mise en service globale font partie du cycle de vie de sûreté de l'ensemble de l'I&C (voir l'Article 7).

a) L'installation du système doit être réalisée conformément au plan d'installation défini en 6.3.6.

b) Des moyens appropriés, par exemple étiquetage ou code couleur, doivent être utilisés pour identifier le système de manière unique et pour réduire la probabilité d'erreurs d'installation, d'exploitation et de maintenance.

6.2.8 Modifications du système

Des modifications système peuvent être demandées en raison de l'identification de nouvelles exigences relatives au système ou de la découverte de défauts de conception du système au cours de l'analyse des comptes-rendus et des enregistrements d'exploitation.

a) L'intégration d'une modification dans un système doit être réalisée conformément aux procédures définies (voir 6.4.7).

b) Un contrôle du bon fonctionnement du système doit être effectué après une modification.

c) Aucune modification matérielle ou logicielle autre que celles spécifiées dans les procédures de maintenance ne peut être apportée dans le cadre des opérations de routine.

d) Si le remplacement du matériel est demandé, il doit être démontré et justifié que ce remplacement respecte la spécification du matériel d'origine.

e) Les processus de modification du logiciel doivent être conformes respectivement à l'Article 11 de la CEI 60880:2006 pour les systèmes de classe 1 et en 5.10 et 6.10 de la CEI 62138:2004 pour les systèmes de classe 2 ou 3. Le processus de modification pour le matériel des systèmes de classe 1/classe 2 doit satisfaire aux exigences de l'Article 12 de la CEI 60987:2007.

6.3 Planification système

6.3.1 Généralités

L'objectif des exigences du présent article est de développer les plans système afin d'assurer que les exigences sur les fonctions d'I&C importantes pour la sûreté supportées par le système seront respectées et maintenues.

Les exigences de 5.5 s'appliquent aux plans globaux. Ces plans spécifient des dispositions complémentaires relatives aux fonctions réparties au sein des systèmes interconnectés.

NOTE Les exigences suivantes relatives aux plans n'excluent pas le fait que ceux-ci puissent être organisés dans plusieurs documents différents.

Les plans système doivent être établis tôt dans le cycle de vie du système, avant le commencement des activités concernées.

6.3.2 Plan d'assurance qualité du système

6.3.2.1 Généralités

a) Un plan d'assurance qualité, couvrant chaque activité en rapport avec le cycle de vie de sûreté du système, doit être établi et mis en œuvre. Les exigences relatives au plan d'assurance qualité du système sont dérivées de l'AIEA GS-G-3.1 et de l'ISO 9001.

b) Le plan d'assurance qualité du système doit comprendre les activités nécessaires à l'obtention d'une qualité appropriée du système, pour vérifier que la qualité désirée est bien atteinte et fournir une preuve objective à cet effet. Les exigences relatives aux activités de vérification figurent dans le plan de vérification du système (voir 6.3.2.2).

c) Le plan d'assurance qualité du système doit traiter de la qualité du système et des aspects de la qualité liés à l'intégration du matériel et du logiciel. Les plans d'assurance qualité spécifiques au matériel et au logiciel sortent du cadre de la présente norme.

NOTE Les exigences relatives au plan d'assurance qualité du logiciel des systèmes de sûreté sont définies en 5.5 de la CEI 60880:2006 pour les systèmes de classe 1 et en 6.1 et 5.1 de la CEI 62138:2004 pour les systèmes de classe 2 et de classe 3.

d) Le plan d'assurance qualité du système doit contenir:

- l'identification des normes et procédures devant être appliquées pour le projet;
- l'identification des phases du cycle de vie du système, les activités élémentaires et les résultats attendus de chaque phase;
- la description des relations et des interactions entre les différentes activités;
- la description de la structure organisationnelle;
- l'approvisionnement des composants auprès des fournisseurs externes;
- l'identification et la traçabilité du produit. Les exigences correspondantes figurent dans le plan de gestion de la configuration (voir 6.3.2.3);
- l'identification de toutes les procédures d'inspection et d'essai;
- l'identification des activités et tâches d'assurance qualité;
- l'identification du personnel et des organisations responsables des activités et tâches d'assurance qualité, y compris les exigences relatives à l'indépendance organisationnelle entres les activités pertinentes du cycle de vie du projet;
- les procédures de déclaration et de résolution des non-conformités aux exigences, normes et procédures. Les procédures doivent inclure la prise en compte de l'impact sur la sûreté de la centrale nucléaire et doivent assurer que tous les effets des non conformités sont identifiés, par exemple l'interchangeabilité, la maintenance, les pièces de rechange, la notice de fonctionnement, etc.

e) Le plan d'assurance qualité doit être établi tôt dans le cycle de vie du système et doit être prévu dans le programme général des autres activités du cycle de vie de sûreté de l'I&C.

Le plan peut soit faire partie de la spécification du système, soit constituer un document associé (voir 5.5 de la CEI 60880:2006 pour les systèmes de classe 1 et 6.1/5.1 de la CEI 62138:2004 pour les systèmes de classe 2 et de classe 3).

6.3.2.2 Plan de vérification du système

a) Un plan de vérification du système doit être établi et décrire

- le processus de vérification au cours de toutes les phases du cycle de vie de sûreté du système,
- l'organisation et les responsabilités correspondantes.

b) Les résultats de chaque phase du cycle de vie de sûreté du système doivent être vérifiés par rapport à des entrées identifiées.

c) Chaque étape de vérification doit conduire à un rapport sur l'analyse effectuée et les conclusions atteintes. Lorsqu'une phase est achevée, un rapport final doit être rédigé, montrant la conformité des résultats de la phase aux exigences initiales et la résolution des anomalies.

d) La vérification doit être réalisée par des personnes compétentes dans les sujets concernés et possédant une bonne compréhension des informations d'entrée vis à vis desquelles la vérification est effectuée, l'implication des représentants des personnes concernées par l'utilisation des résultats est recommandée.

e) La minutie apportée au plan de vérification doit être proportionnelle à la classe de sûreté du système. Le plan de vérification doit souligner les aspects importants à vérifier pour la sûreté et il convient qu'il reconnaisse le fait que la probabilité d'une erreur ou omission dans les sujets complexes soit plus importante que dans les plus simples.

f) Les documents soumis à une vérification doivent être identifiés dans le plan d'assurance qualité du système.

g) Les documents associés à une vérification, c'est-à-dire les entrées et sorties des activités, les rapports de vérification et, éventuellement, les outils utilisés, doivent être gérés en termes de configuration.

h) Pour les systèmes de classe 1, le plan de vérification doit être développé et mis en œuvre par des personnes indépendantes de celles ayant conçu le système (selon 8.2.1 de CEI 60880:2006).

6.3.2.3 Plan de gestion de configuration du système

a) Identification de la configuration:

- des unités de configuration appropriées doivent être définies en des points de contrôle au cours du cycle de vie du système et les éléments à contrôler doivent être définis. Les éléments contrôlés peuvent être des résultats intermédiaires et finals (tels que la documentation du matériel, du logiciel ou de vérification, le manuel de l'utilisateur) et des éléments de l'environnement de soutien (tels que les compilateurs, outils, bancs d'essai);
- tous les éléments à contrôler doivent être identifiés. Chaque élément à contrôler doit être identifié. Chaque élément unique doit avoir une référence unique et les différentes versions doivent être identifiées de façon unique;
- les liens entre les éléments d'une unité de configuration et les éléments à partir desquels ils ont été développés doivent être établis et enregistrés;
- le système de gestion de configuration doit être capable de reconstituer la configuration de toutes les unités de configuration du système;
- il convient que des moyens de recherche soient disponibles afin que les liens et les occurrences multiples d'éléments puissent être facilement identifiés.

b) Contrôle de configuration:

- le contrôle de configuration doit permettre de geler un état de la conception. Les procédures et l'autorité requises pour toute autre modification après le gel doivent être définies, y compris l'allocation aux organisations et aux individus dans la structure du

projet, des responsabilités et de l'autorité pour ce qui concerne les activités de gestion des configurations;

- l'état de chaque élément contrôlé doit faire l'objet d'un suivi; ceci inclut les informations sur la version initiale approuvée, la nature des changements demandés et la réalisation des changements approuvés;
- le plan de gestion des configurations doit identifier les audits et les revues de configuration qui doivent avoir lieu;

NOTE 1 Il est de bonne pratique de distinguer entre les éléments internes (par exemple ceux développés dans le cadre du projet) et ceux externes (ceux fournis par des vendeurs ou des sous-contractants) et de définir les activités pour contrôler les interfaces des éléments externes.

c) Le plan de gestion de configuration doit être défini au début du projet du système et doit être conservé pendant tout le cycle de vie du système.

NOTE 2 L'ISO 10007 [17] fournit des définitions et des recommandations pour la gestion des configurations, l'IEEE 828 [18] fournit des recommandations à propos des plans de gestion des configurations logiciel.

6.3.2.4 Procédure de résolution des défauts

On doit établir, avant que les phases suivantes ne commencent, les procédures de compte rendu et de résolution relatifs aux défauts trouvés durant la vérification de l'intégration système, durant la validation système et dans les phases ultérieures.

a) Ces procédures doivent être référencées au niveau des plans d'intégration système et validation système.

b) Ces procédures doivent être appliquées pour tous les défauts trouvés durant la phase d'intégration système et la phase de validation système qui entraînent des modifications des logiciels ou du matériel vérifiés ou des documents de conception du système.

c) Elles doivent garantir que toutes les revérifications de la conception du système, du logiciel ou du matériel sont réalisées conformément au plan de gestion de la configuration du système.

d) Elles doivent garantir que toutes modifications nécessaires de la conception du système, du matériel ou du logiciel sont réalisées conformément à la procédure de modification des paragraphes 6.2.8 et 6.4.7, ainsi qu'au plan de gestion de configuration du système.

e) Une évaluation de chaque défaut doit être réalisée pour déterminer si un défaut systématique existe et aussi pour déterminer si le défaut est de nature telle qu'il aurait du être détecté lors d'une phase de vérification précédente.

f) Si c'est le cas (à savoir que le défaut aurait du être détecté lors d'une phase précédente), alors on doit réaliser des investigations sur cette phase pour déterminer s'il existe une déficience systématique au niveau de la vérification.

g) Si l'évaluation des défauts montre qu'il y a une déficience systématique au niveau vérification qui entraîne l'apparition de défauts sur le logiciel ou le matériel qui peuvent rester non détectés, alors la déficience doit être identifiée et corrigée ou faire l'objet de justifications.

6.3.3 Plan de sécurité du système

Le plan de sécurité du système est défini en cohérence avec le plan de sécurité globale de l'I&C (voir 5.5.3).

a) Durant la spécification et la conception du système, il convient que les exigences relatives aux contre-mesures techniques identifiées pour le système dans le plan de sécurité global (voir 5.5.3) soient converties en exigences de conception techniques et soient documentées.

b) Une évaluation de la conception doit avoir lieu afin de vérifier que les contre-mesures identifiées dans le cadre de l'analyse de sécurité du système ont été mises en œuvre correctement.

c) Durant la vérification et la validation du système, l'efficacité des fonctions de sécurité doit être démontrée par des essais appropriés, le système étant dans sa configuration finale.

6.3.4 Plan d'intégration du système

Le plan d'intégration du système traite des mesures administratives et techniques utilisées pour intégrer les sous-systèmes au système et pour intégrer le matériel et le logiciel.

a) Un plan d'intégration du système doit être préparé et définir les types d'essais à effectuer, l'environnement des essais et les critères d'acceptation.

b) Les essais d'intégration doivent être fondés sur un concept d'intégration progressive.

c) Il convient de faire la distinction entre les essais propres au système (fonctions du logiciel système et du matériel) et les essais spécifiques à la centrale (fonctions d'application).

NOTE Les essais des modules (matériel, logiciel, modules combinés, la programmation des composants électroniques complexes tels que les PLDs ou les FPGAs) réalisés lors du développement du produit ou de la préqualification ou des projets antérieurs peuvent être utilisés afin d'éviter la répétition de cas d'essais identiques ou inutiles.

d) Dans le plan d'intégration système, il doit être montré que la simulation de toute partie de système ou de ses interfaces est essentielle et quelle est équivalente à celle du composant réel. Le plan doit identifier les essais réalisés sur le système réel et ceux réalisés en utilisant la simulation des interfaces. L'équivalence de la simulation doit être montrée. Le simulateur doit être couvert par la gestion de configuration.

e) Le plan d'intégration système doit identifier les essais à réaliser pour chaque exigence relative aux unités informatiques ou aux interfaces des sous-systèmes.

f) Le plan d'essais prévu pour l'intégration système doit faire l'objet d'une revue par une équipe de vérification possédant une bonne connaissance des spécifications système.

6.3.5 Plan de validation du système

Le plan de validation du système traite des mesures administratives et techniques prises pour démontrer que le système est conforme à sa spécification et à ses exigences. La validation des exigences relatives aux fonctions d'application est traitée dans la phase de validation fonctionnelle (voir 6.2.4.2.1).

a) Un plan de validation du système doit être établi et décrire la ou les configuration(s) du système utilisée(s) pour sa validation, ainsi que les essais et analyses à réaliser et les rapports à produire.

   1) Les documents relatifs aux essais de validation doivent spécifier la configuration du système à soumettre aux essais, les informations d'entrée, les méthodes, outils et étalonnages à utiliser et les critères d'acceptation appropriés. Si cela est pertinent, il convient d'estimer la précision et l'influence des outils d'observation sur le comportement du système.

   2) Les documents relatifs aux analyses de validation doivent spécifier ce qu'il convient que les essais montrent, les résultats attendus et les critères d'acceptation appropriés.

      NOTE 1 Il est de bonne pratique que la préparation du plan de validation système et de la spécification des essais débutent dès la fin de développement de la première version des spécifications d'exigence système, pour qu'on puisse utiliser les observations faites durant la préparation de la spécification des essais comme un premier retour pour la préparation des spécifications d'exigences.

b) Pour des fonctions de catégorie A, le plan de validation du système doit être établi, les activités de validation doivent être réalisées ainsi que les résultats évalués par des équipes indépendantes de celles qui ont conçu, réalisé ou modifié le système (voir Article 10 de la CEI 60880:2006).

   NOTE 2 L'indépendance n'est pas demandée entre les personnes impliquées dans la réalisation du plan de validation et à la production du rapport de validation.

c) Pour les fonctions de catégorie B, l'équipe de développement du plan de validation du système doit inclure, et être sous la responsabilité, de personnes qui n'ont pas participé à la conception, à la réalisation et/ou à la modification du système.

d) Pour les fonctions de catégorie A et B, le plan de validation du système doit prévoir la traçabilité entre la spécification et les essais et analyses correspondants.

e) Pour les fonctions de catégorie C, il convient que le plan de validation du système prévoie la traçabilité entre la spécification et les essais et analyses correspondants.

Il est de bonne pratique de mettre en œuvre les essais de validation en plusieurs étapes à l'usine et sur le site. Une stratégie de mise en œuvre par étape des essais de validation (voir aussi 5.5.4) peut comprendre des étapes telles que

- des essais de simulation/émulation pour valider le logiciel d'application,
- un premier ensemble d'essais de validation compris dans le domaine des essais d'intégration en usine,
- un deuxième ensemble d'essais de validation réalisé durant les essais d'intégration sur site,
- la fin des essais de validation dans le cadre du programme d'ensemble de mise en service de la centrale.

6.3.6 Plan d'installation du système

Le plan d'installation du système traite des mesures administratives et techniques pour l'installation du système sur site et pour le contrôle de son aptitude à une utilisation opérationnelle. Le plan est complété par les plans d'intégration et de mise en service globales (voir 5.5.4).

a) Un plan d'installation du système doit être établi et décrire les mesures à prendre pour assurer et vérifier que la configuration du système et de tous les paramètres modifiables est correcte, que le système est complet, correctement installé, assemblé et connecté, et fonctionne comme prévu et spécifié.

b) Pour les systèmes de classe 1, le plan d'installation doit être conforme aux exigences de l'Article 10 de la CEI 60987:2007.

c) Pour les fonctions de catégorie A, l'exactitude de chaque voie doit être démontrée sur site.

6.3.7 Plan d'exploitation du système

Le plan d'exploitation du système traite de la manière dont le système doit être exploité et des exigences qui lui sont applicables pendant son fonctionnement.

a) Un plan d'exploitation du système doit spécifier la manière dont le système doit être exploité dans tous ses modes de fonctionnement. Le plan doit être en accord avec le plan de maintenance du système (voir 6.3.8) et avec les plans d'exploitation et de maintenance globaux (voir 5.5.5 et 5.5.6).

b) Il convient que le plan d'exploitation du système spécifie les conditions à remplir avant la mise en exploitation du système. En particulier:

   - l'installation, l'intégration et la décision de mise en service du système doivent être achevées (voir 5.5.4),
   - le plan de maintenance du système (voir 6.3.8) et le manuel d'utilisation doivent être disponibles.

c) Lorsque des essais périodiques sont prévus (voir 6.2.2.3.5), le plan d'exploitation du système doit spécifier:

   - la fréquence et la durée de chaque essai, les conditions à remplir avant la mise en œuvre d'un essai et les effets, le cas échéant, sur l'exploitation du système et de la centrale,
   - les étapes nécessaires pour réaliser chaque essai, les outils à utiliser et leurs étalonnages, l'analyse de la justesse des résultats,
   - la vérification du retour complet à l'état normal, si des modifications provisoires du système sont effectuées.

NOTE Les essais périodiques concernent aussi bien l'équipe opérationnelle que celle chargée de la maintenance. Cette activité peut également être considérée comme faisant partie de la maintenance de routine (voir 6.3.8).

d) Le plan d'exploitation du système doit spécifier les enregistrements à faire durant le fonctionnement du système. Les enregistrements doivent contenir les détails concernant les défaillances, les enregistrements des essais du système et un enregistrement des demandes de sollicitation du système.

e) Le plan d'exploitation du système doit être pris en compte pour l'impact qu'il peut avoir sur la sûreté de la centrale.

f) Le plan d'exploitation du système doit définir les essais périodiques du système conformément aux dispositions prévues en 6.2.2.3.5.

6.3.8 Plan de maintenance du système

La maintenance du système comprend les mesures administratives et les techniques à mettre en œuvre pour conserver la fonctionnalité du système opérationnel. Le plan de maintenance du système est établi de façon consistante avec le plan d'exploitation du système et avec les plans d'exploitation et de maintenance d'ensemble (voir 5.5.5 et 5.5.6).

a) Un plan de maintenance du système doit être établi et doit spécifier

- les mesures courantes et les procédures à suivre pour détecter les défaillances cachées du système, pour maintenir la performance fonctionnelle et la fiabilité du système « comme prévues à la conception » (maintenance préventive),
- les mesures et procédures qui doivent être suivies afin de remettre le système dans un état totalement opérationnel (maintenance corrective).

b) Il convient que l'étendue de la maintenance préventive soit déterminée par une méthode d'analyse systématique telle que l'analyse des modes de défaillance et de leurs conséquences ou par l'utilisation d'un modèle de maintenance axée sur la fiabilité, ou par l'examen des arbres de défaillances des fonctions du système.

c) Les procédures de remplacement des composants doivent assurer que

- les composants de rechange sont fonctionnellement identiques à ceux qui sont remplacés et sont conformes aux exigences relatives à la qualité,
- si le remplacement est effectué en marche, son impact sur la fonctionnalité du système est estimé et documenté avant de procéder au remplacement,
- un enregistrement de tous les remplacements, permettant de satisfaire aux exigences de traçabilité, est tenu à jour.

d) Les procédures de réétalonnage doivent assurer que

- le nouvel étalonnage se trouve dans des limites définies (lorsque la vérification du respect de ces limites est pris en charge par le système, il n'est pas nécessaire d'imposer de contraintes formelles supplémentaires au personnel de maintenance),
- si le réétalonnage est effectué en marche, son impact sur la fonctionnalité du système est estimé et documenté avant de procéder au réétalonnage,
- un enregistrement de tous les réétalonnages, permettant de satisfaire aux exigences de traçabilité, est tenu à jour.

6.4 Exigences relatives à la documentation

6.4.1 Généralités

Le présent paragraphe définit la documentation produite des phases du cycle de vie du système: contenu, caractéristiques et principaux points devant être vérifiés.

La documentation produite doit constituer un ensemble de documents, correctement référencés et cohérents entre eux, assurant la traçabilité de la conception finale depuis les exigences initiales.

6.4.2 Documentation de la spécification des exigences du système

6.4.2.1 Contenu

La spécification des exigences portant sur le système doit être complète, fournissant toutes les informations nécessaires aux activités aval du cycle de vie de sûreté du système et à la qualification du système.

6.4.2.2 Caractéristiques

Les caractéristiques de la documentation de spécification des exigences du système sont les suivantes:

a) les exigences doivent être non ambiguës et vérifiables;

b) les principaux utilisateurs de la spécification des exigences sont les vérificateurs et les personnes en charge de la spécification du système et de la validation fonctionnelle. Les exigences doivent être claires concises, complètes, consistantes et exactes, et développées en gardant en tête quels en seront les lecteurs;

c) il convient que les exigences relatives aux fonctions d'application soient spécifiées en termes fonctionnels plutôt qu'informatiques afin de permettre leur vérification par les ingénieurs de fonctionnement et par les opérateurs de la centrale qui peuvent avoir des connaissances limitées en technologie informatique;

d) il convient que les exigences soient spécifiées en utilisant des méthodes, des outils et des directives liés à l'ingénierie système et que ceux-ci soient documentés;

NOTE Les exigences détaillées relatives aux outils logiciels pour les systèmes de classe 1 figurent à l'Article 14 de la CEI 60880:2006.

e) il convient que les exigences soient rédigées et organisées pour faciliter l'évaluation de la conformité des spécifications du système et constituer une référence pour le plan de qualification du système.

6.4.2.3 Vérification

Les points suivants doivent être vérifiés:

a) les exigences doivent être traçables et cohérentes avec les exigences portant sur le système établies lors de la conception de l'architecture et de l'affectation des fonction (voir 5.6);

b) les exigences relatives aux interfaces du système considéré doivent être cohérentes avec celles des systèmes et des équipements auxquels il est connecté;

c) il convient d'identifier les exigences qui augmentent inutilement la complexité du système (la complexité peut accroître le risque d'erreurs dans la spécification des exigences du système et/ou dans le système lui-même).

6.4.3 Documentation de la spécification du système

6.4.3.1 Contenu

a) La documentation de spécification du système doit être complète et non ambiguë et doit fournir toutes les informations nécessaires aux activités aval dans le cycle de vie de sûreté du système, notamment pour les phases de conception et de validation du système.

b) La documentation de spécification du système doit identifier les équipements à utiliser, c'est-à-dire les équipements préexistants ou bien ceux à développer. L'aptitude à l'emploi des équipements choisis doit être justifiée.

c) La documentation de spécification du système doit décrire l'architecture du système:

- la décomposition du système en sous-systèmes et/ou en composants matériels et logiciels;

- le comportement interne du système (voir 6.2.2.3.3), y compris la description des principaux événements postulés internes au système et sa réaction face à ces événements (voir 6.2.3.3.4);
- les limites, les conditions environnementales, la fiabilité attendue du matériel, le comportement, les fonctions, les performances et interfaces de chaque sous-système,
- le classement de chaque sous-système; il convient de justifier le classement si la classe d'un sous-système est inférieure à celle du système ou du sous-système dans lequel il est inclus;
- les conditions d'utilisation et la connexion des sous-systèmes identifiés dans le système.

NOTE La description des sous-systèmes peut être réalisée hiérarchiquement afin d'en faciliter la compréhension, et ceci en partant d'une vue d'ensemble et en descendant jusqu'aux sous-systèmes élémentaires (c'est-à-dire les sous-systèmes qui, dans la documentation de conception du système, ne sont pas décomposés d'avantage). Des informations « horizontales » peuvent également s'avérer être utiles.

d) La documentation de spécification du système doit contenir la spécification du logiciel (voir 6.2.3.4).

e) Dans un système de la classe 1 ou 2, l'affectation des fonctions aux sous-systèmes doit être précisée, c'est-à-dire que la spécification du système doit indiquer les sous-systèmes qui contribuent et/ou sont nécessaires à la réalisation d'une fonction donnée.

6.4.3.2 Caractéristiques

Les caractéristiques de la documentation de spécification du système sont les suivantes:

a) les principaux utilisateurs de la documentation de spécification système sont les vérificateurs et les personnes en charge de la production de la conception du système et de la réalisation de l'intégration et de la validation. Il convient que la documentation soit claire, concise, complète, cohérente et exacte, et écrite de façon appropriée pour les lecteurs visés;

b) il convient que la spécification des fonctions d'application soit rédigée en des termes qui facilite la vérification ainsi que sa compréhension par les ingénieurs de fonctionnement et par les opérateurs de la centrale;

c) il convient que la spécification du système soit développée avec des méthodes, outils et directives d'ingénierie système documentés. Il convient que ces méthodes, outils et directives minimisent « l'écart » existant avec les méthodes, outils et directives utilisés pour la spécification des exigences du système;

NOTE Les méthodes et outils d'ingénierie logicielle peuvent améliorer la qualité de la spécification de la conception du système final, même comparée à la spécification de la conception d'un système câblé.

d) il convient que la spécification du système soit rédigée et structurée afin de faciliter l'estimation de sa cohérence avec la spécification des exigences du système, et de constituer un outil de référence efficace pour la validation du système, c'est-à-dire qu'il convient qu'elle facilite une identification complète des spécifications (au lieu de les noyer dans des explications et autres informations secondaires).

6.4.3.3 Vérification

a) Il convient que la vérification de la spécification du système par rapport à la spécification des exigences portant sur le système soit effectuée avant l'achèvement de la conception détaillée. Il convient qu'elle permette de mettre en place des mesures correctives avant la réalisation et l'intégration du système.

b) Il convient de mettre en place un système de communication efficace entre l'équipe chargée de la spécification du système et les fournisseurs afin de permettre de vérifier l'aptitude à l'emploi des équipements choisis.

c) La vérification doit expliciter la cohérence et enregistrer toute non-conformité de la spécification du système relativement à la spécification des exigences du système.

d) La traduction de la spécification des exigences des fonctions d'application dans la spécification du logiciel d'application doit être vérifiée pour quelle soit correcte.

e) Pour les systèmes de classe 1 et 2, toute non-conformité doit être corrigée ou justifiée par rapport à la sûreté, en tenant compte d'éventuelles mesures de compensation.

f) Pour les systèmes de classe 1 et 2, les caractéristiques qui augmentent la complexité du système et qui ne découlent pas de la spécification des exigences portant sur le système doivent être identifiées et justifiées par rapport à la sûreté.

NOTE La présence de caractéristiques non exigées par la spécification des exigences système peut accroître considérablement la complexité du système, ce qui pourrait potentiellement diminuer la confiance en son bon fonctionnement.

6.4.4 Documentation de la conception détaillée et de la réalisation du système

6.4.4.1 Généralités

La conception détaillée peut être effectuée en un certain nombre d'itérations. Les exigences du présent paragraphe traitent de la documentation finale du système, qui est disponible lorsque la conception détaillée, la réalisation, l'intégration et la validation du système sont achevées et que celui-ci est prêt à être livré et installé sur le site.

La documentation de conception détaillée du système peut généralement être répartie en quatre groupes de documents. A savoir:

- les documents relatifs à la conception du système;
- les analyses exigées (voir 6.2.4.2);
- les documents relatifs à la conception du logiciel d'application;
- les documents relatifs à la conception du logiciel système et des composants matériel du système.

NOTE 1 Si le système est réalisé avec des équipements préexistants, les documents relatifs à la conception du logiciel système et du matériel du système font partie de la documentation des équipements préexistants.

Seuls les deux premiers groupes sont traités ici, dans la mesure où la conception du logiciel et du matériel sort du cadre de la présente norme (voir 6.2.4).

NOTE 2 Pour les systèmes de classe 1 et de classe 2 ou 3, les exigences relatives à la documentation du logiciel figurent respectivement dans la CEI 60880 et dans la CEI 62138, et les exigences relatives à la documentation du matériel dans la CEI 60987.

6.4.4.2 Contenu

a) Les documents relatifs à la conception du système doivent être complets et non ambiguës et doivent apporter toutes les informations nécessaires aux activités aval du cycle de vie de sûreté du système, y compris, pour ce qui concerne l'intégration, la validation, l'installation, l'exploitation et la maintenance.

b) Les documents relatifs à la conception du système complètent les documents relatifs à la spécification et doivent fournir une description détaillée de la structure interne et du comportement interne du système. Le niveau de détail de cette description peut être adapté suivant la classe de sûreté du système.

c) Les documents relatifs à la conception du système doivent contenir la description de l'installation des équipements dans la centrale et les dispositions relatives aux essais du système.

d) Les documents relatifs à la conception du système doivent contenir la description des fonctionnalités et des performances qui ont été validées pour le système, en particulier le temps de réponse attendu dans les différentes conditions d'exploitation de la centrale, les valeurs de sûreté nominales des points de consigne et des algorithmes de contrôle, et les valeurs des marges de sûreté.

6.4.4.3 Caractéristiques

Les caractéristiques de la documentation de conception du système sont les suivantes:

a) Les principaux destinataires de la documentation de conception système sont les auteurs et les auditeurs des plans d'intégration, de qualification, d'installation, d'exploitation et de maintenance du système, le personnel de maintenance, les auteurs et vérificateurs des modifications. Il convient que la documentation soit écrite de façon appropriée pour les lecteurs visés;

b) La documentation de conception détaillée doit être conservée pendant le développement du système afin d'assurer que la version finale des documents est conforme à exécution.

6.4.4.4 Vérification

a) Il convient que la vérification de la conception détaillée du système et de sa documentation soit réalisée avant la réalisation de nouveaux matériels et logiciels; il convient qu'un délai suffisant soit accordé pour permettre, le cas échéant, la mise en œuvre de mesures correctives suite à la vérification.

b) Il convient que le caractère réaliste des exigences de la fiabilité portant sur les fonctions d'application du système (voir 6.2.4.2.1) soient vérifié très tôt durant la phase de conception détaillée.

NOTE L'analyse de fiabilité du système peut nécessiter la modification de la conception détaillée, de l'architecture du système, par exemple le degré de redondance voire même le choix des solutions de l'architecture globale de l'I&C.

c) Les possibilités de perturbation des fonctions d'application par les fonctions de service du système doivent être rigoureusement analysées à l'aide de moyens adaptés suivant l'importance pour la sûreté des fonctions d'application.

d) Les hypothèses faites lors de la vérification de la conception détaillée doivent être explicitées et documentées.

6.4.5 Documentation de l'intégration du système

6.4.5.1 Contenu

La documentation d'intégration du système doit contenir le plan d'intégration, les rapports d'essais d'intégration et toutes les informations nécessaires à la phase suivant la validation.

6.4.5.2 Caractéristiques

Les rapports d'essais d'intégration doivent contenir les informations suivantes:

- les versions des modules matériels et logiciels, de la spécification des essais utilisée, des outils et équipements utilisés, et toute valeur d'étalonnage, d'initialisation pertinente, toute simulation d'équipement ou d'interface utilisée;
- les résultats de chaque essai et la liste des écarts observés entre résultats attendus et ceux obtenus; pour chaque écart, le rapport de l'analyse faite et des décisions prises quant à la poursuite de l'essai ou la mise en œuvre d'une modification;
- la résolution de tous les défauts ayant fait l'objet d'un compte rendu et les résultats des évaluations qui ont suivi doivent être documentés de façon suffisamment détaillée et de façon qu'une personne non directement impliquée dans le plan de vérification et de développement du système puisse auditer.

6.4.5.3 Vérification

a) Il convient que la vérification des rapports d'intégration du système relativement au plan d'intégration du système soit réalisée avant de débuter l'activité de validation.

b) Pour les systèmes de classe 1 et de classe 2, la traçabilité entre la documentation de conception et les essais et analyses de l'intégration des composants correspondants doit être réalisée, de manière à permettre l'évaluation des essais et analyses relativement à

leur taux de couverture. La granularité de la traçabilité pour les systèmes de classe 2 peut être moins fine que celle exigée pour ceux de classe 1.

c) Pour les systèmes de classe 3, il convient que la traçabilité entre la documentation de conception et les essais et analyses de l'intégration des composants correspondants soit réalisée, de manière à permettre l'évaluation des essais et analyses relativement à leur taux de couverture.

6.4.6 Documentation de la validation du système

6.4.6.1 Contenu

La documentation de validation du système doit contenir le plan de validation, les rapports d'essais de validation et toutes les informations nécessaires à la qualification du système.

6.4.6.2 Caractéristiques

a) Le rapport de validation système doit documenter les résultats portant sur les aspects logiciel de la validation du système.

b) Le rapport doit identifier le matériel, le logiciel et les autres données de configuration et de programmation ainsi que la configuration du système utilisée, les équipements utilisés et leur étalonnage ainsi que les modèles de simulation utilisés.

c) Le rapport doit aussi identifier toutes les discordances observées entre les résultats attendus et les résultats réels, et pour chaque discordance, le rapport de l'analyse faite et des décisions prises concernant le fait de continuer l'essai ou de mettre en œuvre une modification.

d) Le rapport doit faire le bilan des résultats de la validation système.

e) Le rapport doit évaluer la conformité du système à toutes ses exigences.

f) Le rapport et les résultats des évaluations qui ont suivi doivent être mémorisés sous une forme et avec un niveau de détail suffisant pour pouvoir être audités par des personnes qui n'ont pas été directement engagées dans la validation.

g) Il convient d'identifier les outils logiciel utilisés dans le processus de validation dans un paragraphe du rapport de validation. Les simulations de la centrale et de ses systèmes utilisés pour la validation doivent être documentées.

6.4.6.3 Vérification

Les résultats des essais et des analyses de validation doivent être documentés et comparés aux exigences figurant dans le plan de validation du système afin de confirmer que la performance fonctionnelle du système est bien conforme à ces exigences.

NOTE La documentation de validation ainsi que la documentation de validation fonctionnelle (voir d) de 6.4.4.2) confirment la conformité du système à la fois à la spécification du système et à la spécification des exigences du système.

6.4.7 Documentation des modifications du système

6.4.7.1 Contenu

a) Demande de modification

Ce document doit indiquer

- la justification de la modification et l'impact (le cas échéant) de celle-ci sur la sûreté de la centrale nucléaire,
- la description fonctionnelle de la modification (avec schémas modifiés légendés, schémas mécaniques, schémas de configuration, etc.) et les moyens proposés pour mettre en œuvre la modification,
- les relations entre la modification et toute autre modification concernant la centrale.

b) Lot de modification

Lorsque la modification de conception est achevée, c'est-à-dire lorsque les composants logiciels, les composants matériels et la documentation sont le reflet exact de la nouvelle conception, il convient de construire un lot de modification permettant l'introduction de la modification dans le système opérationnel. La documentation du lot de modification doit décrire les modules matériels, les modules logiciels et les moyens pour mettre en œuvre la modification, c'est-à-dire les équipements qui devraient être mis hors tension, la procédure qui doit être suivie pour charger le nouveau logiciel, ou bien aussi la référence qui peut être faite à des procédures de modification déjà existantes.

6.4.7.2 Caractéristiques

La demande de modification doit être identifiée de manière unique et doit être évaluée, par le personnel compétent et responsable qui l'approuve ou la rejette. Le résultat de cette évaluation (accord ou refus) doit être enregistré.

6.4.7.3 Vérification

a) Pour les systèmes de classe 1, le caractère exhaustif et la correction technique du lot de modification doivent être examinés par une équipe n'ayant pas été directement impliquée dans la réalisation de la modification mais qui néanmoins soit techniquement compétente pour l'évaluer.

b) Le lot de modification ne doit pas être chargé dans le système avant l'évaluation de la modification.

6.5 Qualification du système

6.5.1 Généralités

Le présent paragraphe établit les exigences relatives à la qualification des systèmes d'I&C classés (voir 6.2.2.7). Ce processus garantit qu'un système d'I&C est en mesure de satisfaire, de façon permanente, les exigences fonctionnelles et de performance imposées par le dimensionnement de conception aux fonctions importantes pour la sûreté, lorsque ce système est soumis aux conditions d'environnement et aux contraintes spécifiées (voir 6.2.2.2 à 6.2.2.6).

NOTE La série CEI 61508 peut être utilisée pour fournir des recommandations supplémentaires pour la qualification et l'évaluation des composants.

6.5.2 Qualification générique et particulière à l'application

Il est pratique de tirer bénéfice de preuves de qualification de composants matériel et logiciel établies hors du cadre de la conception de la centrale ou d'une application particulière (c'est-à-dire la préqualification ou la qualification générique de produits commerciaux ou d'une famille d'équipements), de façon à répartir l'essentiel de l'effort de qualification sur plusieurs projets (voir 6.2.3.2). Une qualification générique peut avoir été réalisée en commun pour plusieurs projets de centrales nucléaires, ou par le vendeur d'une plate-forme d'équipements pour des applications liées à la sûreté. Une préqualification peut aussi avoir été réalisée pour des produits initialement destinés à d'autres domaines que celui de la conception de centrales nucléaires, et pas nécessairement complètement en conformité avec les méthodes et les procédures imposées par le projet.

NOTE 1 La certification des produits commerciaux aux niveaux d'intégrité de sûreté SIL 1, 2 et 3 conformément à la série CEI 61508 par un évaluateur indépendant et accrédité pour la sûreté est un exemple de préqualification des équipements commerciaux. Du fait que la série CEI 61508 est la norme générique correspondant à la CEI 61513, une telle certification est un bon point de départ pour la qualification des produits commerciaux pour des applications spécifiques, et pour démontrer la conformité aux exigences de la CEI 61513 et celles de ses normes filles.

L'utilisation de la préqualification d'un équipement préexistant implique qu'une qualification propre à l'application soit réalisée, de façon ou bien à confirmer la pertinence des preuves de la préqualification par rapport aux exigences du système d'I&C, ou bien à combler les manques identifiés. Cette qualification propre à l'application peut reposer sur différentes activités telles que l'acceptation des résultats de la qualification existante basée sur l'analyse

de la documentation existante, la réalisation d'audits, la réalisation d'essais complémentaires, fonctionnels ou liés à l'environnement ou aux séismes ou l'évaluation de retour d'expérience.

a) Suivant l'étendue de la documentation disponible et les preuves de pré-qualification, un programme de qualification adapté doit être défini et inclut dans le plan de qualification (voir 6.5.3).

b) La qualification propre à l'application doit prendre en compte les propriétés et les caractéristiques qui ne sont pas couvertes par la préqualification.

c) La qualification propre à l'application doit prendre en compte les différences entre la méthodologie et les procédures de préqualification, et celles imposées par la spécification d'exigences système (voir 6.2.2.7)

NOTE 2 Généralement pour la qualification particulière d'une application on considère que

- les preuves amenées pour la préqualification sont acceptables et permettent de satisfaire les exigences portant sur les systèmes d'I&C,
- tout les écarts au niveau preuve sont identifiées et sont à compenser,
- lors du remplacement d'un matériel, toutes différences significatives de conception par rapport au matériel ou au système remplacé sont à examiner et l'absence de conséquences négatives est à confirmer,
- les critères de réception et de performance utilisés pour les essais de préqualification sont acceptables pour l'application considérée.

Le processus de qualification système peut être réalisé par étapes: premièrement en qualifiant individuellement les composants matériel et logiciel du système d'I&C et puis en qualifiant le système d'I&C intégré (par exemple la conception réalisée finale).

d) La qualification du matériel et du système logiciel système d'un système réalisé en configurant les composants d'une famille d'équipements ou en connectant des composants préexistants peut être tirée de la qualification réalisée sur les composants individuels et les configurations de composants interconnectés. Dans ce cas, une analyse doit être réalisée pour démontrer que la qualification couvre la configuration finale du système utilisé sur la centrale, y compris pour ce qui concerne les systèmes de montage, la distribution de charge et de température à l'intérieur des armoires.

e) Sur la base des analyses précédentes, il convient que le plan de qualification identifie les nouvelles caractéristiques de conception du système et détermine si des essais de qualification et des évaluations supplémentaires sont à réaliser.

6.5.3 Plan de qualification

6.5.3.1 Généralités

On doit élaborer un plan de qualification, identifiant tous les aspects à évaluer et à estimer afin de qualifier le système et les fonctions importantes pour la sûreté qu'il met en œuvre, ainsi que pour maintenir cet état de qualifié.

Le plan de qualification couvre les aspects système, matériel et logiciel. Même si les composants matériel ou logiciel qui sont utilisés ont subi une préqualification conforme aux normes de qualification applicables, la documentation de qualification disponible doit être, au minimum, évaluée par rapport aux exigences système de façon à évaluer son acceptabilité par rapport au besoin, de plus les aspects système intégré doivent être évalués (analyse d'adéquation par rapport au besoin).

La Figure 6 fournit une vue d'ensemble des activités.

NOTE La qualification d'un composant préexistant ou d'un produit commercial est toujours rattachée à une version particulière de ce produit. Toutes les modifications de conception correspondent à un changement d'indice de version et la qualification aura besoin d'être ré-évaluée.

6.5.3.2 Qualification fonctionnelle et environnementale

NOTE 1 La qualification fonctionnelle et environnementale est également appelée « qualification du matériel ».

Plusieurs techniques peuvent être utilisées pour la qualification fonctionnelle et environnementale. Généralement, celle ci est réalisée en différentes étapes, tout d'abord au niveau des composants individuels ou des assemblages sous-système, et puis au niveau de l'ensemble du système. La qualification des composants et des assemblages sous-système comprend les essais de type, les essais fonctionnels, les analyses et évaluations de la conception et l'expérience opérationnelle pour des applications similaires. L'essai de type est la méthode privilégiée (voir 4.1 de la CEI 60780:1998).

NOTE 2 Généralement, la qualification fonctionnelle comprend le fonctionnement des équipements intégrés avec le logiciel propriétaire ou le logiciel système en présence d'applications représentatives. De plus, il constitue généralement la dernière étape des essais d'intégration logiciel propriétaire et matériel dans le cycle de développement d'un système programmé.

a) Les systèmes de classe 1 et 2 doivent être qualifiés pour ses conditions environnementales conformément aux exigences de la CEI 60780 et de la CEI 60980. Les conditions environnementales doivent inclure celles prescrites en 6.2.2.6.

b) Les systèmes de classe 3 pour lesquels une qualification environnementale particulière est exigée (par exemple résistance aux séismes, ou fonctionnement dans des conditions environnementales particulières), peuvent être qualifiés suivant des normes industrielles. Les caractéristiques prétendues auxquelles il est fait appel pour satisfaire au fonctionnement en conditions environnementales anormales, à la qualification sismique suivant des normes industrielles ou aux autres performances fonctionnelles prétendues doivent être justifiées par des preuves documentaires. En présence de facteurs de vieillissement significatifs, et si la durée de vie certifiée ne peut pas être démontrée conformément à la définition fournie par la CEI 60780, on doit proposer un programme de qualification progressif et justifié sa conformité par rapport à la CEI 60780.

c) La qualification CEM doit être réalisée conformément aux exigences applicable de la série de normes CEI 61000-4. Les conditions d'ambiance doivent comprendre celles spécifiées en 6.2.2.6.

d) Des séquences d'essais, y compris les critères d'acceptation, doivent être définies pour les essais des composants, ou de configurations de composants, ou du système complet selon les cas, afin de

   - vérifier les caractéristiques fonctionnelles dans les conditions d'ambiance normales et dans toutes les conditions extrêmes d'exploitation spécifiées,
   - vérifier les caractéristiques relatives aux positions de repli et à l'auto-surveillance ainsi que les modes de fonctionnement dégradé,
   - démontrer la résistance aux conditions d'ambiance pertinentes (y compris les conditions sismiques et les conditions d'ambiance électromagnétique).

e) Des analyses doivent être réalisées autant que nécessaires, de façon à justifier les propriétés du système qui ne peuvent pas l'être par un autre moyen. Ceci peut comprendre

   - les analyses de fiabilité fournissant ou justifiant des données de fiabilité,
   - les analyses de modes de défaillance et de leurs effets confirmant les modes de défaillance spécifiés et fournissant des données concernant le taux couverture des fonctions d'auto-surveillance,
   - des analyses des circuits confirmant les fonctionnalités, la précision et les marges spécifiées.

6.5.3.3 Evaluation et estimation des logiciels

NOTE 1 L'évaluation et l'estimation du logiciel sont également appelées « qualification du logiciel ».

L'évaluation et estimation du logiciel prennent en compte la rigueur du processus de développement du logiciel et l'étendue des essais et de la validation effectués sur le système intégré. Pour les logiciels préexistants (LPD), le retour d'expérience opérationnelle peut constituer, sous certaines conditions, un facteur de compensation pour pallier au manque d'information sur le processus de développement.

Les logiciels du système programmé à qualifier incluent:

- le logiciel système, qui peut être un logiciel prédéveloppé non spécifique à la centrale;
- le logiciel d'application, qui est spécifique à la centrale.

a) La qualification doit évaluer et estimer le logiciel système et le logiciel d'application afin de garantir que la qualité des logiciels est appropriée pour atteindre le niveau de fiabilité requis pour les fonctions réalisées par le système.

b) Pour les systèmes de classe 1, les nouveaux logiciels doivent être évalués et estimés conformément aux exigences de la CEI 60880.

c) Il convient que les logiciels des équipements préexistants sélectionnés pour les systèmes de classe 1 aient été élaborés conformément à des directives et normes reconnues et appropriées au niveau de qualité élevé requis pour les fonctions de catégorie A (voir 7.2.2.1 de la CEI 61226 :2009). En particulier, les exigences de la CEI 60880 relatives aux logiciels et outils préexistants, et celles de la CEI 60987 doivent être respectées.

NOTE 2 Le paragraphe 15.3.3 de la CEI 60880:2006 définit des critères d'acceptation et des restrictions quant à l'utilisation d'informations concernant le retour d'expérience en matière de processus de qualification.

d) Il convient que les logiciels des équipements préexistants sélectionnés pour les systèmes de classe 2 aient été développés conformément à des directives et normes reconnues. Dans le cas contraire, les logiciels peuvent être qualifiés conformément aux critères fournis par la CEI 62138, prenant en compte un historique documenté de leurs utilisations passées faisant état de leur fonctionnement satisfaisant dans des applications similaires.

e) Les critères à utiliser pour l'évaluation, l'estimation et l'acceptation du logiciel des systèmes de classe 3 sont fournis par la CEI 62138.

6.5.4 Qualification supplémentaire pour les systèmes interconnectés

a) Un plan doit être établi pour les essais supplémentaires qui peuvent être exigés pour les systèmes d'I&C interconnectés, afin de compléter leur qualification individuelle, par exemple des essais d'interférence électromagnétique des interfaces pour une implantation et une mise à la terre spécifiques, ou des essais de robustesse du système en cas disfonctionnement ou de surcharge réseau.

b) La faisabilité et la cohérence des essais supplémentaires doivent être vérifiées dans le cadre de la vérification de la conception de l'architecture d'I&C.

6.5.5 Maintien de la qualification

a) Un plan complémentaire doit être établi pour maintenir la qualification pendant le fonctionnement et la maintenance du système, lorsque certaines pièces sont remplacées par des pièces qui ne sont pas identiques et en cas de modifications fonctionnelles.

b) Le plan complémentaire doit permettre l'identification des modules qui réalisent des fonctions de catégorie A ou B, afin d'assurer la cohérence avec les versions validées.

NOTE Ce plan complémentaire peut être traité dans un paragraphe particulier du plan de qualification (voir 6.5.2) couvrant les modifications, ou dans un document particulier séparé. Il convient que ce plan complémentaire soit établi suffisamment tôt. Il convient aussi que les recommandations portant sur la qualification des modifications soient déjà établies lors du processus de conception initiale et soient encore disponibles au plus tard de la mise en service.

6.5.6 Documentation

a) Il convient que les informations qui seront communiquées à l'autorité délivrant les licences figurent dans une liste.

NOTE Généralement, les rapports de qualification du système d'I&C pour les systèmes de classe 1 ou 2 et pour les systèmes de classe 3 choisis (par exemple ceux associés aux salles de commande principale ou auxiliaire) seront soumis aux autorités réglementaires dans le cadre du processus d'autorisation.

b) Il convient que la liste fasse la distinction entre les informations nécessaires avant l'installation d'un système et les informations que doit fournir le candidat à la licence parallèlement à l'installation et à la mise en service, par exemple les rapports d'essais. Parmi les types d'informations pouvant être demandés, figurent notamment

- les descriptions (représentations détaillées des faits),

- les explications (représentations des faits et raisonnements),
- les démonstrations,
- les justifications,
- les preuves (déclarations vérifiables prouvant les assertions).

c) La documentation peut être regroupée en fonction de l'utilisation pour laquelle elle est nécessaire, mais dans son contenu doivent figurer

- le rapport d'analyse préliminaire de sûreté et les documents récapitulatifs, afin d'évaluer la conception préliminaire du système d'I&C,
- des descriptions détaillées partielles ou de l'ensemble du système, afin de permettre une vérification et une validation indépendantes. Cette documentation peut contenir des informations détaillées sur les essais de type des composants,
- des explications détaillées ou des bilans, des démonstrations ou des preuves, nécessaires pour justifier les décisions relatives à la conception et pour simplifier le processus de vérification et de validation indépendantes,
- des informations concernant l'installation, l'intégration, la mise en service et les essais de réception réalisés en usine et sur site, afin de vérifier les étapes du cycle de vie de sûreté qui se situent entre les phases de conception et d'exploitation,
- la documentation relative aux informations nécessaires à l'exploitation du système, afin de vérifier les procédures de maintien à long terme de la qualité du système d'I&C.

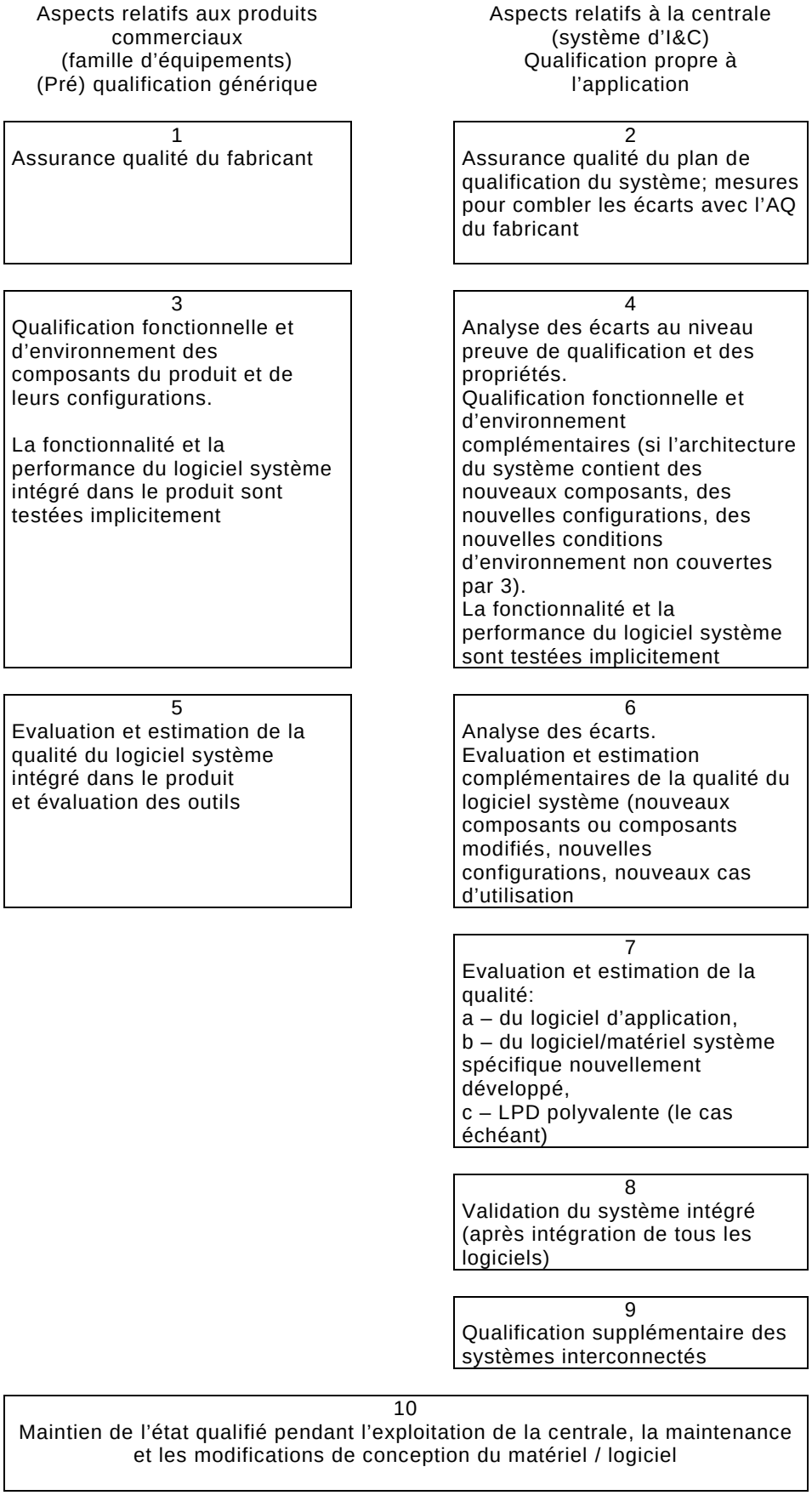


Figure 6 – Aspects produit et propre à l'application de la centrale devant être traités par le plan de qualification du système

7 Intégration et mise en service d'ensemble

7.1 Généralités

L'objectif de cette phase est d'intégrer sur site les systèmes d'I&C et d'assurer que toutes les fonctions d'I&C importantes pour la sûreté s'exécutent comme prévu pendant les essais de mise en service de la centrale. Le plan de mise en service des systèmes d'I&C est inclus dans le programme de mise en service des systèmes de la centrale (voir 4.4 de l'AIEA 75-INSAG-3:1999).

7.2 Exigences relatives aux objectifs à atteindre

a) Les activités doivent être menées d'une manière systématique, selon une stratégie établie conformément aux plans d'installation des systèmes, aux plans d'intégration et de mise en service globaux et aux plans de sécurité définis en 5.5 et 6.3.

b) Il convient que l'activité d'intégration globale soit effectuée avec tous les systèmes d'I&C concernés installés et contrôlés individuellement (voir 6.2.7).

c) Les logiciels et les bases de données paramétrables doivent être chargées et les valeurs enregistrées doivent être justifiées et testées.

d) Le matériel et le logiciel des systèmes programmés doivent être soumis à la gestion de configuration.

e) La vérification et la validation de toutes les fonctions importantes pour la sûreté doivent être terminées avant que celles-ci soit mises en service sur la centrale.

7.3 Documentation produite

a) La documentation de l'intégration des systèmes d'I&C contenant les enregistrements de l'évolution chronologique des activités de vérification et de validation sur site doit être disponible avant l'étape d'exploitation.

b) Le rapport de mise en service globale doit confirmer que les systèmes d'I&C satisfont à toutes les attentes relatives à leur utilisation, et que les fonctions importantes pour la sûreté satisfont aux spécifications d'exigences d'ensemble (voir 5.3).

c) Les différences par rapport aux objectifs initiaux de conception sont évaluées, corrigées ou signalées à l'organisation en charge de l'exploitation, afin que tout effet sur le fonctionnement de la centrale puisse être pris en compte.

NOTE Les exigences exactes relatives à la documentation dépendront de l'organisation spécifique en charge de l'exploitation.

8 Exploitation et maintenance d'ensemble

8.1 Généralités

L'exploitation des systèmes d'I&C peut débuter dès que l'évaluation des rapports de mise en service indique que l'étape a été franchie avec succès. L'exploitation peut continuer si les enregistrements relatifs à l'exploitation n'exigent ni réparation ni modification. L'exploitation peut reprendre après une réparation ou une modification réussie et après l'évaluation des rapports correspondants.

Il convient que les conditions à respecter avant d'entrer dans la phase d'exploitation soient fixées au préalable avant la cession de la centrale par l'organisation en charge de la mise en service à celle en charge de l'exploitation. Les exigences suivantes sont indépendantes de cet accord de cession:

- il convient que les systèmes aient été soumis à suffisamment d'essais pour confirmer que la fonctionnalité spécifiée a bien été obtenue. Si les essais ont identifié des défauts, ceux-ci doivent être documentés et, si possible, corrigés avant la mise à disposition;
- un manuel de l'utilisateur adéquat et les plans de maintenance doivent être disponibles.

8.2 Exigences relatives aux objectifs à atteindre

Les systèmes d'I&C sont exploités et entretenus afin que les exigences relatives aux fonctions d'I&C importantes pour la sûreté soient toujours satisfaites.

a) Les plans d'exploitation, de maintenance et de sécurité définis en 5.5 et 6.3 doivent être mis en œuvre.

b) Les procédures que doivent suivre les opérateurs de la centrale ou les équipes de maintenance dans les conditions d'exploitation normales et accidentelles, doivent être disponibles dans la salle de commande ou à proximité. Leur présentation et leur contenu doivent être en accord avec la réglementation internationale ou nationale.

c) Les procédures de maintenance, d'essais et de modifications des matériels et des logiciels doivent être mises en œuvre conformément à la CEI 62138, CEI 60880 et à la CEI 60987.

8.3 Documentation produite

La documentation chronologique d'exploitation, de réparation et de maintenance doit être tenue à jour. Il convient que les enregistrements d'exploitation fassent l'objet de revue régulière pour détecter les tendances négatives d'évolution des performances, et il convient que toutes tendances d'évolution indiquant une dégradation inacceptable du matériel d'I&C fassent l'objet d'actions correctives appropriées.

NOTE Les exigences exactes relatives à la documentation dépendront de l'organisation spécifique en charge de l'exploitation.

Annexe A
(informative)

Questions de sûreté fondamentales dans les centrales nucléaires

A.1 Généralités

La présente annexe identifie les principaux concepts de sûreté qui sont pris en compte dans la présente norme pour la conception de l'I&C dans les centrales nucléaires. Cette annexe fournit la vue d'ensemble du contenu des documents AIEA mais n'a pas pour objectif d'en élever le niveau d'exigences.

A.2 Objectifs de sûreté de la centrale

Toute activité industrielle présentant des risques pour le personnel, le public et l'environnement nécessite que l'exploitant prenne toutes les mesures réalisables afin de minimiser ces risques. Un des risques liés à l'énergie nucléaire est le risque potentiel associé aux rayonnements ionisants (voir l'Article 2 de l'AIEA NS-R-1:2000).

L'objectif général de la sûreté nucléaire est de protéger les personnes, la société et l'environnement en établissant et maintenant une défense efficace contre le risque radiologique lié aux centrales nucléaires.

L'objectif technique de sûreté pour les centrales nucléaires existantes est d'atteindre d'une « probabilité cible » de survenance d'un endommagement grave du cœur inférieure à 10^{-4} événements par année d'exploitation de la centrale. La mise en œuvre des principes de sûreté pour les futures centrales devrait permettre l'atteinte d'un meilleur objectif, à savoir moins de 10^{-5} événements par année d'exploitation de la centrale. Des mesures de gestion et d'atténuation des accidents graves devraient réduire, par un facteur au minimum de 10, la probabilité de survenance d'un important dégagement radiologique hors du site nécessitant une réponse extérieure au site (voir le 2.3 de l'AIEA 75-INSAG-3:1999).

A.3 Analyse de sûreté de la centrale

A.3.1 Généralités

Une analyse de sûreté de la centrale nucléaire est réalisée afin d'établir et de confirmer la conception préliminaire des éléments importants pour la sûreté et d'assurer que la conception de la centrale est en mesure de respecter les limites et les niveaux de référence des doses et dégagements radiologiques fixés par les autorités règlementaires pour chaque condition d'exploitation de la centrale (voir l'Article 5 du document de l'AIEA NS-R-1:2000).

L'analyse de sûreté pourrait inclure:

- la démonstration que les limites et conditions d'exploitation sont respectées lors de l'exploitation normale de la centrale;
- la caractérisation des EIP pertinents pour la conception de la centrale et son implantation;
- l'analyse et l'évaluation des séquences d'événements qui résultent des EIP;
- la comparaison des résultats de l'analyse avec les critères d'acceptation radiologique et les limites de conception;
- l'établissement et la confirmation de la conception préliminaire;

- une démonstration que la gestion des incidents de fonctionnement prévus et des situations accidentelles est possible par une réponse automatique des systèmes de sûreté combinée avec les mesures prévues prises par l'opérateur.

Ce processus d'analyse de sûreté de la centrale nucléaire est réalisé de manière itérative du début de la conception de la centrale jusqu'à l'évaluation finale de la sûreté de la centrale, et il prend en compte tous les aspects relatifs à la configuration de la centrale qui peuvent avoir une influence sur la sûreté. L'analyse de sûreté de la centrale considère le risque d'erreurs humaines au cours de l'exploitation et au cours de situations accidentelles.

L'objectif de l'analyse est de démontrer que les mesures devant être mises en œuvre par les systèmes automatiques et les opérateurs permettront de maintenir les doses de rayonnement reçues par le personnel du site et le public à un niveau inférieur aux limites prévues pour l'exploitation normale de la centrale, les incidents de fonctionnement prévus et les situations accidentelles.

A.3.2 Analyse des séquences d'événements

L'objectif de l'analyse d'une séquence d'événements est l'identification systématique et détaillée de toutes les conséquences possibles d'un EIP sur la centrale, y compris de celles survenant au niveau des systèmes auxiliaires et support et celles faisant suite à une éventuelle erreur de l'opérateur. Les résultats de cette analyse peuvent ensuite être utilisés pour déterminer si les exigences de sûreté établies dans le Code de conception de l'AIEA ont été satisfaites (voir les annexes de l'AIEA NS-R-1:2000).

L'analyse (qualitative) d'un arbre d'événements et l'analyse (quantitative) de l'arbre de défaillances sont des outils analytiques utiles pour identifier les états possibles de la centrale après la survenance d'un EIP.

Il convient de noter qu'il n'est ni possible ni nécessaire d'inclure, dans l'analyse de sûreté, toutes les séquences d'événements pouvant se produire. Cependant, l'analyse de sûreté doit identifier et évaluer de manière détaillée les EIP et les séquences d'événements qui conduisent à des cas enveloppe de sûreté. Le retour d'expérience de centrales existantes doit être utilisé pour guider le choix de ces séquences d'événements.

Même avec la limitation admise aux cas enveloppe décrits ci-dessus, l'application rigoureuse de la méthode par arbre d'événements conduira, dans beaucoup de cas pratiques, à l'identification de plus de configurations de la centrale pour chaque EIP qu'il n'est raisonnablement possible d'analyser en détail. Ainsi, il est en général admissible de restreindre l'analyse détaillée à un certain nombre de séquences d'événements représentatives.

A.3.3 Estimation de la conception: méthodes déterministes et probabilistes

Des méthodes ont été élaborées afin d'évaluer l'atteinte des objectifs de sûreté (voir l'AIEA 75-INSAG-3).

Dans l'approche déterministe, des événements de dimensionnement sont choisis pour limiter la gamme d'événements initiateurs possibles, pouvant amener à une mise en cause de la sûreté de la centrale.

L'analyse probabiliste est utilisée pour évaluer la probabilité d'apparition d'une séquence particulière et ses conséquences. Cette évaluation peut prendre en compte les effets des mesures d'atténuation internes et externes à la centrale.

Comparaison des méthodes déterministe et probabiliste: le manque de données suffisantes sur le comportement des composants ou des systèmes et l'impossibilité de spécifier un mode approprié peuvent empêcher une approche probabiliste quantitative rigoureuse. Cependant, une approche probabiliste partielle peut souvent être complétée par un jugement technique

qualitatif. D'autre part, une approche déterministe requiert un jugement d'ingénieur qui contient implicitement des considérations probabilistes qualitatives.

Au final, la pratique actuelle consiste à utiliser l'approche déterministe pour concevoir les systèmes et l'approche probabiliste pour optimiser des parties appropriées de la conception et pour évaluer la sûreté globale.

A.4 Défense en profondeur

Le concept de défense en profondeur contribue de façon importante contribution à la notion de sûreté. Il convient que ce concept soit appliqué à toutes les activités de sûreté, qu'elles concernent l'organisation, le comportement ou la conception, afin d'assurer que qu'il y a recouvrement au niveau des mesures de sûreté et qu'en cas de défaillance, celle-ci est compensée ou corrigée (voir l'AIEA N-S-R-1, l'AIEA 75-INSAG-3, l'AIEA INSAG-10 et l'AIEA NS-G-1.3).

Une première application du concept de défense en profondeur au processus de conception consiste à prévoir des ensembles indépendants et complémentaires de dispositifs et de procédures afin d'empêcher les accidents ou d'assurer une protection appropriée en cas de défaillance de la prévention.

Exemples de niveaux multiples de protection:

- mise à disposition de différents moyens pour assurer chacune des fonctions de sûreté de base, c'est-à-dire le contrôle de la réactivité, l'évacuation de la chaleur et le confinement de la radioactivité;
- utilisation de dispositifs de protection fiables en complément des moyens de sûreté principaux;
- amélioration de la commande de la centrale par des actions automatiques et manuelles;
- mise à disposition de composants et de procédures permettant d'atténuer les conséquences des accidents.

En règle générale, les lignes de défense doivent être disponibles à tout moment pour les divers modes d'exploitation.

- L'objectif de la première ligne de défense est de maintenir une exploitation normale. Ceci exige que la centrale soit conçue, construite et exploitée en accord avec des niveaux de qualité et des pratiques technologiques appropriées.
- L'objectif de la deuxième ligne de défense est de détecter et prendre en compte tout écart par rapport aux conditions normales d'exploitation afin d'empêcher les incidents de fonctionnement prévus de se transformer en situations accidentelles.
- Pour la troisième ligne de défense, il est supposé, bien que ce soit très improbable, que l'intensification de certains incidents de fonctionnement prévus ne peut être arrêtée par une ligne de défense précédente. Des dispositifs et procédures supplémentaires sont alors prévus pour contrôler les conséquences des situations accidentelles qui en résultent. Un autre objectif essentiel de cette ligne de défense est de parvenir à une situation stable et acceptable suite à un accident.
- Au-delà de la troisième ligne de défense il existe d'autres contributions à la protection du public assurées par des fonctionnalités complémentaires de la centrale (non importantes pour la sûreté), ainsi que des plans de préparation d'urgence, qui sont largement indépendants de la conception des réacteurs.

Une seconde application du concept de défense en profondeur consiste à construire et exploiter la centrale de manière à ce que les matières radioactives soient confinées au sein d'une succession de barrières physiques. Ces barrières sont essentiellement passives et incluent généralement le combustible lui-même, la gaine du combustible, l'enveloppe du

circuit de refroidissement primaire et l'enceinte de confinement. La conception doit garantir l'efficacité appropriée et la protection de chacune de ces barrières.

Une application complémentaire du concept de défense en profondeur est la mise en œuvre de systèmes de secours simple ou multiple des systèmes d'I&C. Afin de minimiser l'ampleur d'une perturbation et d'assurer la défense en profondeur, il est possible d'utiliser plusieurs systèmes agissant progressivement au fur et à mesure que la variable contrôlée s'écarte de la valeur souhaitée. En premier lieu, des systèmes de contrôle non classés prennent des mesures. Ensuite, un ou plusieurs systèmes de contrôle supplémentaires peuvent agir, avant le déclenchement du système de protection, si l'événement entraine l'évolution d'une perturbation opérationnelle mineure vers un transitoire mineur puis vers un transitoire important. L'objectif de chaque étape est de stopper l'événement et de faire revenir le système à une exploitation normale pour les événements mineurs et de l'arrêter d'une manière sûre si les événements s'aggravent.

Annexe B
(informative)

Catégorisation des fonctions et classement des systèmes

B.1 Contexte associé au schéma de catégorisation et de classement

L'AIEA NS-R-1 établit une liste de fonctions de sûreté, permettant à la conception de la centrale de satisfaire aux exigences de sûreté, commençant par les moyens à mettre en œuvre pour l'arrêt sûr du réacteur jusqu'à l'évacuation de chaleur résiduelle du cœur et la réduction du potentiel de dégagement de matières radioactives. Il développe l'idée de classement des composants hydrauliques nécessaires à la réalisation des fonctions selon leur importance pour la sûreté. Il introduit une méthodologie de classement des fonctions de sûreté et d'affectation des exigences de conception, basée sur les conséquences d'une défaillance de la fonction de sûreté, sur la probabilité selon laquelle la fonction pourrait être requise et sur la probabilité selon laquelle la fonction ne serait pas réalisée alors qu'elle est requise.

L'AIEA NS-G-1.3 élargit l'idée de classement aux systèmes d'instrumentation et de contrôle commande. Ce document répartit les systèmes d'I&C en « systèmes importants pour la sûreté » et en « systèmes non importants pour la sûreté ». Il subdivise ensuite les systèmes importants pour la sûreté en « systèmes de sûreté » et en « systèmes liés à la sûreté »et il fournit respectivement des exigences de conception.

La CEI 61226 classifie les fonctions importantes pour la sûreté en trois catégories: A, B et C. Elle fournit les critères d'affectation des fonctions d'I&C à ces catégories et les exigences de conception relatives aux systèmes et équipements associés.

Le nombre de classes définies par l'AIEA est différent du nombre de la CEI 61226 (systèmes de sûreté et liés à la sûreté d'une part, catégories A, B et C d'autre part). De plus, l'AIEA et la CEI n'utilisent pas les mêmes définitions et ni les mêmes concepts (classement des systèmes pour l'AIEA et catégorisation des fonctions/classement des systèmes pour la CEI), ce qui peut causer des interprétations différentes.

La présente norme est conforme à la CEI 61226 pour ce qui concerne la subdivision en trois classes, cette répartition s'adapte bien aux différents niveaux d'assurance que l'on souhaite obtenir en terme de performance et qui sont réalisables en terme de fiabilité lorsqu'on utilise les techniques et produits d'I&C actuels (par exemple équipement développé selon une norme nucléaire, ou équipement préexistant sélectionné puis qualifié ou encore équipement préexistant sélectionné). Cependant, afin d'éviter les ambigüités les fonctions et les systèmes suivent des plans de catégorisation/classement différents.

Les hypothèses de base concernant la catégorisation et le classement de la présente norme sont développées ci-après.

B.2 Base de l'adoption des principes pour la catégorisation et le classement dans cette norme

B.2.1 Généralités

Les fonctions, systèmes et équipements de la centrale nucléaire peuvent être considérés de deux points de vue (Figure B.1):

- Approche fonctionnelle

Cette approche ne considère que les fonctions à effectuer. Bien qu'il soit reconnu que les capteurs, unités de traitement, interfaces, etc. sont nécessaires à la réalisation d'une fonction, l'approche fonctionnelle ne considère pas que ces éléments puissent faire partie d'ensembles plus larges qui réalisent aussi d'autres fonctions, voir « Approche système ». Les moyens nécessaires à la réalisation d'une fonction sont appelés systèmes et équipements associés à la fonction.

- Approche système

Cette approche considère les systèmes comme un ensemble organisé d'équipements réalisant de nombreuses fonctions et sous-fonctions; par exemple, le système de protection, le système d'automatisation et de contrôle, le système d'IHM. Les fonctions réalisées au sein d'un système peuvent être de différentes catégories.

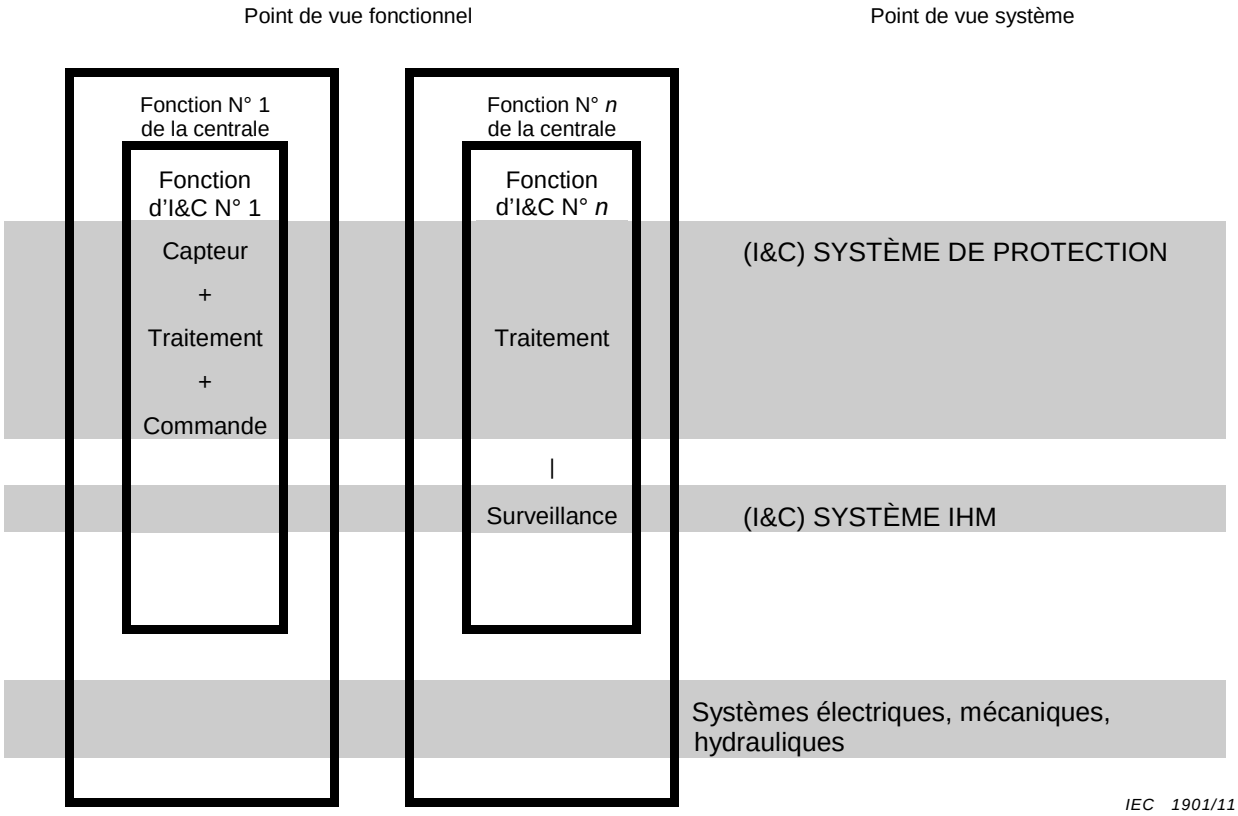


Figure B.1 – Relations entre les fonctions d'I&C et les systèmes d'I&C

B.2.2 Conception du procédé de la centrale

Les ingénieurs de fonctionnement analysent la centrale et les systèmes associés d'un point de vue fonctionnel. Ils définissent les EIP spécifiques à la centrale et au réacteur et les fonctions importantes pour la sûreté nécessaires pour gérer ces EIP et pour empêcher ceux-ci de conduire à des situations accidentelles. Certaines fonctions (ou sous-fonctions) indépendantes peuvent être nécessaires pour chaque EIP, conformément au principe de défense en profondeur: les fonctions (ou sous-fonctions) sont affectées aux catégories A, B ou C, selon qu'elles jouent un rôle essentiel, complémentaire ou auxiliaire pour la sûreté de la centrale.

Les méthodes de catégorisation proviennent généralement de considérations déterministes, probabilistes et de considération portant sur la réduction des risques. Elles prennent en compte différents paramètres, tels que la probabilité d'apparition d'un EIP et son niveau de gravité en cas de défaillance du système d'I&C approprié, la durée pendant laquelle la fonction est requise une fois qu'elle est activée, la fiabilité des fonctions de secours et l'assurance de résoudre une défaillance qui affecterait le système d'I&C.

La catégorisation peut affecter les fonctions d'I&C d'un groupe de sûreté à différentes catégories, par exemple la fonction de mise à l'arrêt sûr du réacteur diversifiée peut être uniquement sollicitée dans les conditions improbables d'un transitoire de fonctionnement prévu combiné avec la défaillance de la fonction de protection primaire. Dans ce cas, au lieu d'être une fonction d'I&C de catégorie A (réalisée dans un système de classe 1), elle peut être simplement de catégorie B ou C.

Les catégories indiquent le niveau des exigences de conception ainsi que classe minimale des systèmes et équipements associés requis pour la réalisation de la fonction.

B.2.3 Conception de l'I&C de la centrale

Les ingénieurs en I&C analysent les fonctions d'I&C et les systèmes et équipements associés avec une approche système. Ils ont pour mission de concevoir des systèmes d'I&C réalisant les fonctions d'I&C avec les niveaux de qualité et d'indépendance requis par les ingénieurs de fonctionnement. Les systèmes sont affectés à des classes selon le niveau de qualité souhaité.

Dans le cas des systèmes programmés, le classement et l'affectation des fonctions aux systèmes se font différemment que pour les systèmes câblés pour les raisons suivantes:

- dans les systèmes électroniques câblés, les fonctions sont généralement réalisées par des chaînes de composants ou de relais séparés, alors que les systèmes programmés permettent l'exécution d'un certain nombre de fonctions par les mêmes composants matériels;
- les systèmes programmés incluent un certain nombre de fonctions auxiliaires, par exemple fonctions d'auto-supervision, fonctions de diagnostique, qui ne correspondent pas à des catégories définies. Ces fonctions peuvent nécessiter un niveau de qualification inférieur mais requièrent l'isolement fonctionnel;
- le choix de l'architecture du système peut être restreint afin de limiter la complexité et de faciliter la réalisation des fonctions de catégories de sûreté élevées;
- le concepteur peut inclure des exigences portant sur l'architecture des systèmes, par exemple la séparation fonctionnelle, le comportement interne, la complexité, des mesures de défense contre les DCC, qui ne sont pas associées aux fonctions mais qui sont liées aux systèmes d'I&C et aux propriétés de la famille d'équipements utilisée pour la réalisation et la qualification de ces systèmes.

Ceci est à l'origine de la nécessité ressentie d'établir une méthode de classement des systèmes d'I&C qui dépende de la fonction réalisée de catégorie la plus élevée.

B.3 Catégorisation des fonctions d'I&C importantes pour la sûreté

Dans la présente norme, il est supposé que la base de conception de sûreté de la centrale, établie par les ingénieurs de fonctionnement, définit la catégorisation des fonctions d'I&C en 3 catégories, A, B et C. Les exigences relatives à la catégorisation identifient par importance de sûreté le niveau de qualité des éléments intervenant dans la réalisation des fonctions.

La catégorisation des fonctions d'I&C est effectuée jusqu'au niveau sous-fonctions (voir Note). De ce fait, les ingénieurs d'I&C ne devraient pas être obligés de procéder à des analyses supplémentaires pour achever la catégorisation.

NOTE Une même fonction importante pour la sûreté peut être réalisée en utilisant un certain nombre de sous-fonctions ou par une fonction unique incluant toutes les sous-fonctions. Ceci peut créer des ambiguïtés lors de la définition des exigences relatives à la catégorisation, dans la mesure où les sous-fonctions peuvent avoir des importances différentes pour la sûreté et où, en conséquence, se voir attribuer des catégories différentes.

En complément des exigences relatives à la catégorisation, la base de conception de sûreté de la centrale définit des exigences en matière d'indépendance et de diversité des fonctions, pour assurer la défense en profondeur. L'indépendance est requise entre les fonctions

intervenant dans des lignes de défense différentes au sein d'un même groupe de sûreté, et entre une fonction de protection et une fonction de réduction du risque.

Les exigences relatives à l'indépendance et à la diversité constituent des informations d'entrée pour le processus d'affectation des fonctions d'I&C aux systèmes d'I&C. Les fonctions peuvent être réparties dans différents systèmes d'I&C, à condition qu'ils aient un classement de sûreté approprié (voir l'Article B.2).

B.4 Classement des systèmes d'I&C

Les systèmes d'I&C, constituant l'architecture globale de l'I&C, regroupent en général un certain nombre de fonctions ou sous-fonctions d'I&C réalisant des tâches similaires pour la centrale. Les systèmes peuvent normalement être caractérisés par la fonctionnalité qu'ils assurent. Le nombre de systèmes d'I&C et leurs fonctionnalités sont spécifiques à la centrale. Des exemples types de systèmes d'I&C importants pour la sûreté sont indiqués ci-après.

a) Systèmes d'automatisation et de contrôle-commande de la centrale

   Ces systèmes commandent les paramètres ou équipements de la centrale permettant de

   - maintenir les variables du processus dans les limites choisies lors de l'analyse de sûreté de la centrale,
   - garantir un fonctionnement sûr des systèmes et équipements de la centrale importants pour la sûreté,
   - minimiser la gravité et le taux de perturbations plausibles,
   - minimiser la fréquence d'apparition d'événements sollicitant le système de protection. Ceci peut être réalisé par des systèmes de contrôle commande de qualité élevée, diversifiés et redondants ou des actions multiple situées à plusieurs niveaux. Par exemple une combinaison d'actions de commande automatiques et d'actions de commande manuelles si le temps pour réagir est suffisant, ou plusieurs combinaisons de ce type.

   Les systèmes d'automatisation et de contrôle commande peuvent avoir un impact direct sur la sûreté car leur performance, leur fiabilité et les conséquences induites en cas de défaillance font partie de la conception préliminaire du système de protection. Les systèmes d'automatisation et de contrôle commande peuvent aussi constituer les moyens principaux de réalisation de fonctions importantes pour la sûreté, par exemple lorsqu'un délai important est disponible pour la mise en œuvre d'actions correctives.

   Des fonctionnalités typiques de ces systèmes sont: la commande en boucle ouverte, la commande en boucle fermée et l'exécution de commandes manuelles.

b) Systèmes d'IHM

   Ces systèmes informent l'opérateur de la centrale ainsi que d'autres personnels de l'état de la centrale et de celui de ses systèmes importants pour la sûreté. Ils sont aussi utilisés pour aider l'opérateur à la prise de décision et permettre la mise en œuvre d'actions de commande manuelles afin de préserver la sûreté de la centrale.

   Les fonctionnalités typiques de ces systèmes consiste à

   - convertir les informations provenant des capteurs ou des signaux envoyés par d'autres systèmes en informations appropriées pour l'affichage ou l'enregistrement sur des appareils indicateurs, des écrans, des imprimantes, etc. Le système produit des informations telles que les vues d'ensemble, les alarmes synthétiques, et les guides d'exploitation,
   - afficher les alarmes, les avertissements et d'autres informations,
   - fournir des interfaces pour mettre en œuvre les commandes manuelles.

c) Systèmes de protection et des actionneurs de sûreté

Ces systèmes assurent que les limites spécifiées dans la phase de conception ne sont pas dépassées lors des incidents de fonctionnement prévus et que les conséquences des accidents sont maintenus dans les limites de la conception.

Les fonctionnalités types de ces systèmes sont les suivantes:

- la détection d'une condition accidentelle et la mise en service automatique des systèmes appropriés, y compris ceux associés à l'arrêt du réacteur;
- la gestion les priorités entre les fonctions de différentes catégories (par exemple pour annuler des actions du système de contrôle-commande).

d) Système d'actionneurs liés à l'alimentation électrique de secours

Fonctionnalités types:

- délestage;
- séquence de montée en charge des groupes diesel et autres alimentations.

Les systèmes d'I&C réalisant les fonctions importantes pour la sûreté sont affectés à une des trois classes qui définissent les exigences à satisfaire au niveau de la conception, de la fabrication, et de la qualification, ce qui permet ainsi à ces systèmes de réaliser les fonctions d'une ou plusieurs des catégories A, B, C ou non classé (voir l'Article B.2). Un exemple de classement type des systèmes d'I&C est présenté au Tableau B1.

Tableau B.1 – Classement typique des systèmes d'I&C

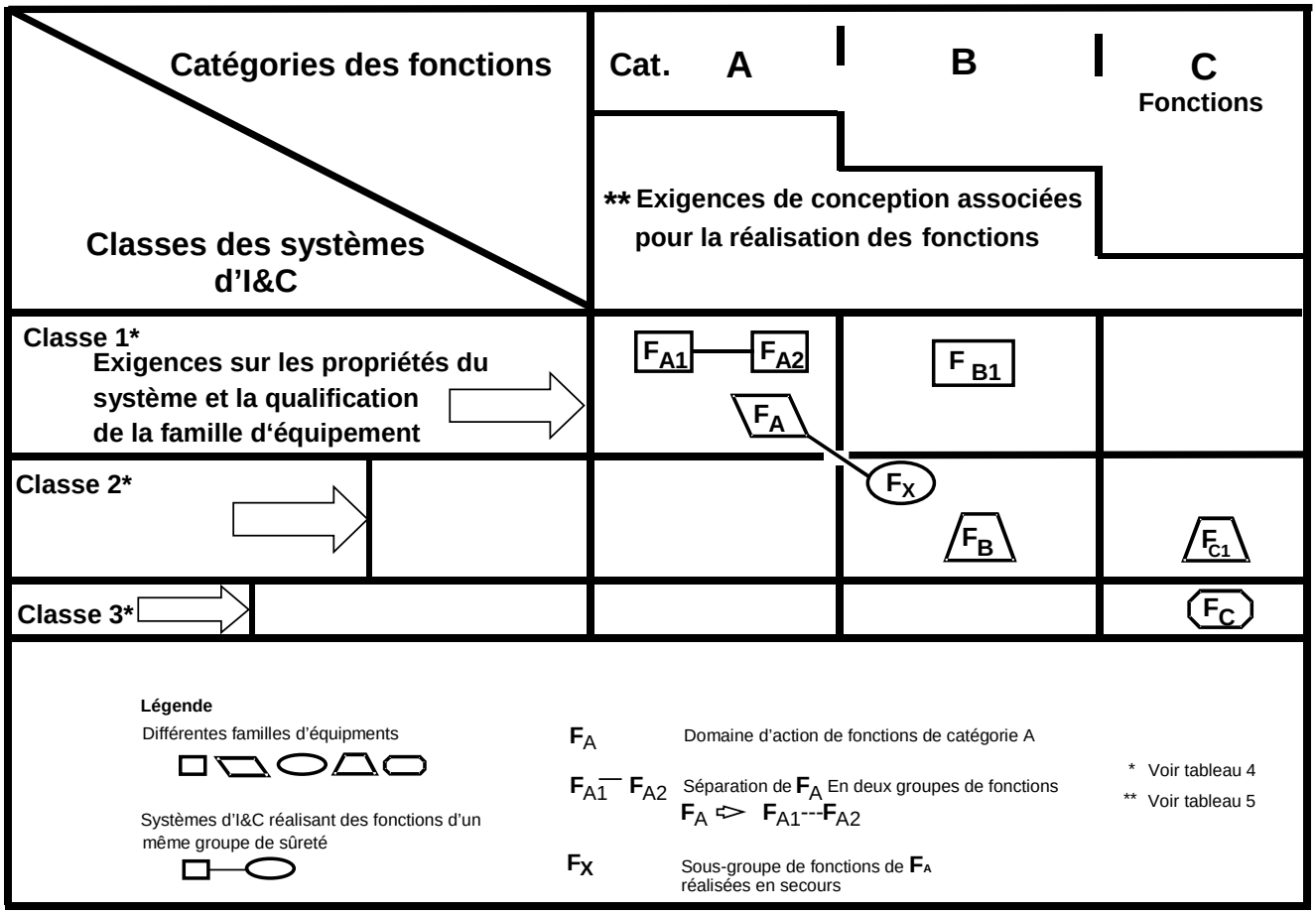
	Classe 1	**Classe 2**	**Classe 3**	**Non classé**
Systèmes d'automatisation et de contrôle-commande de la centrale		x	x	x
Systèmes d'IHM (l'IHM de classe 1 peut être limité à quelques indicateurs et boutons poussoir critiques)	x	x	x	x
Système de protection et des actionneurs de sûreté	x			
Système d'actionneurs lié à l'alimentation de secours	x			

Les exigences relatives à la fonction de catégorie la plus élevée de sûreté déterminent la classe du système.

Annexe C
(informative)

Défense qualitative contre les DCC

C.1 Exemple d'affectation des fonctions d'un groupe de sûreté aux systèmes d'I&C



IEC 1902/11

Figure C.1 – Exemples d'affectation des fonctions d'un groupe de sûreté aux systèmes d'I&C

Les exigences relatives aux propriétés et à la qualification des équipements, telles que par exemple la robustesse du logiciel ou celles relatives aux conditions d'environnement, peuvent être satisfaites en choisissant judicieusement une famille d'équipements. Les exigences systèmes se concentrent sur les caractéristiques de conception, comme par exemple, la tolérance aux fautes de l'architecture système, et l'adéquation des procédures de V&V de la conception pour garantir que les fonctionnalités sont correctes.

La Figure C.1 montre des exemples d'affectation des fonctions d'un groupe de sûreté à des systèmes d'I&C, exemples qui représentent différentes stratégies de conception mises en œuvre pour obtenir la fiabilité requise compte tenu des DCC possibles.

FA1---FA2: Le domaine du groupe de sûreté comprend deux fonctions de catégorie A avec diversité fonctionnelle FA1 and FA2. L'estimation issue de l'analyse des DCC montre que l'application de la diversité fonctionnelle donne une protection efficace contre la DCC. Les

deux fonctions sont alors réalisées dans des systèmes de classe 1 indépendants basés sur la même famille d'équipements.

FA---FX: Le domaine du groupe de sûreté comprend une fonction principale FA1 de catégorie A et une fonction additionnelle FX, de catégorie B ou C, utilisée en secours. L'estimation issue de l'analyse des DCC montre que dans ce cas l'application de la diversité des équipements donne une protection suffisante contre la DCC. La fonction FA est affectée à un système de classe 1 et la fonction FX est réalisée dans un système de classe 2 basé sur une famille d'équipements différente.

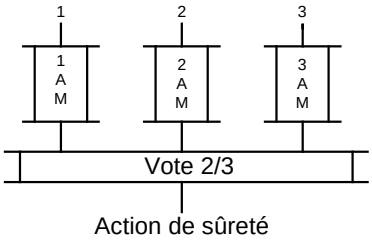
FB1---FB: Le domaine du groupe de sûreté comprend deux fonctions de catégorie B avec diversité fonctionnelle, FB1 et FB. L'estimation issue de l'analyse des DCC montre que l'application de la diversité matériel en complément à la diversité fonctionnelle donne une protection suffisante contre la DCC. La fonction FB1 est affectée à un système de classe 1 et la fonction FB est réalisée dans un système de classe 2 basé sur une famille d'équipements différente pour disposer d'une diversité d'équipement.

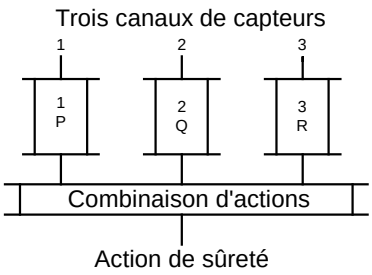
Le cas de FC1 et FC est analogue à celui de l'exemple précèdent.

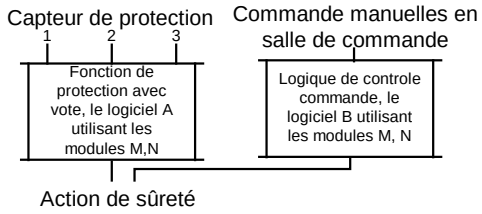
C.2 Exemples de sensibilité aux DCC des groupes de sûreté

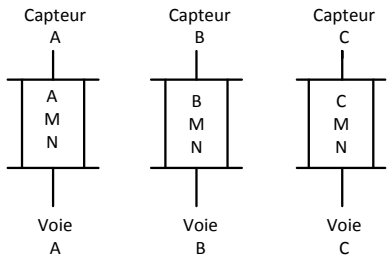
Les situations types suivantes peuvent exister.

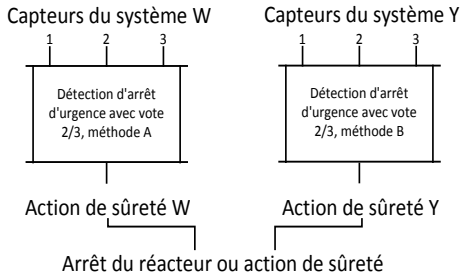
Tableau C.1 – Exemples de sensibilité aux DCC des groupes de sûreté

Exemple 1 Groupe de sûreté constitué d'un système avec trois voies redondantes identiques réalisant une fonction de protection A unique	
Causes potentielles de DCC Potentiel: (H) = Elevé; (M) = Moyen; (L) = Faible	**Défense possible** Efficacité: (H) = Elevée; (M) = Moyenne; (L) = Faible
– Une erreur dans la spécification des exigences de la fonction d'application A (H)	Vérification indépendante de la spécification (M)
– Une erreur dans la spécification ou le développement du logiciel d'application ou une erreur dans le module du logiciel système (M). Une défaillance peut se produire suite à des trajectoires similaires de signaux dans trois voies ((L) pour les systèmes de classe A)	Classe 1 de développement du système (H)
– Une défaillance simultanée dans le matériel des trois voies suite à un événement dangereux dans la centrale	Indépendance physique, électrique (H)
– Une défaillance dans le vote 2 sur 3 (ou autres mesures prises par les voies).	Classe 1 de développement du système (H); retour d'expérience fiable (module standard) (H)

Exemple 2 Groupe de sûreté constitué d'un système avec des voies redondantes réalisant une fonction de protection A unique avec une spécification des exigences commune et une mise en œuvre logicielle différente (unités P, Q, R.)	
Causes potentielles de DCC Potentiel: (H)= Elevé; (M) = Moyen; (L) = Faible	**Défense possible** Efficacité: (H) = Elevée; (M) = Moyenne; (L) = Faible
– Une erreur dans la spécification des exigences de la fonction d'application A (H)	Idem exemple 1
– Une erreur dans la spécification ou le développement du logiciel d'application ou une erreur dans le module du logiciel système (M). Une défaillance peut se produire suite à des trajectoires similaires de signaux dans trois voies (L)	Classe 1 de développement du système (H) Inconvénient: mise en œuvre logicielle multiple
– Une défaillance simultanée dans le matériel des trois voies suite à un événement dangereux dans la centrale	Idem exemple 1
– Une défaillance dans le vote 2 sur 3 (ou autres mesures prises par les voies).	Idem exemple 1

Exemple 3 Groupe de sûreté constitué d'un système avec deux voies réalisant différemment la même mesure de protection * * Ceci suppose que l'opérateur dispose d'un délai et d'informations suffisants pour réagir	
Causes potentielles de DCC Potentiel: (H)= Elevé; (M) = Moyen; (L) = Faible	**Défense possible** Efficacité: (H) = Elevée; (M) = Moyenne; (L) = Faible
– Une erreur dans la spécification des exigences des deux fonctions (L)	La défense est assurée par la diversité fonctionnelle (automatique, manuelle) (H)
– Une erreur dans la spécification ou le développement du logiciel d'application ou une erreur dans les modules M, N du logiciel système commun ((L) pour fonctionnement asynchrone)	Classe 1 de développement du système (H)
– Une défaillance simultanée dans le matériel des voies suite à un événement dangereux dans la centrale	Idem exemple 1
– Une défaillance dans le vote 2 sur 3 (ou autres mesures prises par les voies).	Commande manuelle agissant en aval du voteur (H)

Exemple 4 Groupe de sûreté constitué de diverses fonctions de protection A, B, C utilisant différents capteurs et actionneurs et un matériel similaire dans chaque voie de commande	
Causes potentielles de DCC Potentiel: (H)= Elevé; (M) = Moyen; (L) = Faible	**Défense possible** Efficacité: (H) = Elevée; (M) = Moyenne; (L) = Faible
– Une erreur dans la spécification des exigences des trois fonctions (L)	La défense est assurée par la diversité fonctionnelle (P, Q, R) (H)
– Une erreur dans la spécification ou le développement du logiciel d'application ou une erreur dans les modules M, N du logiciel système commun ((L) pour fonctionnement asynchrone). Les trajectoires des signaux sont différentes (L)	Matériel totalement indépendant Classe 1 de développement du système (H)
– Une défaillance simultanée dans le matériel des voies suite à un événement dangereux dans la centrale	Idem exemple 1
– Une défaillance dans le vote 2 sur 3 (ou autres mesures prises par les voies).	Commande manuelle agissant en aval du voteur (H)

Exemple 5 Groupe de sûreté constitué de diverses fonctions de protection W et Y réparties dans deux systèmes différents (matériel et logiciel système divers avec similitudes possibles, par exemple algorithmes similaires, synchronisation similaire, documentation similaire, personnel commun)	
Causes potentielles de DCC Potentiel: (H)= Elevé; (M) = Moyen; (L) = Faible	**Défense possible** Efficacité: (H) = Elevée; (M) = Moyenne; (L) = Faible
– Une erreur dans la spécification des exigences des deux fonctions (L)	La défense est assurée par la diversité fonctionnelle (W, Y) (H)
Une erreur dans la spécification ou le développement du logiciel d'application ou une erreur dans les modules M, N du logiciel système commun ((L) pour fonctionnement asynchrone)	Matériel totalement indépendant Classe 1 de développement du système (H)
– Une défaillance simultanée dans le matériel des voies suite à un événement dangereux dans la centrale	Idem exemple 1
– Une défaillance dans les deux mesures d'actionnement de sûreté (L)	Systèmes d'actionnement différents (divers) (H)

Annexe D
(informative)

Relations de la CEI 61508 avec la CEI 61513 et les normes du secteur nucléaire

D.1 Généralités

Cette annexe compare la présente norme avec la CEI 61508-1:2010, la CEI 61508-2:2010 et la CEI 61508-4:2010.

Les Parties 3, 5, 6 et 7 de la CEI 61508 ne sont pas prises en compte car les sujets traités sortent du domaine de la présente norme. Par exemple le domaine d'application de la Partie 3 de la CEI 61508, sur le logiciel, est partiellement couvert par la CEI 60880 et la CEI 62138.

La présente annexe comporte quatre articles:

- D.2 identifie les principales différences entre les domaines d'application et les concepts utilisés dans les deux normes,
- D.3 compare la présente norme avec la CEI 61508-1 (exigences générales)
- D.4 compare la présente norme avec la CEI 61508-2 (aspects système)
- D.5 compare la présente norme avec la CEI 61508-4 (définitions).

Abréviations

E/E/EP	Electrique/Electronique/Electronique programmé
EUC	Equipement commandé
SIL	Niveau d'intégrité de sûreté

D.2 Comparaison des domaines d'application et concepts

La comparaison révèle tout d'abord certaines différences importantes au niveau des domaines d'application des deux normes.

Les systèmes traités dans la CEI 61508 peuvent être électriques, électroniques ou électroniques programmables, et bien que la présente norme établisse les principes relatifs aux exigences d'architecture pour les trois technologies, l'accent est mis sur les systèmes programmés.

La CEI 61508 fait en général référence aux « systèmes liés à la sûreté » alors que la présente norme suit la pratique de l'AIEA et fait référence aux « systèmes importants pour la sûreté » (c'est-à-dire importants pour la sûreté nucléaire »).

NOTE Il est fait l'hypothèse que pour la conception des systèmes d'I&C qui sont supports de fonctions de sûreté conventionnelle (par exemple pour garantir la sécurité des travailleurs, la protection des biens, la prévention contre les risques chimiques, la prévention contre les risques liés au procédé énergétique) on applique des normes nationales ou internationales, dont les exigences sont basées sur celles de la normes CEI 61508.

a) Etendue du cycle de vie de sûreté d'ensemble

Le cycle de vie de sûreté d'ensemble de la norme CEI 61508 inclut tous les systèmes prévus par la conception de sûreté des équipements sous contrôle y compris: les systèmes d'I&C (E/E/EP), les systèmes d'autres technologies et les installations de réduction des risques externes.

La présente norme n'aborde pas spécifiquement l'analyse de sûreté de la centrale ni n'identifie les méthodes d'estimation de l'adéquation des exigences de performance et de

fiabilité résultant de l'analyse. La pratique dans le secteur nucléaire veut que la conception de sûreté de la centrale soit réalisée conformément aux principes spécifiques de l'AIEA, aux règles CEI et aux réglementations nationales qui ne sont pas couverts par le domaine d'application de la présente norme. La base de conception de la centrale définit les séquences d'EIP, le concept de défense en profondeur de la centrale, les catégories des fonctions requises pour assurer les défenses. Cependant, la présente norme identifie les informations d'entrée requises issues de la conception de la centrale et de l'analyse de sûreté qui doivent être mises à la disposition des concepteurs de l'I&C afin de guider la conception ultérieure des systèmes d'I&C.

b) Validation/estimation de la sûreté d'ensemble

Dans la présente norme, la vérification et la validation globales de chaque fonction affectée et importante pour la sûreté sont enregistrées dans le rapport d'intégration et de mise en service d'ensemble.

Dans le secteur nucléaire, l'estimation de l'adéquation de ce rapport relativement à la sûreté est réglementée dans le cadre de procédures d'attribution des licences.

c) Systèmes d'I&C et architecture d'I&C

Les systèmes d'I&C de la présente norme sont équivalents aux systèmes E/E/EP de la norme CEI 61508. Dans la présente norme, l'architecture d'I&C (voir Article 5) définit un certain nombre de systèmes réalisant les fonctions importantes pour la sûreté, avec des classes et des exigences d'indépendance précises. Pour chacun de ces systèmes, l'Article 6 définit un cycle de sûreté individuel. Dans la CEI 61508 la répartition en systèmes, le cas échéant, est effectuée dans la Partie 2.

Il convient de ne pas oublier cette différence afin d'éviter tout malentendu.

d) Niveau et classement de l'intégrité de la sûreté

La CEI 61508 classifie le niveau d'intégrité de la sûreté requis pour un système programmé en fonction de la réduction du risque que le système est tenu d'assurer. Cela est réalisé en déterminant la gravité du risque associé au danger et en estimant la fréquence du danger et la protection que le système doit apporter pour ramener le risque à un niveau acceptable.

L'industrie nucléaire utilise traditionnellement une méthode déterministe pour évaluer l'importance pour la sûreté d'un système et son impact sur la gravité du risque associé avec un possible rejet radioactif (voir Guides AIEA pour la sûreté et CEI 61226).

Le niveau d'intégrité le plus élevé possible est généralement considéré nécessaire à tout système qui empêche ou atténue les conséquences d'un rejet radioactif. Un niveau inférieur peut être acceptable pour les systèmes qui contribuent à la protection contre les rejets mais qui ne les empêchent ni ne les atténuent directement. En conséquence, il n'existe pas de procédé d'utilisation courante dans le secteur nucléaire qui soit équivalent aux niveaux SIL de fiabilité/réduction des risques proposés par la CEI 61508. Cette approche déterministe s'est en général avérée suffisante dans l'industrie nucléaire et a conduit, dans la pratique, à la détermination d'objectifs très élevés pour toutes les fonctions de protection. Cependant, le secteur nucléaire reconnaît que l'approche numérique et les méthodes d'analyse probabiliste de sûreté (APS) pourraient permettre de déterminer des objectifs plus précis pour la fiabilité des systèmes programmés.

L'affectation des fonctions de sûreté à des « niveaux d'intégrité » de la CEI 61508 est très similaire à la catégorisation appliquée aux fonctions de sûreté nucléaire dans l'industrie nucléaire. Cependant, il existe une différence considérable dans la procédure d'affectation:

- dans la CEI 61508, l'affectation des fonctions de sûreté nucléaire aux niveaux d'intégrité de la sûreté est basée sur un risque probabiliste et une analyse du risque;
- dans la CEI 61226, l'affectation aux catégories est basée sur des critères déterministes et un jugement technique des conséquences en cas de dysfonctionnement.

D.3 Correspondances entre la CEI 61508-1 et la présente norme

CEI 61508–1	CEI 61513
5 Documentation	5.6 Exigences relatives à la documentation
6 Gestion de la sécurité fonctionnelle	5.5.2 Conformément aux documents AIEA GS-R-3 et GS-G-3.1, toutes les activités liées à une centrale nucléaire, sont couvertes par un programme d'AQ ou de préférence un système de gestion intégré
7 Exigences relatives au cycle de sécurité global	5 Cycle de vie de sûreté de l'ensemble de l'I&C
7.1 Généralités	
Le cycle de vie de sûreté d'ensemble comprend: les E/E/PES, les autres technologies et les réductions du risque externe	Le cycle de vie de sûreté de l'ensemble de l'I&C comprend les fonctions, les systèmes et les équipements d'I&C importants pour la sûreté et l'architecture globale des systèmes d'I&C (voir a) de l'Article D.2)
7.2 Concept	
Description de l'EUC, de ses fonctions de commande requises et de l'environnement physique	Revue de la conception de sûreté de la centrale (5.2): – pour identifier les conditions environnementales imposées (5.2.4) – les fonctions d'I&C importantes pour la sûreté – actions automatiques et mesures prises par l'opérateur
Identification des sources de danger	Les événements dangereux internes et externes sont définis par la conception de sûreté de la centrale et constituent une information d'entrée pour l'I&C (5.2.4) (voir a) de l'Article D.2)
7.3 Définition du domaine d'application global	
Pour déterminer la limite de l'EUC	Pour identifier les limites imposées à la centrale/l'I&C (5.2.4)
Pour spécifier l'étendue du danger, l'analyse du risque et les événements initiateurs d'accidents	Les événements initiateurs (EIP) sont définis par la base de conception de sûreté de la centrale et constituent une information d'entrée pour l'I&C (5.2) (voir point a) de l'Article D.2)
7.4 Analyse du danger et des risques	
Identification du danger de l'EUC…	Hors du champ d'application de la présente norme, fait partie de la conception de la centrale (voir point a) de l'Article D.2)
…et du système de commande de l'EUC	Les contraintes déterministes pour l'I&C, par exemple le critère de défaillance unique pour les fonctions de catégorie A et l'isolement fonctionnel, proviennent de la conception de la centrale
Pour déterminer la séquence des événements jusqu'aux événements dangereux	Les séquences d'EIP sont définies par la conception de sûreté de la centrale et constituent une information d'entrée pour l'I&C (voir 5.2) (voir point a) de l'Article D.2)
Pour déterminer le risque d'EUC	La catégorisation des fonctions d'I&C constitue une entrée pour l'I&C (voir 5.2.3) (voir point a) de l'Article D.2)
7.5 Exigences globales de sécurité	5.3 Spécification des exigences globales relatives aux fonctions d'I&C
Les fonctions de sûreté nécessaires sont spécifiées. Elles incluent:	Les spécifications des exigences globales relatives aux fonctions d'I&C importantes pour la sûreté proviennent de la conception de la centrale. Elles incluent:
o les spécifications des exigences relatives aux fonctions	la spécification des exigences de fonctionnalité et performance (voir a) 1) et a) 2) de 5.3)
o les spécifications des exigences relatives à l'intégrité de la sûreté	la spécification des catégories de fonctions d'I&C (voir a) 3) 5.3) la spécification des exigences d'indépendance (b de 5.3)
La spécification des exigences relatives à la sécurité globale comprend l'I&C (systèmes E/E/EP), les systèmes d'autres technologies et les installations de réduction des risques	Les mesures liées aux autres technologiques et à la réduction des risques sont définies par la conception de sûreté de la centrale selon le principe de défense en profondeur. Elles sont en dehors du cadre de la présente norme (voir point a) de l'Article D.2)

CEI 61508–1	CEI 61513
7.6 Allocation des exigences de sécurité	5.4.2 Conception de l'architecture d'I&C 5.4.3 Affectation des fonctions aux systèmes
Allouer les fonctions de sûreté aux systèmes et allouer un niveau d'intégrité de la sûreté à chaque fonction. La possibilité de DCC est prise en compte (7.6.2.7) et la sûreté cible d'un E/E/EP unique est limitée (7.6.2.11)	Décomposer l'ensemble de l'I&C en suffisamment de systèmes d'I&C de la classe appropriée Allouer les fonctions d'I&C aux systèmes d'I&C en fonction de le classement, de la défense en profondeur et en tenant compte des DCC
Planification globale	5.5 Planification globale
6 Gestion de la sécurité fonctionnelle	5.5.2 Plan d'assurance qualité globale
7.8 Planification globale de la validation de la sécurité	5.5.4 Plan d'intégration et de mise en service globales
	5.5.3 Plan de sécurité globale
7.9 Planification globale de l'installation et de la mise en service	5.5.4 Plan d'intégration et de mise en service globales
7.7 Planification globale de l'exploitation et de la maintenance	5.5.5 Plan d'exploitation globale
	5.5.6 Plan de maintenance global
	5.5.7 Plan de formation
7.10 Spécification des exigences de sûreté	6.2.2 Spécification des exigences système
7.11 Réalisation: systèmes E/E/EP	6 Cycle de sûreté du système
Voir Partie 2 de la CEI 61508 (aspects système)	Voir Article 6 (cycle de sûreté du système)
Voir Partie 3 de la CEI 61508 (exigences relatives au logiciel)	Le logiciel est hors du domaine d'application de la présente norme
7.12 Autres dispositifs de réduction de risque – Spécification et réalisation	Hors du domaine d'application de la présente norme (voir point a) de l'Article D.2)
7.13 Installation et mise en service globales	7 Intégration et mise en service globales
7.14 Validation globale de la sécurité Pour valider le respect par les E/E/EP de la spécification des exigences globales selon l'affectation	7.2 Mise en service globale Pour vérifier et valider les fonctions importantes pour la sûreté réparties sur plusieurs systèmes 6.5 Qualification
7.15 Exploitation, maintenance et réparation globales	8 Exploitation et maintenance globales
7.16 Modification et remise à niveau globales	1 Domaine d'application La norme (ou une partie) s'applique à l'I&C des nouvelles centrales nucléaires ainsi qu'aux améliorations et aux modifications. 6.2.8 Modification de la conception système
7.17 Mise hors service ou au rebut	Hors du domaine d'application de la présente norme
7.18 Vérification	5.5.2 Plan global d'assurance qualité
8 Evaluation de la sécurité fonctionnelle Pour analyser et parvenir à un jugement sur la sûreté fonctionnelle atteinte par les systèmes E/E/EP	Dans le secteur nucléaire, cette estimation est liée au processus d'autorisation et dépend des organismes de réglementation de sûreté et des réglementations nationales

D.4 Correspondances entre la CEI 61508-2 et la présente norme

CEI 61508–2 Aspects système	CEI 61513
5 Documentation	6.4 Documentation produite
6 Gestion de sûreté fonctionnelle	5.5.2 Plan d'assurance qualité
7 Exigences sur le cycle de vie de sécurité des systèmes E/E/EP	6 Cycle de vie de sûreté du système Le cadre du cycle de vie de sûreté du système

CEI 61508–2 Aspects système	CEI 61513
Le cadre du cycle de vie de sécurité des systèmes E/E/EP comprend les objectifs et exigences relatifs aux systèmes E/E/EP	comprend les objectifs et exigences relatifs aux systèmes individuels d'I&C de l'architecture d'I&C (voir point c) de l'Article D.2)
7.1 Généralités Le Tableau 1 indique, pour toutes les phases, les objectifs et exigences, l'étendue de la phase, les entrées et les sorties requises	 Le Tableau 3 indique, pour toutes les phases, les objectifs et exigences, les entrées et les sorties requises
7.2 Spécification des exigences relatives à la conception des systèmes E/E/EP Elle inclut:	6.2.2 Exigences sur le système Elle inclut:
– les exigences relatives aux fonctions de sécurité	les exigences relatives aux fonctions d'application les exigences relatives aux fonctions de service les conditions environnementales (6.2.2.6)
– les exigences relatives à l'intégrité de sécurité	la catégorisation des fonctions d'I&C (entrée de 5.3), les exigences relatives aux contraintes de conception (6.2.2.3) le classement des systèmes
NOTE Ces articles de la CEI 61508 et de la présente norme couvrent les mêmes sujets, mais la présente norme fait une distinction entre les exigences relatives aux fonctions d'I&C et celles relatives aux systèmes d'I&C réalisant ces fonctions.	
7.3 Planification de la validation de la sécurité des systèmes E/E/EP	6.3 Exigences relatives aux plans
	– Plan de validation du système (6.3.5) – Validation fonctionnelle de la spécification des exigences (6.2.4.2.1) – Exigences pour la qualification du système (6.5)
7.4 Conception et développement des systèmes E/E/EP	6.2.3 Spécification du système 6.2.4 Conception et réalisation du système
7.4.2 Exigences générales	– contraintes de conception (6.2.2.3) – architecture du système (6.2.3.3) – documentation de spécification système (6.4.3)
7.4.3 Synthèse des éléments permettant d'atteindre les capacités système	– cycle de sûreté du système (Article 6) – exigences portant sur les contraintes de conception (6.2.2.3)
7.4.4 Contraintes d'architecture sur l'intégrité de la sécurité du matériel	– exigences relatives aux contraintes de conception (6.2.2.3)
7.4.5 Exigences relatives à la quantification des effets des défaillances matériel	– évaluation de la fiabilité (6.2.4.2.2)
7.4.6 Exigences pour l'évitement des erreurs systématiques	– conception de l'architecture d'ensemble de l'I&C (5.4.2) de façon à satisfaire les principes de défense en profondeur – évaluation de la fiabilité et des défenses contre les DCC (5.4.4.2) – évaluation des facteurs humains (5.4.4.3) – répartition géographique des sous-systèmes (6.2.3.3.2) – indépendance (6.2.3.3.3) – défense contre la propagation et les effets secondaires des défaillances (6.2.3.3.4)
7.4.7 Exigences pour le contrôle des erreurs systématiques	
7.4.8 Exigences portant sur le comportement du système pour la détection des défauts	– architecture système (6.2.2.3.2) – auto-supervision et tolérance aux défaillances

CEI 61508–2 Aspects système	CEI 61513
	(6.2.2.3.4)
7.4.9 Exigences pour la réalisation des systèmes E/E/EP	– sélection des composants préexistants (6.2.3.2)
7.4.10 Exigences portant sur les éléments approuvés sur la base de leur retour d'expérience	– sélection des composants préexistants (6.2.3.2) avec référence aux recommandations particulières de la CEI 60880, CEI 62138 et CEI 60987
7.4.11 Exigences supplémentaires portant sur les communications de données	– exigences portant sur les communications de données (5.4.2.4) complétées par la CEI 61500 – comportement interne du système (6.2.2.3.3)
7.5 Intégration des systèmes E/E/EP	6.2.5 Intégration du matériel/logiciel système
7.6 Procédures d'exploitation et de maintenance des systèmes E/E/EP	6.3.7 Plan d'exploitation des systèmes
7.7 Validation de sécurité des systèmes E/E/EP	6.2.6 Validation des systèmes
7.8 Modification des systèmes E/E/EP	6.2.8 Modification des systèmes
7.9 Vérification des systèmes E/E/EP	6.3.2.2 Plan de vérification du système
8 Evaluation de la sécurité fonctionnelle des systèmes E/E/EP Voir la CEI 61508-1	Voir Article D.3, dernier élément

D.5 Correspondances entre certains termes importants de la CEI 61508-4 et les définitions en usage dans la présente norme et dans le secteur nucléaire

Sujet: Analyse des risques	
CEI 61508-4	**CEI 61513**
3.1.2 phénomène dangereux Une source potentielle de nuisance (Guide 51 ISO/CEI) [19] NOTE Ce terme comprend le danger sur des personnes survenant dans un laps de temps très court (feu ou explosions), mais aussi le danger à long terme sur la santé d'une personne (dégagement d'une substance toxique).	**3.25 événement dangereux**

Sujet: Défense en profondeur	
CEI 61508-4	**CEI 61513**
3.4.2 autres mesures de réduction de risque Mesure destinée à réduire ou atténuer les risques qui sont séparées et distinctes et n'utilisent pas de système E/E/PE relatif à la sécurité	**concept de « défense en profondeur » (voir l'Article A.4)** Le concept de réduction du risque est implicite dans l'analyse de sûreté d'une centrale nucléaire avec le concept de défense en profondeur et les lignes de défense

Sujet: Systèmes importants pour la sûreté	
CEI 61508-4	**CEI 61513**
3.4.1 système relatif à la sécurité Un tel système est un système qui, à la fois: – met en œuvre les fonctions de sécurité requises pour atteindre un état de sécurité pour l'EUC ou pour maintenir un tel état; – est conçu pour atteindre, par lui-même ou grâce à des systèmes E/E/EP relatifs à la sécurité, ou des systèmes relatifs à la sécurité basés sur une autre	**3.33 constituant important pour la sûreté**

technologie ou des dispositifs externes de réduction de risque, le niveau d'intégrité de sécurité nécessaire à la mise en œuvre des fonctions de sécurité requises.	

Sujet: Systèmes d'I&C	
CEI 61508-4	**CEI 61513**
3.2.13 électrique/électronique/électronique programmable (E/E/PE) Technologie basée sur la technologie électrique (E) et/ou électronique (E) et/ou électronique programmable (EP)	**3.29 système d'I&C**

Sujet: Fiabilité	
CEI 61508-4	**CEI 61513**
3.5.4 intégrité de sécurité Probabilité pour qu'un système relatif à la sécurité exécute de manière satisfaisante les fonctions de sécurité requises dans toutes les conditions spécifiées dans une période de temps spécifiée. NOTE 3 Il convient que l'évaluation de l'intégrité de sécurité prenne en compte toutes les causes de défaillance (à la fois les défaillances aléatoires du matériel et les défaillances systématiques) conduisant à un état de non sécurité, par exemple les défaillances de matériel, les défaillances induites du logiciel et les défaillances dues aux perturbations électriques. Certaines de ces défaillances, en particulier les défaillances accidentelles du matériel, peuvent être quantifiées à l'aide de mesures telles que celle du taux de défaillance en mode de défaillance dangereux, ou de la probabilité de défaillance de fonctionnement à la demande d'un système de protection de sécurité. Cependant, la sécurité intégrale d'un système dépend également de plusieurs facteurs qui ne peuvent être précisément quantifiés, mais simplement considérés d'un point de vue qualitatif.	**3.43 fiabilité** Dans la présente norme, l'estimation de la fiabilité est généralement qualitative (voir 6.2.2.2.2) (voir 6.2.2.2 et 6.2.4.2.2)

Sujet: Classement des systèmes importants pour la sûreté	
CEI 61508-4	**CEI 61513**
3.5.8 niveau d'intégrité de sécurité niveau discret (parmi quatre possibles) permettant de spécifier les exigences concernant l'intégrité de sécurité des fonctions de sécurité à allouer aux systèmes E/E/PE relatifs à la sécurité. Le niveau 4 d'intégrité de sécurité possède le plus haut degré d'intégrité; le niveau 1 possède le plus bas	**3.6 classe d'un système d'I&C** Tous les composants, structures et systèmes importants pour la sûreté sont classés selon leurs fonctions et leur importance pour la sûreté. Ils sont conçus, fabriqués et installés de manière à ce que leur qualité soit proportionnelle à ce classement (Article 78 de l'AIEA 75-INSAG-3:1999) La CEI 61226 fixe une limite pour la valeur de l'objectif de fiabilité qu'on peut prétendre atteindre (10^{-4}) avec les systèmes contenant un logiciel. Pour certains systèmes, les objectifs de fiabilité peuvent être plus élevés que ce qui peut être démontré. S'il est nécessaire de garantir cette plus grande fiabilité fonctionnelle, des systèmes indépendants supplémentaires sont utilisés, chacun d'entre eux étant capable d'accomplir la fonction de sûreté attribuée. La diversité et la séparation physique de ces systèmes réduisent les possibilités de défaillances de cause commune (objectifs de fiabilité (AIEA 75-INSAG-3; 1999, Articles 174-176)

Sujet: Défaillance de cause commune	
CEI 61508-4	**CEI 61513**
3.6.10 défaillance de cause commune Défaillance résultant d'un ou plusieurs événements qui, provoquant des défaillances simultanées de deux ou plusieurs canaux séparés dans un système multicanal conduit à la défaillance du système. NOTE Les paragraphes 7.6.2.7 et 7.6.2.8 de la CEI 61508-1:2010 fournit les exigences d'attribution relatives à l'indépendance de deux systèmes.	**3.8 défaillance de cause commune** Voir 5.4.2.6

Annexe E
(informative)

Modifications à réaliser dans les prochaines révisions de normes du SC 45A pour les adapter à la présente version de la CEI 61513

CEI 60880:2006	Modifications à réaliser
3 Termes et définitions	Les définitions doivent être alignées
6.3 Essais périodiques	Tout supprimer sauf 6.3.1 et 6.3.2. Maintenant couvert par 6.2.2.3.5 de la CEI 61513
9.3 Vérification du système intégré	Supprimer le paragraphe. Maintenant couvert par 6.2.5 et 6.3.4 de la CEI 61513
9.4 Procédure de résolution des défauts	Supprimer le paragraphe. Maintenant couvert par 6.3.2.4 de la CEI 61513
9.5 Aspects logiciel dans le compte rendu de vérification du système intégré	Supprimer le paragraphe. Maintenant couvert par 6.4.5 de la CEI 61513
10.1 Aspects logiciel du plan de validation système	Supprimer le paragraphe. Maintenant couvert par les 6.2.6 et 6.3.5 de la CEI 61513
10.3 Aspects logiciel du compte rendu de validation système	Supprimer le paragraphe. Maintenant couvert par le 6.4.6 de la CEI 61513
10.4 Procédure de résolution des défauts	Supprimer le paragraphe. Maintenant couvert par 6.3.2.4 de la CEI 61513
12.4 Formation des opérateurs	Supprimer le paragraphe. Maintenant couvert par le 5.5.7 de la CEI 61513.

CEI 62138:2004	Modifications à réaliser
3 Termes et définitions	Les définitions doivent être alignées
5.6 et 6.6 Aspects logiciel de l'intégration système	Considérer la suppression des paragraphes. Le sujet est maintenant couvert par 6.2.5 et 6.3.4 de la CEI 61513
5.7 et 6.7 Aspects logiciel de la validation système	Considérer la suppression. Le sujet est maintenant couvert par 6.2.6 et 6.3.5 de la CEI 61513

CEI 61226:2009	Modifications à réaliser
3 Termes et définitions	Les définitions doivent être alignées
Nouvelle annexe	Récupérer le contenu de l'Annexe B

Bibliographie

[1] CEI 61508-1:2010, *Sécurité fonctionnelle des systèmes électriques/électroniques/ électroniques programmables relatifs à la sécurité – Partie 1: Prescriptions générales*

[2] IEC 61508-3:2010, *Sécurité fonctionnelle des systèmes électriques/électroniques/ électroniques programmables relatifs à la sécurité – Partie 3: Exigences concernant les logiciels*

[3] Glossaire de Sûreté de l'AIEA, *Technology Used in Nuclear Safety and Radiation Protection –version 2007*

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

[5] CEI 61069-1:1991, *Mesure et commande dans les processus industriels – Appréciation des propriétés d'un système en vue de son évaluation – Partie 1: Considérations générales et méthodologie*

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

[7] ISO 8402:1994, *Management de la qualité et assurance de la qualité – Vocabulaire*

[8] Directives ISO/CEI, Partie 2, 2004: *Règles de structure et de rédaction des Normes internationales*

[9] ISO/CEI 12207:2008, *Ingénierie des systèmes et du logiciel – Processus du cycle de vie du logiciel*

[10] CEI 60050-394 :2007, *Vocabulaire Electrotechnique International – Partie 394: Instrumentation nucléaire – Instruments, systèmes, équipements et détecteurs*

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

[12] CEI 62342, *Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle-commande importants pour la sûreté – Gestion du vieillissement*

[13] CEI 61000-6-2, *Compatibilité électromagnétique (CEM) – Partie 6-2: Normes génériques – Immunité pour les environnements industriels*,

[14] CEI 61000-6-4, *Compatibilité électromagnétique (CEM) – Partie 6-4: Normes génériques – Norme sur l'émission pour les environnements industriels,*

[15] CEI 62003:2009, *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Exigences relatives aux essais de compatibilité électromagnétique*

[16] CEI 61225, *Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle-commande importants pour la sûreté – Exigences pour les alimentations électriques*

[17] ISO 10007, *Systèmes de management de la qualité – Lignes directrices pour la gestion de la configuration*

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

[19] ISO/IEC Guide 51:1990, *Guide pour l'introduction dans les normes des aspects liés à la sûreté*

_____

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

3, rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

Tel: + 41 22 919 02 11
Fax: + 41 22 919 03 00
info@iec.ch
www.iec.ch