

**NORME
INTERNATIONALE
INTERNATIONAL
STANDARD**

**CEI
IEC**

61513

Première édition
First edition
2001-03

**Centrales nucléaires –
Instrumentation et contrôle commande des
systèmes importants pour la sûreté –
Prescriptions générales pour les systèmes**

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



Numéro de référence
Reference number
CEI/IEC 61513:2001

Numérotation des publications

Depuis le 1er janvier 1997, les publications de la CEI sont numérotées à partir de 60000. Ainsi, la CEI 34-1 devient la CEI 60034-1.

Editions consolidées

Les versions consolidées de certaines publications de la CEI incorporant les amendements sont disponibles. Par exemple, les numéros d'édition 1.0, 1.1 et 1.2 indiquent respectivement la publication de base, la publication de base incorporant l'amendement 1, et la publication de base incorporant les amendements 1 et 2.

Informations supplémentaires sur les publications de la CEI

Le contenu technique des publications de la CEI est constamment revu par la CEI afin qu'il reflète l'état actuel de la technique. Des renseignements relatifs à cette publication, y compris sa validité, sont disponibles dans le Catalogue des publications de la CEI (voir ci-dessous) en plus des nouvelles éditions, amendements et corrigenda. Des informations sur les sujets à l'étude et l'avancement des travaux entrepris par le comité d'études qui a élaboré cette publication, ainsi que la liste des publications parues, sont également disponibles par l'intermédiaire de:

- Site web de la CEI (www.iec.ch)
- Catalogue des publications de la CEI

Le catalogue en ligne sur le site web de la CEI (www.iec.ch/catlg-f.htm) vous permet de faire des recherches en utilisant de nombreux critères, comprenant des recherches textuelles, par comité d'études ou date de publication. Des informations en ligne sont également disponibles sur les nouvelles publications, les publications remplacées ou retirées, ainsi que sur les corrigenda.

- IEC Just Published

Ce résumé des dernières publications parues (www.iec.ch/JP.htm) est aussi disponible par courrier électronique. Veuillez prendre contact avec le Service client (voir ci-dessous) pour plus d'informations.

- Service clients

Si vous avez des questions au sujet de cette publication ou avez besoin de renseignements supplémentaires, prenez contact avec le Service clients:

Email: custserv@iec.ch
Tél: +41 22 919 02 11
Fax: +41 22 919 03 00

Publication numbering

As from 1 January 1997 all IEC publications are issued with a designation in the 60000 series. For example, IEC 34-1 is now referred to as IEC 60034-1.

Consolidated editions

The IEC is now publishing consolidated versions of its publications. For example, edition numbers 1.0, 1.1 and 1.2 refer, respectively, to the base publication, the base publication incorporating amendment 1 and the base publication incorporating amendments 1 and 2.

Further information on IEC publications

The technical content of IEC publications is kept under constant review by the IEC, thus ensuring that the content reflects current technology. Information relating to this publication, including its validity, is available in the IEC Catalogue of publications (see below) in addition to new editions, amendments and corrigenda. Information on the subjects under consideration and work in progress undertaken by the technical committee which has prepared this publication, as well as the list of publications issued, is also available from the following:

- IEC Web Site (www.iec.ch)
- Catalogue of IEC publications

The on-line catalogue on the IEC web site (www.iec.ch/catlg-e.htm) enables you to search by a variety of criteria including text searches, technical committees and date of publication. On-line information is also available on recently issued publications, withdrawn and replaced publications, as well as corrigenda.

- IEC Just Published

This summary of recently issued publications (www.iec.ch/JP.htm) is also available by email. Please contact the Customer Service Centre (see below) for further information.

- Customer Service Centre

If you have any questions regarding this publication or need further assistance, please contact the Customer Service Centre:

Email: custserv@iec.ch
Tel: +41 22 919 02 11
Fax: +41 22 919 03 00

**NORME
INTERNATIONALE
INTERNATIONAL
STANDARD**

**CEI
IEC**

61513

Première édition
First edition
2001-03

**Centrales nucléaires –
Instrumentation et contrôle commande des
systèmes importants pour la sûreté –
Prescriptions générales pour les systèmes**

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

© IEC 2001 Droits de reproduction réservés — Copyright - all rights reserved

Aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'éditeur.

No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from the publisher.

International Electrotechnical Commission
Telefax: +41 22 919 0300

3, rue de Varembé Geneva, Switzerland
e-mail: inmail@iec.ch IEC web site <http://www.iec.ch>



Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

CODE PRIX
PRICE CODE **XD**

*Pour prix, voir catalogue en vigueur
For price, see current catalogue*

SOMMAIRE

AVANT-PROPOS	6
INTRODUCTION	8
1 Domaine d'application	10
1.1 Généralités	10
1.2 Application: centrales nouvelles et préexistantes	10
1.3 Cadre général	10
2 Références normatives	16
3 Définitions	20
4 Symboles et abréviations	42
5 Cycle de vie et de sûreté global de l'I&C	42
5.1 Elaboration des exigences relatives à l'I&C à partir de la conception de la sûreté de la centrale	50
5.2 Documentation	54
5.3 Conception de l'architecture globale de l'I&C et affectation des fonctions d'I&C	56
5.4 Planification globale	68
5.5 Documentation	78
6 Cycle de vie et de sûreté du système	78
6.1 Prescriptions	86
6.2 Planification du système	110
6.3 Prescriptions relatives à la documentation	120
6.4 Qualification du système	130
6.5 Résumé des principales prescriptions spécifiques aux différentes classes et catégories	140
7 Intégration et mise en service globales	142
7.1 Prescriptions relatives aux objectifs à atteindre	142
7.2 Prescriptions relatives à la documentation	142
8 Exploitation et maintenance globales	142
8.1 Prescriptions relatives aux objectifs à atteindre	144
8.2 Prescriptions relatives à la documentation	144
Annexe A (informative) Problèmes de base de sûreté dans les centrales nucléaires	146
Annexe B (informative) Catégorisation des fonctions et classification des systèmes	154
Annexe C (informative) Défense qualitative contre les DCC	164
Annexe D (informative) Relations de la CEI 61508 avec la CEI 61513 et les normes du secteur nucléaire	172
Bibliographie	188

CONTENTS

FOREWORD	7
INTRODUCTION	9
1 Scope	11
1.1 General.....	11
1.2 Application: new and pre-existing plants	11
1.3 Framework.....	11
2 Normative references	17
3 Definitions	21
4 Symbols and abbreviations	43
5 Overall safety life cycle of the I&C	43
5.1 Deriving the I&C requirements from the plant safety design base.....	51
5.2 Output documentation	55
5.3 Design of the total I&C architecture and assignment of the I&C functions	57
5.4 Overall planning	69
5.5 Output documentation	79
6 System safety life cycle	79
6.1 Requirements	87
6.2 System planning	111
6.3 Output documentation	121
6.4 System qualification	131
6.5 Summary of main specific requirements for different classes and categories	141
7 Overall integration and commissioning	143
7.1 Requirements on the objectives to be achieved	143
7.2 Output documentation	143
8 Overall operation and maintenance	143
8.1 Requirements on the objectives to be achieved	145
8.2 Output documentation	145
Annex A (informative) Basic safety issues in the NPP	147
Annex B (informative) Categorisation of functions and classification of systems	155
Annex C (informative) Qualitative defence approach against CCF	165
Annex D (informative) Relations of IEC 61508 with IEC 61513 and standards of the nuclear application sector	173
Bibliography	189

Figure 1 – Cadre général de la présente norme.....	14
Figure 2 – Relations types entre logiciel et matériel d'un système informatique.....	40
Figure 3 – Relations entre défaillance, défaillance aléatoire et défaut systématique.....	40
Figure 4 – Liens entre le cycle de vie et de sûreté global de l'I&C et les cycles de vie et de sûreté des systèmes d'I&C.....	48
Figure 5 – Cycle de vie et de sûreté du système	84
Figure 6 – Aspects devant être traités par le plan de qualification du système	138
Figure B.1 – Relations entre les fonctions d'I&C et les systèmes d'I&C.....	156
Figure C.1 – Exemples d'affectation des fonctions d'un groupe de sûreté aux systèmes d'I&C.....	164
Tableau 1 – Vue d'ensemble du cycle de vie et de sûreté global de l'I&C.....	46
Tableau 2 – Corrélation entre les classes des systèmes d'I&C et les catégories des FSE d'I&C.....	56
Tableau 3 – Vue d'ensemble du cycle de vie et de sûreté du système	82
Tableau 4 – Exigences relatives à la conception et à la qualification des systèmes et des équipements d'I&C.....	140
Tableau 5 – Exigences relatives à la spécification et à la mise en œuvre des FSE.....	140
Tableau B.1 – Classification typique des systèmes d'I&C	162

Withholding

Figure 1 – Overall framework of this standard	15
Figure 2 – Typical relations of hardware and software in a computer-based system	41
Figure 3 – Relations between system failure, random failure and systematic fault.....	41
Figure 4 – Connections between the overall safety life cycle of the I&C and the safety life cycles of the individual I&C systems	49
Figure 5 – System safety life cycle	85
Figure 6 – Topics to be addressed in the system qualification plan	139
Figure B.1 – Relations between I&C functions and I&C systems	157
Figure C.1 – Examples of assignment of functions of a safety group to I&C systems	165
Table 1 – Overview of the overall safety life cycle of the I&C	47
Table 2 – Correlation between classes of I&C systems and categories of I&C FSE	57
Table 3 – Overview of the system safety life cycle.....	83
Table 4 – Requirements for design and qualification of I&C systems and equipment.....	141
Table 5 – Requirements for the specification and implementation of the FSE	141
Table B.1 – Typical classification of I&C systems	163

Withdrawn

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

CENTRALES NUCLÉAIRES – INSTRUMENTATION ET CONTRÔLE COMMANDE DES SYSTÈMES IMPORTANTS POUR LA SÛRETÉ – PRESCRIPTIONS GÉNÉRALES POUR LES SYSTÈMES

AVANT-PROPOS

- 1) La CEI (Commission Electrotechnique Internationale) 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. 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 intéressés sont représentés dans chaque comité d'études.
- 3) Les documents produits se présentent sous la forme de recommandations internationales. Ils sont publiés comme normes, spécifications techniques, rapports techniques ou guides et agréés comme tels par les Comités nationaux.
- 4) Dans le but d'encourager l'unification internationale, les Comités nationaux de la CEI s'engagent à appliquer de façon transparente, dans la mesure possible, les Normes internationales de la CEI dans leurs normes nationales et régionales. Toute divergence entre la norme de la CEI et la norme nationale ou régionale correspondante doit être indiquée en termes clairs dans cette dernière.
- 5) La CEI n'a fixé aucune procédure concernant le marquage comme indication d'approbation et sa responsabilité n'est pas engagée quand un matériel est déclaré conforme à l'une de ses normes.
- 6) L'attention est attirée sur le fait que certains des éléments de la présente Norme internationale peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. La CEI ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété.

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

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
45A/405/FDIS	45A/418/RVD

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

Les annexes A, B, C et D sont données uniquement à titre d'information.

Cette publication a été rédigée selon les Directives ISO/CEI, Partie 3.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant 2006. A cette date, la publication sera

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

INTERNATIONAL ELECTROTECHNICAL COMMISSION

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

FOREWORD

- 1) The IEC (International Electrotechnical Commission) is a world-wide organisation for standardisation comprising all national electrotechnical committees (IEC National Committees). The object of the IEC is to promote international co-operation on all questions concerning standardisation in the electrical and electronic fields. To this end and in addition to other activities, the IEC publishes International Standards. 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 organisations liaising with the IEC also participate in this preparation. The IEC collaborates closely with the International Organisation for Standardisation (ISO) in accordance with conditions determined by agreement between the two organisations.
- 2) The formal decisions or agreements of the 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 National Committees
- 3) The documents produced have the form of recommendations for international use and are published in the form of standards, technical specifications, technical reports or guides and they are accepted by the National Committees in that sense.
- 4) In order to promote international unification, IEC National Committees undertake to apply IEC International Standards transparently to the maximum extent possible in their national and regional standards. Any divergence between the IEC Standard and the corresponding national or regional standard shall be clearly indicated in the latter.
- 5) The IEC provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with one of its standards.
- 6) Attention is drawn to the possibility that some of the elements of this International Standard may be the subject of patent rights. The IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 61513 has been prepared by subcommittee 45A: Reactor instrumentation, of IEC technical committee 45: Nuclear instrumentation.

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

FDIS	Report on voting
45A/405/FDIS	45A/418/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.

Annexes A, B, C and D are for information only.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 3.

The committee has decided that the contents of this publication will remain unchanged until 2006. At this date, the publication will be

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

INTRODUCTION

La présente Norme internationale établit les prescriptions 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.

La présente norme souligne les relations entre

- les objectifs de sûreté de la centrale nucléaire et les exigences relatives à l'architecture globale des systèmes d'I&C importants pour la sûreté;
- l'architecture globale des systèmes d'I&C et les exigences applicables à chacun des systèmes d'I&C importants pour la sûreté

Relations avec les autres normes

Les normes internationales CEI et ISO, la série de documents de l'AIEA relatifs à la sûreté et d'autres documents consensuels ont été utilisés pour l'élaboration de la présente norme. Notamment:

a) Les normes CEI du secteur nucléaire

La présente norme fait référence à d'autres normes CEI du secteur nucléaire, en particulier celles qui concernent les sujets ayant trait à la qualification, à la conception des salles de commande, à la catégorisation des fonctions et classification des systèmes (voir 3.4 et 3.6) et au multiplexage.

Lorsqu'il s'agit d'un système informatique de classe 1 (voir 5.1.2.1 et annexe B), la présente norme s'utilise conjointement avec la CEI 60880, la CEI 60880-2 et la CEI 60987 afin d'assurer l'exhaustivité des exigences relatives au logiciel et au matériel du système.

b) Autres normes internationales

La présente norme a adopté une présentation similaire à celle de la CEI 61508 avec un cycle de vie et de sûreté global et un cycle de vie des systèmes. Elle offre également une interprétation des prescriptions générales des parties 1, 2 et 4 de la CEI 61508 pour le secteur nucléaire. La conformité à la présente norme facilite la compatibilité avec les prescriptions de la CEI 61508 telles qu'elles ont été interprétées dans l'industrie nucléaire.

La présente norme fait référence aux normes ISO pour les thèmes liés à l'assurance qualité.

c) Documents de l'AIEA, série sûreté:

La présente norme a été élaborée 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. Ces documents s'appliquent plus généralement à toutes les normes du comité d'études 45 relatives à l'instrumentation et au contrôle commande. La terminologie et les définitions utilisées dans la présente norme sont conformes avec celles utilisées par l'AIEA (voir note).

NOTE Conformément à «l'accord de coopération sur les sujets d'intérêt commun» de mai 1981.

La présente norme fait référence à l'AIEA 50-C-QA (Rév. 1) pour les thèmes ayant trait à l'assurance qualité.

INTRODUCTION

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 total architecture of the I&C systems important to safety;
- total architecture of the I&C systems and the requirements of the individual systems important to safety.

Relationship with other standards

IEC and ISO International Standards, IAEA safety series documents and other consensus documents were used in the development of this standard. Notably:

a) IEC nuclear sector standards

This standard refers to other IEC nuclear standards, in particular those for topics related to qualification, control room design, categorisation of functions and classification of systems (see 3.4 and 3.6), and multiplexing.

When class 1 computer-based systems are addressed (see 5.1.2.1 and annex B), this standard is used in conjunction with IEC 60880, IEC 60880-2 and IEC 60987 to assure the completeness of the system requirements for the software and hardware.

b) Other international standards

This standard has adopted a presentation format similar to basic safety publication IEC 61508 with an overall safety life-cycle and a system life-cycle. The standard also provides an interpretation of the general requirements of IEC 61508, parts 1, 2 and 4, for the nuclear application sector. Compliance with this standard will facilitate consistency with the requirements of IEC 61508 as they have been interpreted for the nuclear industry.

This standard refers to ISO for topics related to quality assurance.

c) IAEA safety series documents

This standard has been developed to be consistent with the principles and basic safety aspects of the IAEA Code on the safety of nuclear power plants and the IAEA safety guides. Indeed, the IAEA documents apply to all technical committee 45 instrumentation and control standards. The terminology and definitions used by this standard are consistent with that used by the IAEA (see note).

NOTE According to the "agreement of co-operation on matters of common interest" of May 1981.

This standard refers to IAEA 50-C-QA (Rev 1) for topics in relation to quality assurance.

CENTRALES NUCLÉAIRES – INSTRUMENTATION ET CONTRÔLE COMMANDE DES SYSTÈMES IMPORTANTS POUR LA SÛRETÉ – PRESCRIPTIONS 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. La présente Norme internationale fait état des prescriptions et recommandations (voir note) relatives à l'architecture globale des systèmes d'I&C incluant l'une ou l'autre de ces technologies ou les deux.

NOTE Dans la suite de la présente norme, le terme «prescriptions» 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 y a lieu de» ou «il convient que».

La présente norme souligne la nécessité d'exigences complètes et précises, issues des objectifs de sûreté de la centrale, comme condition préalable à l'établissement des exigences générales relatives à l'architecture globale des systèmes d'I&C et à chaque système d'I&C important pour la sûreté.

La présente norme introduit les concepts de cycle de vie et de sûreté global pour l'ensemble de l'architecture d'I&C, et de cycle de vie et de sûreté pour chaque système d'I&C. 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.

1.2 Application: centrales nouvelles et préexistantes

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 prescriptions est applicable. Ce sous-ensemble est défini au début de chaque projet.

1.3 Cadre général

La figure 1 présente le cadre général de la présente norme, avec ses articles normatifs:

- l'article 5 traite de l'architecture globale des systèmes d'I&C importants pour la sûreté:
 - définition des exigences relatives aux fonctions d'I&C et aux systèmes et équipements associés (FSE d'I&C) déduites de l'analyse de sûreté de la centrale, de la catégorisation des fonctions d'I&C, de l'aménagement de la centrale et du contexte opérationnel;
 - découpage de l'architecture globale 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 une défense en profondeur et à la minimisation du risque de défaillance de cause commune (DCC);
 - établissement des plans relatifs à l'architecture globale des systèmes d'I&C.

NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL FOR SYSTEMS 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. This International Standard provides requirements and recommendations (see note) for the total I&C system architecture which may contain either or both technologies.

NOTE In the following, the term requirements 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".

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

This standard introduces the concept of a safety life cycle for the total I&C system architecture, and a safety life cycle for the individual systems. 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.

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 is identified at the beginning of any project.

1.3 Framework

Figure 1 presents the overall framework of this standard, with its normative clauses:

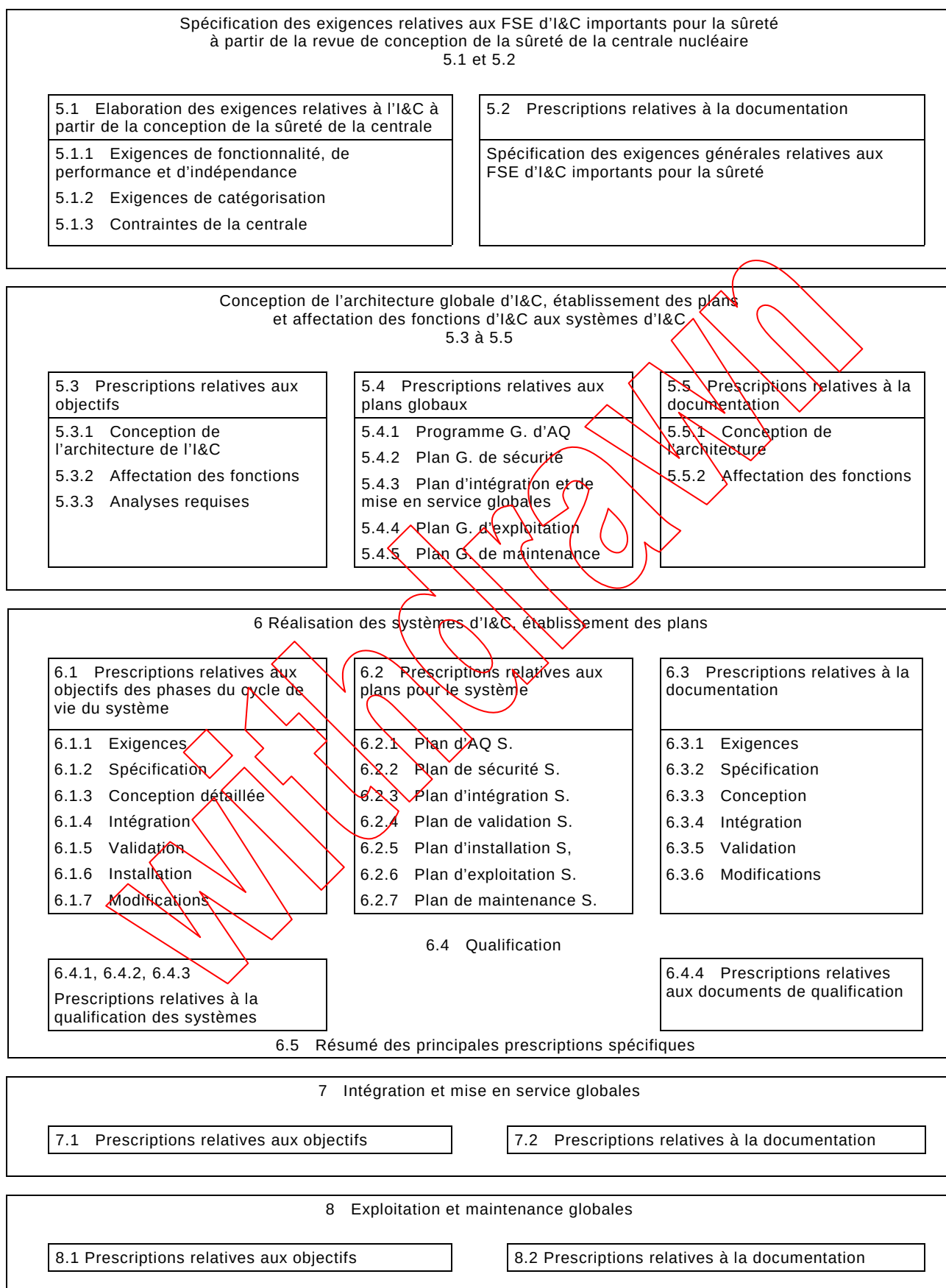
- clause 5 addresses the total architecture of the I&C systems important to safety:
 - defining requirements for the I&C functions, and associated systems and equipment (I&C FSE) derived from the safety analysis of the NPP, the categorisation of I&C functions, and the plant lay-out and operation context;
 - structuring the totality of the 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 minimise potential for common cause failure (CCF);
 - planning the total architecture of I&C systems.

- l'article 6 traite des prescriptions relatives à chacun des systèmes d'I&C importants pour la sûreté, en particulier celles relatives aux systèmes informatiques;
- les articles 7 et 8 traitent de l'intégration, mise en service, exploitation et maintenance globales des systèmes d'I&C;
- 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 classification;
- l'annexe C présente des exemples de sensibilité de l'I&C aux DCC;
- l'annexe D est un guide pour la comparaison de la présente norme avec les parties 1, 2 et 4 de la CEI 61508. Elle examine les principales prescriptions de la CEI 61508 afin de vérifier que les questions liées à la sûreté sont abordées correctement. Elle envisage l'emploi de termes communs et justifie s'il y a lieu d'adopter des techniques ou des termes différents ou complémentaires.

Withdrawn

- clause 6 addresses the requirements for the individual I&C systems important to safety, particularly the requirements for computer-based systems;
- clauses 7 and 8 address the overall integration, commissioning, operation and maintenance of the I&C systems;
- 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.

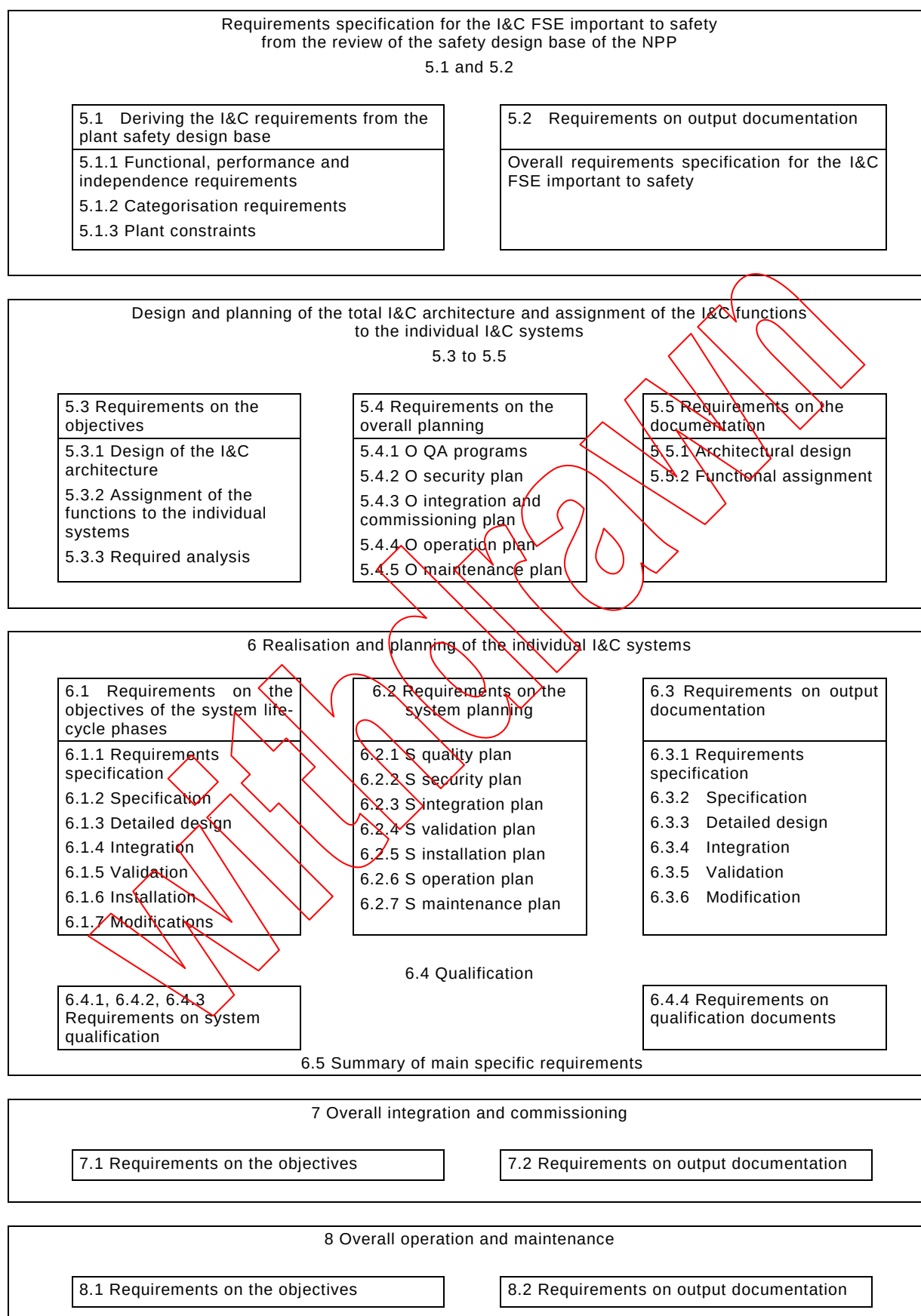
Withdrawn



Légende: AQ: Assurance Qualité; G: Global; S: Système

IEC 188/01

Figure 1 – Cadre général de la présente norme



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

IEC 188/01

Figure 1 – Overall framework of this standard

2 Références normatives

Les documents normatifs suivants contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions valables pour la présente Norme internationale. Pour les références datées, les amendements ultérieurs ou les révisions de ces publications ne s'appliquent pas. Toutefois, les parties prenantes aux accords fondés sur la présente Norme internationale sont invitées à rechercher la possibilité d'appliquer les éditions les plus récentes des documents normatifs indiqués ci-après. Pour les références non datées, la dernière édition du document normatif en référence s'applique. Les membres de la CEI et de l'ISO possèdent le registre des Normes internationales en vigueur.

CEI 60709:1981, *Séparation dans le système de protection des réacteurs*

CEI 60780:1998, *Centrales nucléaires – Equipements électriques de sûreté – Qualification*

CEI 60880:1986, *Logiciel pour les calculateurs utilisés dans les systèmes de sûreté des centrales nucléaires*

CEI 60880-2:2000, *Logiciel pour les calculateurs de sûreté des centrales nucléaires – Partie 2: Défense contre les défaillances de cause commune provoquées par le logiciel, utilisation d'outils logiciels et de logiciels prédéveloppés*

CEI 60964:1989, *Conception des salles de commande des centrales nucléaires*

CEI 60965:1989, *Points de commande supplémentaires pour l'arrêt des réacteurs sans accès à la salle de commande principale (salle de commande de repli)*

CEI 60987:1989, *Calculateurs programmés importants pour la sûreté des centrales nucléaires*

CEI 61000-4-1:2000, *Compatibilité électromagnétique (CEM) – Partie 4-1: Techniques d'essai et de mesure – Vue d'ensemble de la série CEI 61000-4*

CEI 61000-4-2:1995, *Compatibilité électromagnétique (CEM) – Partie 4: Techniques d'essai et de mesure – Section 2: Essais d'immunité aux décharges électrostatiques. Publication fondamentale en CEM*

CEI 61000-4-3:1995, *Compatibilité électromagnétique (CEM) – Partie 4: Techniques d'essai et de mesure – Section 3: Essai d'immunité aux champs électromagnétiques rayonnés et aux fréquences radioélectriques*

CEI 61000-4-4:1995, *Compatibilité électromagnétique (CEM) – Partie 4: Techniques d'essai et de mesure – Section 4: Essais d'immunité aux transitoires électriques rapides en salves. Publication fondamentale en CEM*

CEI 61000-4-5:1995, *Compatibilité électromagnétique (CEM) – Partie 4: Techniques d'essai et de mesure – Section 5: Essai d'immunité aux ondes de choc*

CEI 61000-4-6:1996, *Compatibilité électromagnétique (CEM) – Partie 4: Techniques d'essai et de mesure – Section 6: Immunité aux perturbations conduites, induites par les champs radioélectriques*

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*

CEI 61226:1993, *Centrales nucléaires – Systèmes d'instrumentation et de contrôle-commande importants pour la sûreté – Classification*

2 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this International Standard. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this International Standard are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the normative document referred to applies. Members of IEC and ISO maintain registers of currently valid International Standards.

IEC 60709:1981, *Separation within the reactor protection system*

IEC 60780:1998, *Nuclear power plants – Electrical equipment of the safety system – Qualification*

IEC 60880:1986, *Software for computers in the safety systems of nuclear power stations*

IEC 60880-2:2000, *Software for computers important to safety for nuclear power plants – Part 2: Software aspects of defence against common cause failures, use of software tools and of pre-developed software*

IEC 60964:1989, *Design for control rooms of nuclear power plants*

IEC 60965:1989, *Supplementary control points for reactor shutdown without access to the main control room*

IEC 60987:1989, *Programmed digital computers important to safety for nuclear power stations*

IEC 61000-4-1:2000, *Electromagnetic compatibility (EMC) – Part 4-1: Testing and measurement techniques – Overview of IEC 61000-4 series*

IEC 61000-4-2:1995, *Electromagnetic compatibility (EMC) – Part 4: Testing and measurement techniques – Section 2: Electrostatic discharge immunity test. Basic EMC Publication*

IEC 61000-4-3:1995, *Electromagnetic compatibility (EMC) – Part 4: Testing and measurement techniques – Section 3: Radiated, radio-frequency, electromagnetic field immunity test*

IEC 61000-4-4:1995, *Electromagnetic compatibility (EMC) – Part 4: Testing and measurement techniques – Section 4: Electrical fast transient/burst immunity test. Basic EMC Publication*

IEC 61000-4-5:1995, *Electromagnetic compatibility (EMC) – Part 4: Testing and measurement techniques – Section 5: Surge immunity test*

IEC 61000-4-6:1996, *Electromagnetic compatibility (EMC) – Part 4: Testing and measurement techniques – Section 6: Immunity to conducted disturbances, induced by radio-frequency fields*

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*

IEC 61226:1993, *Nuclear power plants – Instrumentation and control systems important for safety – Classification*

CEI 61500:1996, *Centrales nucléaires – Systèmes de contrôle commande importants pour la sûreté – Prescriptions fonctionnelles pour la transmission de données multiplexées*

CEI 61508-1:1998, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 1: Prescriptions générales*

CEI 61508-2:2000, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 2: Prescriptions pour les systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité*

CEI 61508-4:1998, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 4: Définitions et abréviations*

ISO/CEI 12207:1995, *Technologies de l'information – Processus du cycle de vie du logiciel*

ISO 8402:1994, *Management de la qualité et assurance de la qualité – Vocabulaire*

ISO 9000-3:1997, *Normes pour le management de la qualité et l'assurance qualité – Partie 3: Conseils pour l'application de l'ISO 9001:1994 au développement, à la mise à disposition, à l'installation et à la maintenance du logiciel*

ISO 9001:1994, *Systèmes qualité – Modèles pour l'assurance de la qualité en conception, développement, production, installation et prestations associées*

AIEA Série Sûreté n° 50-C-D (Rév 1):1988, *Code de sûreté des centrales nucléaires: Conception*

AIEA Série Sûreté n° 50-C-QA (Rév 1):1988, *Code de sûreté des centrales nucléaires: Assurance Qualité*

AIEA Série Sûreté n° 50-SG-D1:1979, *Fonctions de sûreté et classification des composants pour les BWR, PWR et PTR – Guide de sûreté*

AIEA Série Sûreté n° 50-SG-D3:1980, *Système de protection et dispositifs associés dans les centrales nucléaires – Guide de sûreté*

AIEA Série Sûreté n° 50-SG-D8:1984, *Systèmes de contrôle commande liés à la sûreté dans les centrales nucléaires – Guide de sûreté*

AIEA Série Sûreté n° 50-SG-D11:1986, *Principes généraux de sûreté pour la conception des centrales nucléaires – Guide de sûreté*

AIEA Série Sûreté 75-INSAG-3:1988, *Principes de sûreté fondamentaux pour les centrales nucléaires*

IEC 61500:1996, *Nuclear power plants – Instrumentation and control systems important for safety – Functional requirements for multiplexed data transmission*

IEC 61508-1:1998, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements*

IEC 61508-2:2000, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

IEC 61508-4:1998, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations*

ISO/IEC 12207:1995, *Information technology - Software life cycle processes*

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

ISO 9000-3:1997, *Quality management and quality assurance standards – Part 3: Guidelines for the application of ISO 9001:1994 to the development, supply, installation and maintenance of computer software*

ISO 9001:1994, *Quality systems – Model for quality assurance in design, development, production, installation and servicing*

IAEA Safety Series No. 50-C-D (Rev 1):1988, *Code on the Safety of NPPs: Design*

IAEA Safety Series No. 50-C-QA (Rev 1):1988, *Code on the Safety of NPPs: Quality assurance*

IAEA Safety Series No. 50-SG-D1:1979, *Safety functions and Component Classification for BWR, PWR and PTR – A Safety Guide*

IAEA Safety Series No. 50-SG-D3:1980, *Protection system and related features in NPPs – A Safety Guide*

IAEA Safety Series No. 50-SG-D8:1984, *Safety-Related Instrumentation and Control Systems for NPPs – A Safety Guide*

IAEA Safety Series No. 50-SG-D11:1986, *General Design Safety Principles for NPPs – A Safety Guide*

IAEA Safety series 75-INSAG-3:1988, *Basic Safety Principles for NPPs*

3 Définitions

Pour les besoins de la présente Norme internationale, les définitions suivantes 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

[2.1 de la CEI 60880, modifié]

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

Voir figure 2.

NOTE 1 Voir également «fonction d'application», «bibliothèque d'application», «logiciel système».

NOTE 2 Le logiciel d'application contraste avec le logiciel système.

3.3

bibliothèque d'application

ensemble de modules logiciels qui exécutent des fonctions d'application standard

Voir figure 2.

NOTE Si des équipements préexistants sont utilisés, cette bibliothèque est considérée comme faisant partie du logiciel système et est qualifiée comme telle.

3.4

catégorie d'une fonction d'I&C

l'une des trois affectations 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 FSE de I&C. A chaque catégorie correspond un ensemble de prescriptions 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 dont 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

canal

ensemble de composants interconnectés dans un système générant un signal de sortie unique. Un canal perd ses propriétés lorsque plusieurs signaux de ce type sont combinés avec des signaux provenant d'autres canaux, tels que les canaux d'affichage ou les canaux des actionneurs de sûreté

[AIEA 50-SG-D8]

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'importance différente pour la sûreté. Une affectation «Non Classée» 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», «élément important pour la sûreté», «systèmes de sûreté».

3 Definitions

For the purposes of this International Standard, the following 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

[2.1 of IEC 60880, modified]

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

See figure 2.

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

NOTE 2 Application software contrasts with system software.

3.3

application software library

collection of software modules implementing typical application functions

See figure 2.

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

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 is not significant to safety

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

NOTE 2 IEC 61226 defines categories of I&C FSE. To each category 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 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 initiate a single output. A channel loses its identity where single-output signals are combined with signals from another channel, such as a monitoring channel or a safety actuation channel

[IAEA 50-SG-D8]

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 relevance. 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

défaillance de cause commune (DCC)

défaillance résultant d'un ou plusieurs événements, provoquant la défaillance simultanée de deux ou plusieurs canaux séparés d'un système multicanal ou de plusieurs systèmes, et conduisant à la défaillances du (des) système(s)

[3.6.10 de la CEI 61508-4, modifié]

NOTE En fonction du contexte, une DCC peut être considérée au niveau du système ou au niveau des systèmes qui constituent un groupe de sûreté.

3.8

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 [1] ¹⁾, modifié]

3.9

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 [1]]

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.

3.10

système informatique

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

Voir figure 2.

NOTE Voir également «système d'I&C».

3.11

mise en service de la centrale nucléaire

processus au cours duquel les composants et systèmes de la centrale nucléaire, une fois construits, sont rendus opérationnels et vérifiés comme étant conformes aux hypothèses de conception et aux critères de performance. Ce processus inclut les essais nucléaires et non nucléaires

[AIEA 50-C-D]

3.12

gestion de la configuration

discipline appliquant des mesures techniques et administratives pour identifier et documenter les caractéristiques fonctionnelles et physiques d'un élément de configuration, contrôler les modifications apportées à ces caractéristiques, enregistrer et signaler le processus des modifications et le statuts de réalisation et vérifier la conformité aux exigences spécifiées

[IEEE 610 [1]]

3.13

données

représentation d'informations ou d'instructions permettant la communication, l'interprétation ou le traitement par ordinateur.

[IEEE 610 [1], modifié]

¹⁾ Les chiffres entre crochets se réfèrent à la bibliographie.

3.7

common cause failure (CCF)

failure, which is the result of one or more events, causing coincident failures of two or more separate channels in a multiple channel system or in multiple systems, leading to system(s) failure

[3.6.10 of IEC 61508-4, modified]

NOTE Depending on the context, a CCF may be considered at the system level or at the level of the systems which constitute a safety group.

3.8

complexity

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

[IEEE 610 [1]¹⁾, modified]

3.9

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 [1]]

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.

3.10

computer-based system

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

See figure 2.

NOTE See also "I&C system".

3.11

commissioning of the NPP

process during which NPP components and systems, having been constructed, are made operational and verified to be in accordance with design assumptions and to have met the performance criteria; it includes both non-nuclear and nuclear tests

[IAEA 50-C-D]

3.12

configuration management

discipline applying technical and administrative direction and surveillance to identify and document the functional and physical characteristics of a configuration item, control changes to those characteristics, record and report change processing and implementation status, and verify compliance with specified requirements

[IEEE 610 [1]]

3.13

data

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

[IEEE 610 [1], modified]

See figure 2.

¹⁾ Figures in square brackets refer to the bibliography.

3.14

concept de la défense en profondeur

Voir article A.3.

3.15

méthode déterministe

Voir A.2.2.

3.16

diversité

existence d'au moins deux manières ou moyens différents d'atteindre un objectif spécifié. La diversité est spécifiquement prévue en tant que défense contre les DCC. Elle peut être réalisée par des systèmes physiquement différents les uns des autres, ou par une diversité fonctionnelle permettant à des systèmes réalisés avec des composants similaires d'atteindre l'objectif spécifié de différentes manières

[3.6 de la CEI 60880-2]

NOTE 1 Voir également «diversité fonctionnelle».

NOTE 2 Cette définition est plus étendue que celle utilisée par l'AtEA 50-C-D qui est rédigée comme suit: «existence de composants ou systèmes redondants pour remplir une fonction déterminée, lorsque ces composants ou systèmes pris collectivement possèdent une ou plusieurs caractéristiques qui les différencient. On peut donner comme exemple de ces caractéristiques: des conditions de fonctionnement différentes, des tailles de composants différentes, des fabricants différents, des principes de fonctionnement différents et des types de matériels utilisant des méthodes physiques différentes».

3.17

équipement

une ou plusieurs parties d'un système. Un composant système est une partie déterminée et définissable (et généralement amovible) d'un système

[CEI 61226, modifié]

NOTE 1 Voir également «composant», «système d'I&C».

NOTE 2 Un composant système peut contenir une partie logicielle.

NOTE 3 Les termes «composant système», «composant» et «module» sont souvent utilisés de manière interchangeable. La relation entre ces termes n'a pas encore été normalisée.

3.18

famille d'équipements

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 de composants fournit normalement un certain nombre de fonctionnalités standard (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».

3.19

erreur

différence entre une valeur ou condition calculée ou mesurée et la valeur ou condition réelle, spécifiée ou théorique

Voir figure 3.

3.14**defence-in-depth concept**

See clause A.3.

3.15**deterministic method**

See A.2.2.

3.16**diversity**

existence of two or more different ways or means of achieving a specified objective. Diversity is specifically provided as a defence against a common mode failure. It may be achieved by providing systems that are physically different from each other, or by functional diversity, where similar systems achieve the specified objective in different ways

[3.6 of IEC 60880-2]

NOTE 1 See also “functional diversity”.

NOTE 2 This definition is wider than that used by the IAEA 50-C-D which is as follows: “the existence of redundant components or systems to carry out an identified function, where such components or systems collectively incorporate one or more different attributes. Examples of such attributes are, different operating conditions, different sizes of equipment, different manufacturers, different working principles and types of equipment that use different physical methods”.

3.17**equipment**

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

[IEC 61226, modified]

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.

3.18**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 (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”.

3.19**error**

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

See figure 3.

3.20

appréciation d'une propriété d'un système

attribution d'une valeur qualitative ou quantitative à cette propriété de système

[2.2.2 de la CEI 61069-1]

3.21

défaillance

une défaillance survient lorsque le service réalisé s'écarte du service voulu

[3.8 de la CEI 60880-2]

Voir figure 3.

NOTE 1 Une défaillance est le résultat d'un défaut du matériel, d'un défaut du logiciel, d'un défaut du système ou d'une erreur de l'opérateur ou de la maintenance. Elle est engendrée par la trajectoire du signal associé.

NOTE 2 Voir aussi «défaut», «défaillance logicielle».

3.22

défaut

imperfection dans un composant matériel, logiciel ou système

Voir figure 3.

NOTE 1 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 2 Un défaut (notamment un défaut de conception) peut ne pas être détecté dans le système jusqu'à une situation telle que le résultat produit n'est pas conforme à la fonction prévue, c'est-à-dire qu'une défaillance se produit.

NOTE 3 Voir aussi «défaut logiciel».

3.23

diversité fonctionnelle

application de la diversité au niveau fonction (par exemple actionnement d'un déclenchement sur la limite de pression et sur la limite de température)

[3.10 de la CEI 60880-2]

NOTE Voir également «diversité».

3.24

validation fonctionnelle

vérification de la conformité des spécifications des fonctions d'application aux exigences des fonctions et des performances primaires de la centrale. Elle est complémentaire de la validation du système, qui vérifie la conformité du système à la spécification des fonctions

3.25

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 référence bibliographique [4]).

3.26

fonction importante pour la sûreté

objectif spécifique devant être atteint pour la sûreté

[AIEA 50-SG-D3 et CEI 61226, modifié]

NOTE Voir également «fonction d'I&C», «sous-fonction d'I&C», «fonction d'application».

3.20**evaluation (of a system property)**

attribution of a qualitative or quantitative value to that system property
[2.2.2 of IEC 61069-1]

3.21**failure**

failure occurs when the delivered service deviates from the intended service

[3.8 of IEC 60880-2]

See figure 3.

NOTE 1 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 2 See also “fault”, “software failure”.

3.22**fault**

defect in a hardware, software or system component

See figure 3.

NOTE 1 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 2 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 3 See also “software fault”.

3.23**functional diversity**

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

[3.10 of IEC 60880-2]

NOTE See also “diversity”.

3.24**functional validation**

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

3.25**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 bibliographical reference [4]).

3.26**function important to safety**

specific purpose that must be accomplished for safety

[IAEA 50-SG-D3 and IEC 61226, modified]

NOTE See also “I&C function”, “I&C subfunction”, “application function”.

3.27

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 la conséquence des EIH (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.

3.28

erreur (ou faute) humaine

action humaine ou procédure produisant un résultat indésirable

[3.12 de la CEI 60880-2]

3.29

équipement indépendant

équipement qui est indépendant et qui possède les deux caractéristiques suivantes:

- a) l'aptitude à réaliser sa fonction n'est pas affectée par le fonctionnement ou la défaillance des autres équipements;
- b) l'aptitude à réaliser sa fonction n'est pas affectée par les effets résultant de l'événement initiateur ayant déclenché son fonctionnement

[AIEA 50-SG-D8]

NOTE Les moyens permettant de garantir l'indépendance dans la conception sont l'isolation électrique (également appelée isolation fonctionnelle dans les documents de l'AIEA), la séparation physique et l'indépendance des communications.

3.30

interruption

suspension d'une opération, par exemple l'exécution d'un programme informatique, provoquée par un événement extérieur à cette opération

[IEEE 610]

3.31

architecture de l'I&C

structure organisant les systèmes d'I&C 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.

3.32

fonction d'I&C

fonction permettant de commander, exploiter et/ou surveiller une partie définie du procédé

NOTE 1 Voir également «sous-fonction d'I&C», «FSE d'I&C», «fonction d'application».

NOTE 2 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 3 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.

3.27**hazard**

event having the potential to cause damage to plant personnel, 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 a consequence of a PIEs (for example, LOCA, steam-line break).

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

3.28**human error (or mistake)**

a human action or procedure that produces an unintended result

[3.12 of IEC 60880-2]

3.29**independent equipment**

equipment that is independent possesses both of the following characteristics:

- a) the ability to perform its required function is unaffected by the operation or failure of other equipment;
- b) the ability to perform its function is unaffected by the presence of the effects resulting from the postulated initiating event for which it is required to function

[IAEA 50-SG-D8]

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

3.30**interrupt**

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

[IEEE 610]

3.31**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 not classified systems and equipment.

3.32**I&C function**

function to control, operate and/or monitor a defined part of the process

NOTE 1 See also "I&C subfunction", "I&C FSE", "application function".

NOTE 2 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 3 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.

3.33

sous-fonction d'I&C

subdivision d'une fonction d'I&C affectée à un système ou à un sous-système I&C

NOTE 1 Voir également «fonction d'I&C», «fonction d'application».

NOTE 2 Le terme «fonction» est souvent utilisé pour «sous-fonction» si le contexte n'est pas ambigu.

3.34

FSE I&C: les fonctions et les systèmes et équipements d'I&C associés

actions menées en réponse à une situation ou pour atteindre un objectif. Les systèmes et équipements associés sont l'ensemble des composants, et les composants eux-mêmes, utilisés pour accomplir ces fonctions

[CEI 61226, modifié]

NOTE Voir également «fonction d'I&C», «système d'I&C».

3.35

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 propres ou partagées.

[3.3.2 de la CEI 61508-4, modifié]

NOTE 1 Voir également «système», «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 leurs fonctionnalités propres, 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 article B.4).

3.36

architecture d'un système d'I&C

structure organisant un système d'I&C

NOTE Voir également «architecture de l'I&C».

3.37

éléments importants pour la sûreté

éléments concernés par un ou plusieurs des groupes suivants:

- structures, systèmes et composants dont le défaut de fonctionnement ou la défaillance pourrait engendrer l'exposition excessive aux rayonnements du personnel du site ou du public;
- structures, systèmes et composants qui empêchent les incidents opérationnels hypothétiques d'engendrer des situations accidentelles;
- moyens prévus pour atténuer les conséquences d'un défaut de fonctionnement ou d'une défaillance des structures, systèmes ou composants.

[AIEA 50-SG-D3]

NOTE 1 Voir également «système de sûreté», «classe d'un système d'I&C».

NOTE 2 Dans la présente norme, les systèmes d'I&C importants pour la sûreté sont répartis en trois classes: 1, 2, 3.

NOTE 3 Le document AIEA 50-SG-D8 répartit les systèmes importants pour la sûreté en «systèmes de sûreté» et «systèmes liés à la sûreté».

3.33

I&C subfunction

subdivision of an I&C function allocated to an I&C system or subsystem

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

NOTE 2 The term “function”, is often used for “subfunction” if the context is not ambiguous.

3.34

I&C FSE: functions, and the associated systems and equipment

functions are carried out for a purpose or to achieve a goal. The associated systems and equipment are the collection of components and the components themselves that are employed to achieve the functions

[IEC 61226, modified]

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

3.35

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.

[3.3.2 of IEC 61508-4, modified]

NOTE 1 See also “system, 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 and control systems, HMI systems, interlock systems and protection systems (see clause B.4).

3.36

I&C system architecture

organisational structure of an I&C system

NOTE See also “I&C architecture”.

3.37

items important to safety

the items which comprise:

- 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 which prevent anticipated operational occurrences from leading to accident conditions; and
- c) those features which are provided to mitigate the consequences of malfunction or failure of structures, systems or components

[IAEA 50-SG-D3]

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

NOTE 2 In this standard, I&C systems important to safety are divided into three classes: 1, 2, 3.

NOTE 3 IAEA 50-SG-D8 divides the systems important to safety into “safety systems” and “safety-related systems”.

3.38

maintenabilité

probabilité de mener à bien, pendant une période donnée, une action d'entretien sur un constituant ayant des conditions d'utilisation données, cet entretien étant effectué dans des conditions fixées et suivant des procédures et des moyens fixés

[2.10 de la CEI 60987, modifié]

3.39

cycle de vie et de sûreté global 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 la sûreté de la centrale) et le retrait du service du dernier système d'I&C

[3.7.1 de la CEI 61508-4, modifié]

NOTE 1 Le cycle de vie et de sûreté global de l'I&C fait référence aux cycles de vie et de sûreté des systèmes.

NOTE 2 Voir aussi «cycle de vie et de sûreté du système».

3.40

analyse de sûreté de la centrale

Voir article A.2.

3.41

événement initiateur hypothétique (EIH)

les EIH représentent les événements engendrant des incidents opérationnels hypothétiques ou des situations accidentelles, ainsi que les effets des défaillances produites

[AIEA 50-C-D]

NOTE 1 Incidents opérationnels hypothétiques: tous les automatismes s'écartant de leur fonctionnement normal. Il est prévu qu'ils surviennent une ou plusieurs fois au cours du temps d'exploitation de la centrale. Ils sont pris en compte des les phases de conception et ne causent ainsi aucun dommage important aux systèmes importants pour la sûreté ni ne conduisent à des situations accidentelles.

NOTE 2 Les causes primaires des EIH peuvent être des défaillances possibles des équipements et des erreurs de l'opérateur (à l'intérieur ou à l'extérieur de la centrale nucléaire), des événements provoqués par l'homme ou des événements naturels. Il faut que la spécification des EIH soit acceptable pour l'organisme de réglementation compétent pour la centrale nucléaire.

3.42

logiciel prédéveloppé

logiciel existant, disponible dans le commerce ou en tant que produit protégé par des droits de propriété, dont l'utilisation est envisagée dans un système informatique

[3.17 de la CEI 60880-2]

NOTE Les logiciels prédéveloppés (LPD) peuvent être séparés en deux groupes: LPD polyvalents n'ayant pas été développés pour un environnement matériel particulier, et LPD intégrés dans des composants matériels et devant être utilisés avec ces derniers.

3.43

méthode probabiliste

Voir A.2.2.

3.44

organisation en charge du projet

organisation(s) ou personnes responsables, pendant les phases du cycle de vie et de sûreté global de l'I&C et/ou pendant les phases des cycles de vie et 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 contraste avec l'«organisation en charge de l'exploitation».

3.38**maintainability**

probability that a given active maintenance action to an item under given conditions of use can be carried out within a stated time interval when the maintenance is performed under stated conditions and using stated procedures and resources

[2.10 of IEC 60987]

3.39**overall safety life cycle of the I&C**

necessary activities involved in the implementation of the systems and equipment important to safety of the 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

[3.7.1 of IEC 61508-4, modified]

NOTE 1 The overall safety lifecycle of the I&C refers to the individual system safety life cycles.

NOTE 2 See also "system safety lifecycle".

3.40**plant safety analysis**

See clause A.2.

3.41**postulated initiating event (PIE)**

PIEs identify events that lead to anticipated operational occurrences or accident conditions and their consequential failure effects

[IAEA 50-C-D]

NOTE 1 Anticipated operational occurrences: All operational processes deviating from normal operation which are expected to occur once or several times during the operating life of the plant and which, in view of appropriate design provisions, do not cause any significant damage to items important to safety nor lead to accident conditions.

NOTE 2 The primary causes of PIE may be credible equipment failures and operator errors (both within and external to the NPP), man-induced or natural events. The specification of the PIEs must be acceptable to the regulatory body for the NPP.

3.42**pre-developed software (PDS)**

software which already exists, is available as a commercial or proprietary product and is being considered for use in a computer-based system

[3.17 of IEC 60880-2]

NOTE Pre-developed software (PDS) may be divided into: general-purpose PDS that has not been specifically developed for a specific hardware environment, and PDS integrated in hardware components that has to be used in association with this hardware.

3.43**probabilistic method**

See A.2.2.

3.44**project organisation**

organisation(s) or individuals that have responsibility during the phases of the overall safety life cycle of the I&C 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".

3.45

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

3.46

qualité

ensemble des caractéristiques d'une entité qui lui confèrent l'aptitude à satisfaire des besoins exprimés ou implicites

[2.1 de l'ISO 8402]

3.47

assurance qualité

toutes les actions planifiées et systématiques nécessaires pour assurer qu'un produit ou un service satisfait aux exigences données en matière de qualité

[3.5 de l'ISO 8402, modifié]

3.48

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

3.49

redondance

mise en place d'éléments ou systèmes supplémentaires (identiques ou différents), afin que chaque élément ou système puisse exécuter la fonction requise indépendamment de l'état de fonctionnement ou de défaillance des autres

[AIEA 50-SG-D8]

3.50

fiabilité

probabilité qu'un dispositif, système ou installation exécute ses fonctions attendues d'une manière satisfaisante pendant une durée donnée dans des conditions opérationnelles données

[AIEA 50-SG-D8]

NOTE La fiabilité d'un système informatique est composée de la fiabilité du matériel et de la fiabilité du logiciel. La fiabilité du matériel est en général quantifiée. Celle du logiciel est en général une valeur qualitative dans la mesure où il n'existe pas de moyen reconnu pour la quantifier.

3.51

logiciel réutilisable

module de logiciel pouvant être utilisé dans plusieurs programmes informatiques ou systèmes de logiciels

[IEEE 610 [1], modifié]

3.52

groupe de sûreté

ensemble des équipements destinés à prendre toutes les mesures nécessaires relatives à un EIH particulier afin d'assurer que les limites spécifiées dans le cahier des charges de cet événement ne sont pas dépassées

[AIEA 50-SG-D3]

NOTE Le groupe de sûreté peut contenir des fonctions d'I&C de différentes catégories.

3.45**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

3.46**quality**

totality of characteristics of an entity that bear on its ability to satisfy stated and implied needs

[2.1 of ISO 8402]

3.47**quality assurance**

all those planned and systematic actions necessary to provide adequate confidence that a product or service will satisfy given requirements for quality

[3.5 of ISO 8402, modified]

3.48**quality plan**

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

3.49**redundancy**

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

[IAEA 50-SG-D8]

3.50**reliability**

probability that a device, system or facility will perform its intended functions satisfactorily for a specified time under stated operating conditions

[IAEA 50-SG-D8]

NOTE The reliability of a CB 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 put a figure on the reliability of software.

3.51**reusable software**

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

[IEEE 610 [1], modified]

3.52**safety group**

assembly of equipment designated to perform all actions required for a particular PIE to ensure that the limits specified in the design basis for the event are not exceeded

[IAEA 50-SG-D3]

NOTE The I&C functions in a safety group may be placed in different categories.

3.53

systèmes de sûreté

systèmes importants pour la sûreté, prévus pour assurer, dans toutes les conditions, l'arrêt sûr du réacteur et l'évacuation de la chaleur du cœur et/ou pour limiter les conséquences des incidents opérationnels hypothétiques et des situations accidentelles

[AIEA 50-SG-D8]

NOTE 1 Voir également «système important pour la sûreté», «classe d'un système d'I&C».

NOTE 2 Le système de sûreté de l'AIEA correspond en général aux systèmes de classe 1 mentionnés dans la présente norme.

3.54

sécurité

capacité d'un système informatique à protéger les informations et les données afin que les personnes ou systèmes non autorisés ne puissent les lire ni les modifier et que les personnes ou systèmes autorisés puissent y accéder

[3.25 de l'ISO/CEI 12207, modifié]

3.55

défaillance unique

défaillance aléatoire qui engendre la perte de capacité d'un composant ou d'un système à exécuter ses fonctions prévues. Les défaillances consécutives à un seul événement aléatoire sont considérées comme faisant partie de la défaillance unique

[AIEA 50-SG-D8, modifié]

NOTE 1 Voir également «critère de défaillance unique».

NOTE 2 La défaillance unique peut être la conséquence d'un événement dangereux interne ou externe à la centrale.

3.56

critère de défaillance unique

un ensemble d'équipements satisfait au critère de défaillance unique s'il est en mesure de remplir son objectif en dépit d'une défaillance aléatoire unique supposée se produire n'importe où dans l'ensemble. Les défaillances consécutives à une défaillance unique sont considérées comme faisant partie intégrante de la défaillance unique

[AIEA 50-C-D]

NOTE 1 Voir également «défaillance unique», «défaillance logicielle».

NOTE 2 Les défaillances dues au logiciel sont des défaillances systématiques et non aléatoires.

3.57

défaillance logicielle

défaillance du système due à l'activation d'un défaut de conception dans un composant du 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».

3.58

défaut logiciel

défaut de conception situé dans un composant du logiciel

NOTE Voir aussi «défaut».

3.59

fiabilité logicielle

composante de la fiabilité du système qui dépend des défaillances du logiciel

3.53**safety systems**

systems important to safety, provided to ensure, in any condition, the safe shutdown of the reactor and the heat removal from the core, and/or to limit the consequences of anticipated operational occurrences and accident conditions

[IAEA 50-SG-D8]

NOTE 1 See also “system important to safety”, “class of an I&C system”.

NOTE 2 The safety system of IAEA corresponds generally to class 1 systems in this standard.

3.54**security**

capability of the CB system to protect information and data so that unauthorized persons or systems cannot read or modify them and authorised persons or systems are not denied access to them

[3.25 of ISO/IEC 12207, modified]

3.55**single failure**

random failure which results in the loss of capability of a component or system to perform its intended functions. Consequential failures resulting from a single random occurrence are considered to be part of the single failure

[IAEA 50-SG-D8, modified]

NOTE 1 See also “single-failure criterion”.

NOTE 2 The single failure may be the consequence of a plant internal or external hazard event.

3.56**single-failure criterion**

assembly of equipment which satisfies the single-failure criterion if it is able to meet its purpose despite a single random failure assumed to occur anywhere in the assembly. Consequential failures resulting from the assumed single failure are considered to be an integral part of the single failure

[IAEA 50-C-D]

NOTE 1 See also “single failure”, “software failure”.

NOTE 2 Failures due to software are systematic and not random failures.

3.57**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”.

3.58**software fault**

design fault located in a software component

NOTE See also “fault”.

3.59**software reliability**

component of the system reliability which depends on software failures

3.60

spécification

document qui spécifie, de manière complète, précise et vérifiable, les prescriptions, la conception, le comportement ou autres caractéristiques d'un système ou composant et, souvent, les procédures permettant de déterminer si ces dispositions ont bien été respectées

[3.21 de la CEI 60880-2 et IEEE 610 [1]]

3.61

système

ensemble de composants qui interagissent conformément à une conception donnée, un élément d'un système pouvant être un autre système, appelé sous système

[3.3.1 de la CEI 61508-4, modifié]

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.

3.62

défaillance systématique

défaillance reliée de façon déterministe à une certaine cause, ne pouvant être éliminée que par une modification de la conception ou du processus de fabrication, des procédures d'exploitation, de la documentation ou d'autres facteurs appropriés

[3.6.6 de la CEI 61508-4]

3.63

cycle de vie et 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 vie et de sûreté du système fait référence aux activités du cycle de vie et de sûreté global.

NOTE 2 Voir aussi «cycle de vie et de sûreté global de l'I&C».

3.64

logiciel système

logiciel conçu pour un système programmé ou pour une famille de systèmes programmés afin de faciliter l'exploitation et la maintenance du système programmé et des programmes associés, par exemple systèmes d'exploitation, compilateurs, utilitaires. Le logiciel système se compose en général du logiciel système opérationnel et du logiciel de support

[3.24 de la CEI 60880-2]

Voir figure 2.

NOTE 1 Logiciels opérationnels: logiciels fonctionnant sur le processeur cible pendant le fonctionnement du système. Exemples : le système d'exploitation, les gestionnaires d'entrée/sortie, le gestionnaire d'exceptions, les logiciels de communication, les bibliothèques d'application, les diagnostics en ligne, la gestion de la redondance et la dégradation progressive.

NOTE 2 Logiciels de soutien: logiciels d'aide au développement, aux essais ou à la maintenance des autres logiciels. Exemples : les compilateurs, les générateurs de code, les éditeurs graphiques, les diagnostics hors-ligne, les outils de vérification et de validation, etc.

NOTE 3 Voir également «logiciel d'application».

3.60 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.

[3.21 of IEC 60880-2 and IEEE 610 [1]]

3.61 system

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

[3.3.1 of IEC 61508-4, modified]

NOTE 1 See also "I&C system".

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

3.62 systematic failure

failure 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

[3.6.6 of IEC 61508-4]

3.63 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 safety life cycle.

NOTE 2 See also "overall safety life cycle of the I&C".

3.64 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

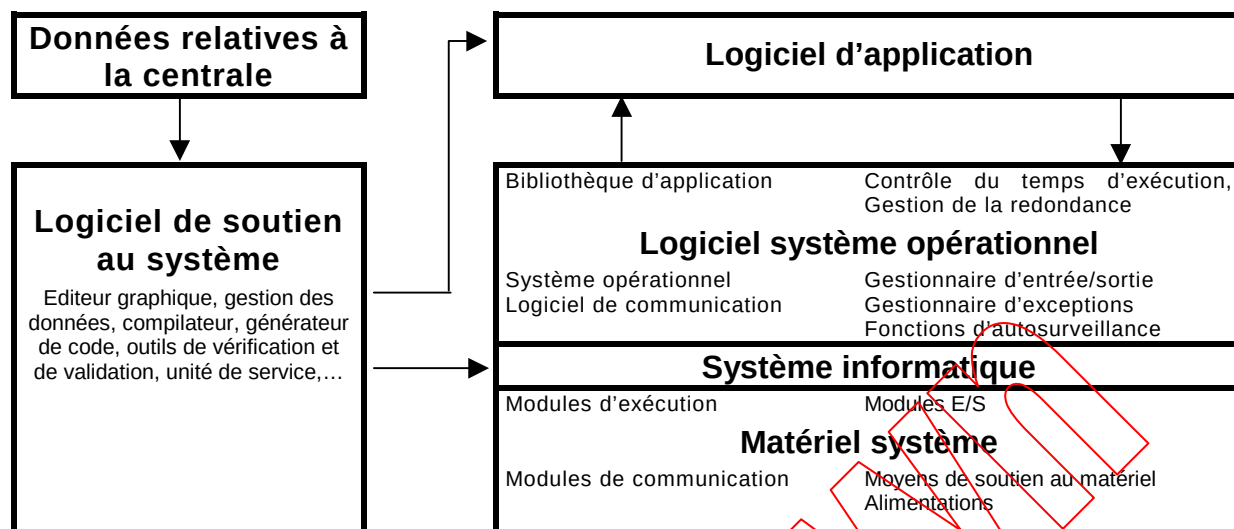
[3.24 of IEC 60880-2]

See figure 2.

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.

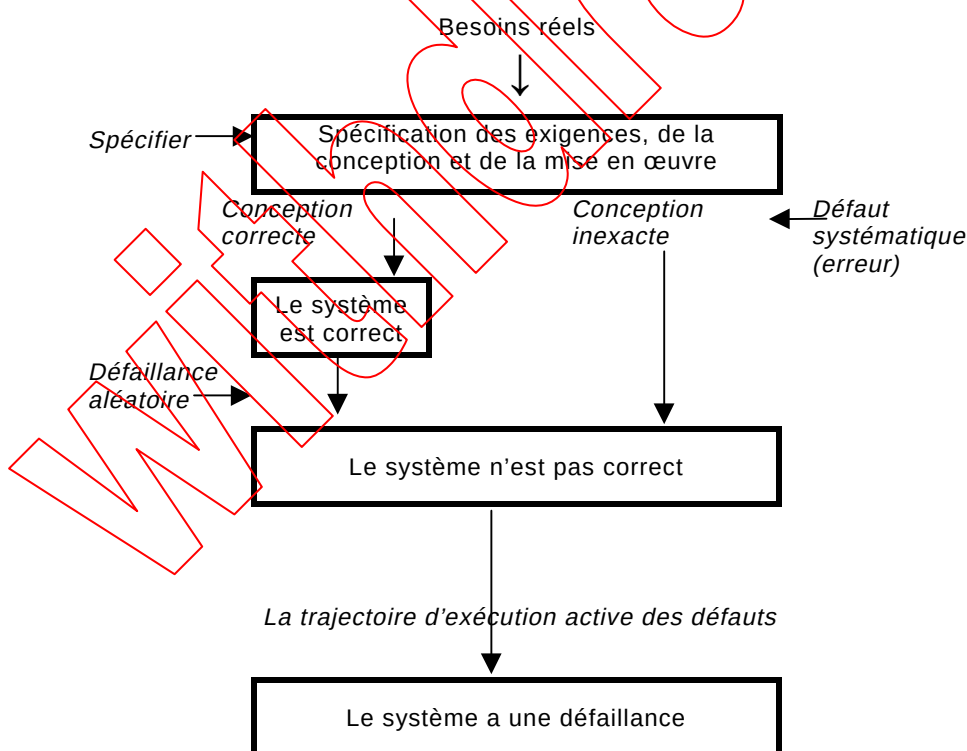
NOTE 2 Support software: software that aids in the development, test, or maintenance of other software and of the system such as compilers, code generators, graphic editor, off-line diagnostic, verification and validation tools, etc.

NOTE 3 See also "application software".



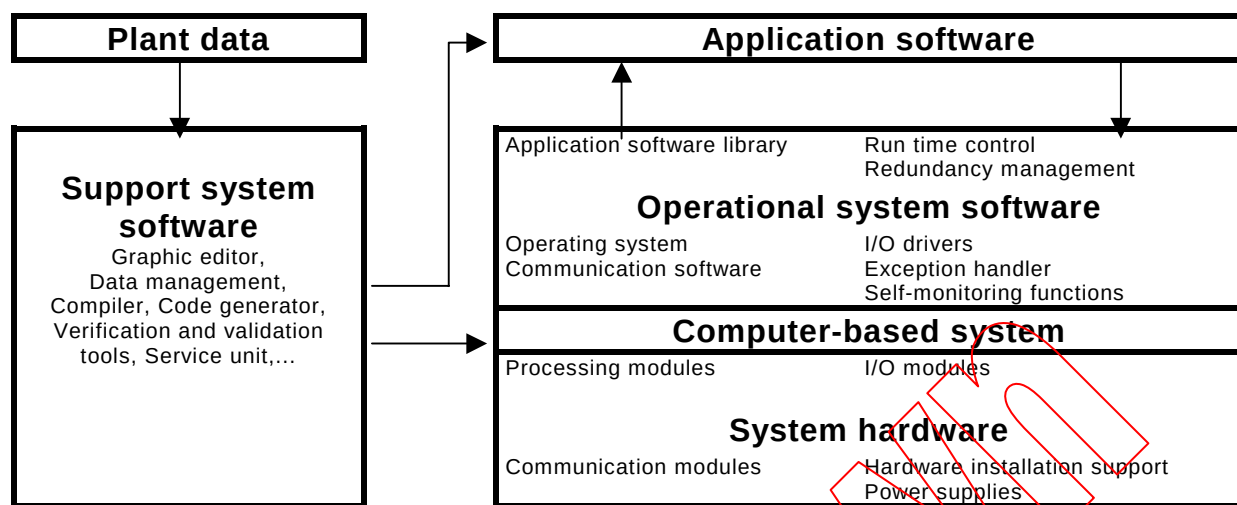
IEC 189/01

Figure 2 – Relations types entre logiciel et matériel d'un système informatique



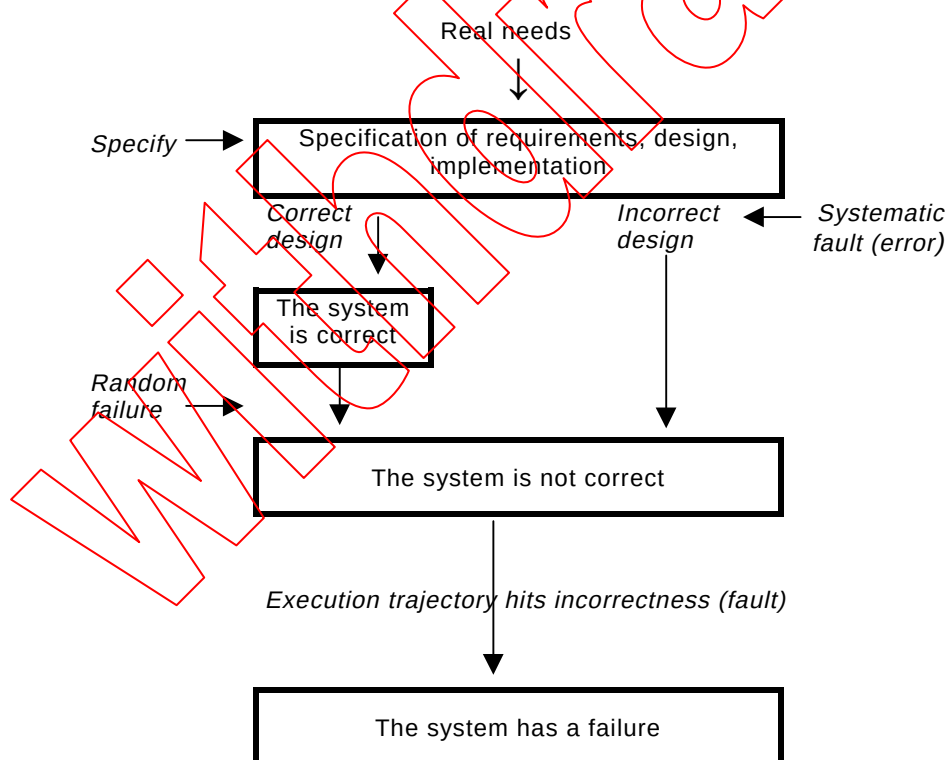
IEC 190/01

Figure 3 – Relations entre défaillance, défaillance aléatoire et défaut systématique



IEC 189/01

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



IEC 190/01

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

4 Symboles et abréviations

DCC	Défaillance de cause commune
COTS	Composants sur étagère du commerce
EUC	Équipement commandé
FSE	Fonctions, et systèmes et équipements associés
IEM	Interférence électromagnétique
IHM	Interface homme-machine
I&C	Instrumentation et contrôle commande
E/S	Entrée/sortie
LOCA	Accident de perte de réfrigérant primaire
EIH	Événement initiateur hypothétique
EPS	Etude probabiliste de sûreté
AQ	Assurance qualité
LPD	Logiciel prédéveloppé
SIL	Niveau d'intégrité de sûreté
E/E/PES	Système électrique/électronique/électronique programmable

5 Cycle de vie et de sûreté global de l'I&C

L'objectif de cet article est de définir la manière de

- déduire les exigences globales relatives aux FSE d'I&C importants pour la sûreté à partir de la conception de la sûreté de la centrale nucléaire (voir articles A.1 et A.2);
- déduire les exigences relatives à l'architecture des systèmes importants pour la sûreté à partir des exigences globales des FSE d'I&C, et
- d'établir les relations entre les exigences relatives à l'architecture de l'I&C et celles relatives aux systèmes individuels d'I&C importants pour la sûreté.

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 et de sûreté global de l'I&C. Ce cycle de vie et de sûreté global fait référence, à son tour, aux cycles de vie et de sûreté des systèmes d'I&C (voir l'article 6).

Les phases d'un cycle de vie et de sûreté global de l'I&C type comprennent:

- a) la revue de la conception de sûreté de la centrale, y compris (voir 5.1):
 - les exigences de fonctionnalité, de performance et d'indépendance;
 - les exigences relatives à la catégorisation;
 - les contraintes de la centrale;
- b) la définition de la spécification des exigences globales relatives aux FSE I&C importants pour la sûreté (voir 5.2);
- c) la conception de l'architecture globale de l'I&C et l'affectation des fonctions d'I&C aux systèmes et équipements (voir 5.3);
- d) la définition de la planification globale (voir 5.4);
- e) la réalisation des systèmes individuels (voir article 6);

4 Symbols and abbreviations

CB	Computer-based
CCF	Common-cause failure
COTS	Commercial off-the-shelf
EMI	Electromagnetic interference
EUC	Equipment under command
FSE	Functions, and associated systems and equipment
HMI	Human machine interface
I&C	Instrumentation and control
I/O	Input/output
LOCA	Loss of coolant accident
NPP	Nuclear power plant
PDS	Pre-developed software
PIE	Postulated initiating events
PSA	Probabilistic safety assessment
QA	Quality assurance
SIL	Safety integrity level
E/E/PES	Electrical/electronic/programmable electronic system

5 Overall safety life cycle of the I&C

The objective of this clause is to define how to

- derive the overall requirements for the I&C FSE important to safety from the safety design base of the NPP (see clause A.1 and A.2);
- derive the requirements for the architecture of the I&C systems important to safety from the overall requirements of the I&C FSE, and
- establish the relations between the requirements of the I&C architecture and the requirements of the individual I&C systems important to safety.

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 an I&C overall safety life cycle. 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 safety life cycle of the I&C include

- a) review of the plant safety design base including (see 5.1):
 - functional, performance and independence requirements;
 - functional categorisation;
 - constraints from the plant context;
- b) definition of the overall requirements specification of the I&C FSE important to safety (see 5.2);
- c) design of the overall I&C architecture and assignment of the I&C functions to individual systems and equipment (see 5.3);
- d) definition of the overall planning (see 5.4);
- e) realisation of the individual systems (see clause 6);

- f) l'intégration et la mise en service globales des systèmes (voir article 7);
- g) l'exploitation et la maintenance globales (voir 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 et de sûreté global et les cycles de vie et de sûreté des systèmes d'I&C sont représentés de manière simplifiée à la figure 4.

- a) Le cycle de vie et de sûreté global 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.

NOTE La responsabilité de la sûreté d'une centrale nucléaire incombe à l'organisation en charge de l'exploitation et ne peut en aucun cas être réduite du fait des responsabilités déléguées aux concepteurs, fournisseurs, constructeurs et régulateurs impliqués dans les différentes activités (voir 3.1.2 de l'AIEA 75 INSAG-3).

Withdrawal

- 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 safety life cycle of the total I&C 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) a phase shall only be finished if the preceding phases have been completed.

NOTE The responsibility for the safety of an NPP rests with the operating organisation and can in no way be diluted by responsibilities delegated to designers, suppliers, constructors and regulators involved in the different activities (see 3.1.2 of IAEA 75-INSAG-3).

Withdrawn

Tableau 1 – Vue d'ensemble du cycle de vie et de sûreté global de l'I&C

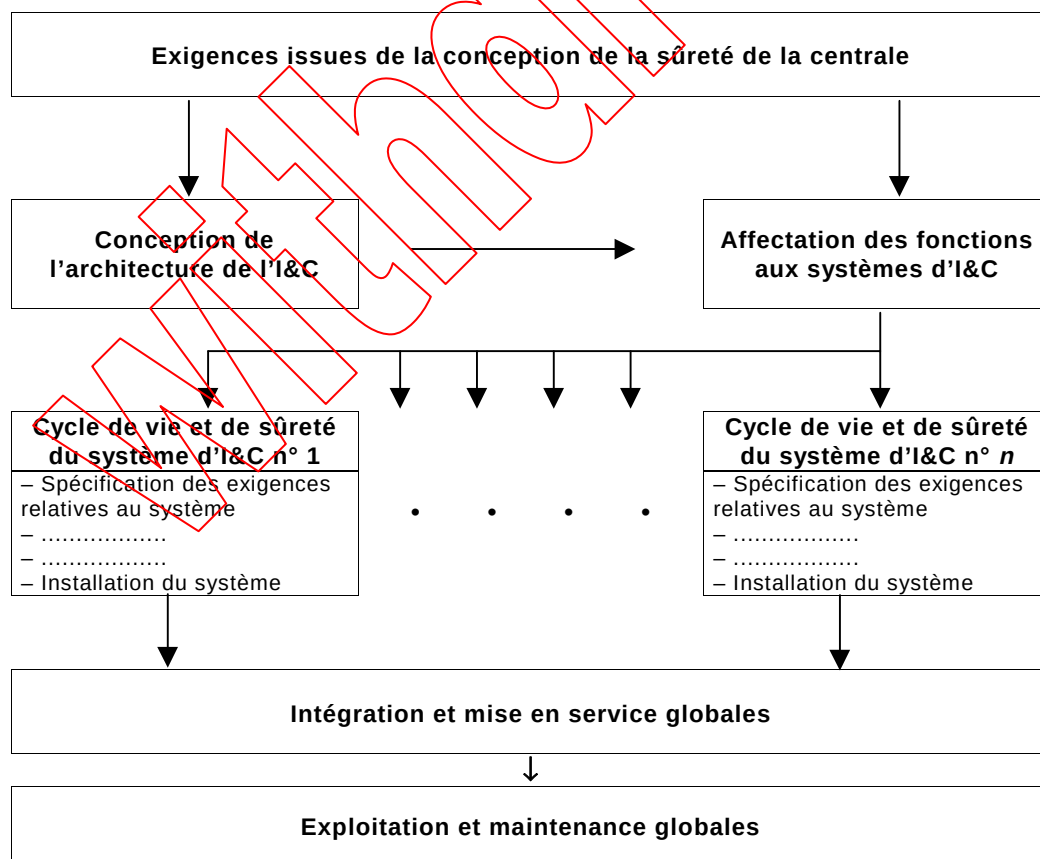
Article ou paragraphe	Entrées	Objectifs de l'activité	Domaine d'application	Sorties
5	Exigences relatives au cycle de vie et de sûreté global et relations avec les cycles de vie et de sûreté des systèmes			
5.1 <i>Elaboration des exigences relatives à l'I&C à partir de la conception de la sûreté de la centrale</i>				
5.1.1 Revue des exigences de fonctionnalité, de performance et d'indépendance	Documents de conception de la sûreté de la centrale Principes d'exploitation de la centrale	Identifier – les exigences de fonctionnalité et de performance des FSE d'I&C importants pour la sûreté – les exigences d'indépendance imposées aux FSE d'I&C par le concept de défense en profondeur de la centrale – les fonctions automatiques et les tâches de l'opérateur	Systèmes de la centrale et FSE d'I&C associés importants pour la sûreté	Identification des exigences relatives aux entrées de 5.2
5.1.2 Revue des exigences de catégorisation	Catégorisation de la sûreté de la centrale	Identifier la catégorisation des FSE Vérifier leur exhaustivité Vérifier la faisabilité des exigences complexes	FSE d'I&C importants pour la sûreté	Identification des exigences relatives aux entrées de 5.2
5.1.3 Revue des contraintes de la centrale	Documents relatifs à l'aménagement de la centrale et base de données de la 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	Disposition de la Centrale Systèmes de la centrale et FSE d'I&C	Identification des contraintes pour la conception de l'architecture (5.3) et pour la spécification des exigences relatives aux systèmes individuels d'I&C (6.1)
5.2 Documentation	Sorties de 5.1	Développer la spécification des exigences globales relatives aux FSE I&C importants pour la sûreté en termes d'exigences de fonctionnalité, performance, indépendance et catégorisation	FSE d'I&C	Spécification des exigences globales relatives aux FSE pour 5.3
5.3 <i>Conception de l'architecture globale de l'I&C et affectation des fonctions d'I&C</i>				
5.3.1 Conception de l'architecture de l'I&C	Sorties de 5.2	Développer une architecture des systèmes d'I&C convenable afin de mettre en œuvre les spécifications des exigences relatives aux FSE 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 de l'I&C en termes de systèmes automatiques, IHM et interconnexions (5.5.1)
5.3.2 Affectation des fonctions	Sorties de 5.3.1 et 5.4 (Itération avec les sorties de 6.3)	Affecter les fonctions d'I&C aux systèmes et équipements d'I&C Concevoir des exigences (limites, classification, 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 (5.5.2)
5.3.3 Analyses requises	Sorties de 5.3.1 et 5.3.2	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 (5.3.3.1) Evaluation des facteurs humains (5.3.3.2)

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

Clause or subclause	Inputs	Objectives of the activity	Scope	Outputs
5	Requirements placed upon the overall safety life cycle and its relationship to the systems' life cycles			
5.1 Deriving the I&C requirements from the plant safety design base				
5.1.1 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 FSE important to safety, – the independence requirements placed upon the I&C FSE by the defence in-depth concept of the plant, – the automatic functions and operator task	Plant systems and related I&C FSE important to safety	Identification of input requirements for 5.2
5.1.2 Review of the categorisation requirements	Plant safety categorisation	To identify the categorisation of FSE To verify for completeness To verify for feasibility of complex requirements	I&C FSE important to safety	Identification of input requirements for 5.2
5.1.3 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 FSE	Identification of constraints for the architectural design (see 5.3) and for the requirements specification of the individual I&C systems (see 6.1)
5.2 Output documentation	Outputs of 5.1	To develop the overall requirements specification of the I&C FSE important to safety in terms of functional, performance, independence and categorisation requirements	I&C FSE	Overall requirements specification of FSE for 5.3
5.3 Design of the total I&C architecture and assignment of the I&C functions				
5.3.1 Design of the I&C architecture	Output of 5.2	To develop the design of the architecture of I&C systems suitable to implement the overall requirements specifications of the I&C FSE 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 5.5.1)
5.3.2 Functional assignment	Output of 5.3.1 and 5.4 (Iteration with output of 6.3)	To assign the I&C functions to the individual I&C systems and equipment To provide requirements (boundaries, classification, functionality, reliability and other required properties) for the individual I&C systems	I&C functions and I&C systems	Requirements for the application functions of systems and HMI, the design of the I&C systems and the tools (see 5.5.2)
5.3.3 Required analysis	Outputs of 5.3.1 and 5.3.2	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 (5.3.3.1) Assessment of human factors (5.3.3.2)

Tableau 1 (suite)

Paragraphe	Entrées	Objectifs de l'activité	Domaine d'application	Sorties
5.4 Planification globale	Sortie de 5.3	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 Cycle de vie et de sûreté du système	Sorties de 5.5	Spécifier et créer des systèmes d'I&C conformes à la spécification de l'architecture de l'I&C (voir article 6)	Systèmes individuels d'I&C	Les sorties sont décrites au tableau 3
7 Intégration et mise en service globales	Sortie de 5.4.3 et 6.2.5	Tester et mettre en service les systèmes interconnectés de l'architecture de l'I&C	Systèmes d'I&C de l'architecture de l'I&C	Systèmes intégrés et mis en service Rapport de mise en service (7.2)
8 Exploitation et maintenance globales	Sortie de 5.4.4, 5.4.5 et 7.1	Exploiter, entretenir et réparer les systèmes afin de maintenir le niveau de sûreté	Systèmes d'I&C de l'architecture de l'I&C	Exécution des fonctions Enregistrements de fonctionnement et de maintenance (8.2)
NOTE Pour une comparaison de cette définition des phases avec celle de la CEI 61508-1, voir l'annexe D.				



IEC 191/01

Figure 4 – Liens entre le cycle de vie et de sûreté global de l'I&C et les cycles de vie et de sûreté des systèmes d'I&C